

SUBMISSION TO THE CONSULTATION  
**ACCC Digital Platforms Inquiry  
Preliminary Report**

Dr. Kate Mathews Hunt  
Honorary Adjunct Assistant Professor| Bond University  
SJD (Bond) LLM (Melb) LLB (Hons) BA (Hons) (Melb)

**To: Australian Competition & Consumer Commission**  
**Att: Secretariat**  
**Date: 5 March 2019**  
**Re: ACCC DIGITAL PLATFORMS INQUIRY PRELIMINARY REPORT DEC 2019 SUBMISSION**

I wish to thank the ACCC for this opportunity to provide a submission to its ACCC Digital Platforms Inquiry Preliminary Report (**Preliminary Report**).

In particular, I appreciate the grant of a formal extension to enable me to complete these comments.

### Overview

The ACCC and its Preliminary Report is to be commended for the following:

1. the calibre and content of the Preliminary Report is comprehensive and high. Having said that, it is a small bite of the big cherry: the ACCC should continue this work, on an ongoing basis, across the entire gamut of online issues facing (and besetting) Australian consumers;
2. the finding of a **regulatory and market failure** as to personal data collection practices in Australia is both significant and exponential.  
It is reflected in my (and many other's) extensive work on this topic.<sup>1</sup> We are significantly and seriously BEHIND the EU, which evidences best practice data protection laws at this time. Having said that, the General Data Protection Regulation ('GDPR') is imperfect and there is no reason why Australia should not aim for the highest consumer protection levels in this area. Is there?
3. For ease of reference, I cite, largely support and comment upon the submission provided by the Consumer Policy Research Centre (CPRC). In particular, their summary as to findings (inclusive of my comments follows):
  - a. **Information asymmetry** between huge, powerful, non-transparent, data-gathering platforms and individual consumers;
  - b. the exertion of that significant (in my view, cleverly, incisively, anti-consumer) **'bargaining power'** as to privacy collection, data-gathering and consent-obtaining practices;
  - c. the inherent difficulty – one might say **impossibility - for consumers** to assess, much less understand, the meaning, effects and impacts of data sharing both now and into the future; and
  - d. the **lack of appropriate, effective, targeted legal deterrents** to the corporate behaviours which create, sustain and promote deceptive and exploitative data collection, use and disclosure practices.
4. The CPRC is correct to make the initial comment that a lack of integration in the digital platforms area is a significant regulatory weakness. Albeit controversial, I endorse the potential for the ACCC to formally adopt this regulatory area (given its neat fit into consumer and competition law generally), and in my view, to overcome the poor enforcement of consumer privacy generally in this country.  
It is quite impossible to separate privacy law from digital platform regulation. This is a regulatory weakness which has been (exploited?) - enjoyed - by the powerful, international digital platforms in this country.

---

<sup>1</sup> Kate Mathews Hunt, consumer-IOT, Thesis 2017. Copy attached.

5. incorporating certain aspects of the *General Data Protection Regulation* (GDPR) into its recommendations, such as the right to deletion/ to be forgotten.  
**I would recommend that Australia adopt the GDPR legislatively in full, given our corporations trading into the EU are obliged to comply with its terms and it is regarded as best practice privacy regulation at this time.** The GDPR was formulated based upon extensive and long-term analysis; we should be guided and informed by their work. Having said that, it also has privacy compromises that we might consider 'not' accepting in the modern digital context.
6. undertaking specific and quite novel consumer research for the Inquiry. In particular, the '*Consumer Views and Behaviours on Digital Platforms*' study is of significant interest. I would encourage the ACCC (perhaps reflecting EU and FTC practice) to conduct a range of investigative law and economic research in this area, going forward. Constant assessment and monitoring is required to regulate digital platforms.
7. Regulators (internationally) as to privacy and consumer law need to work together closely, on a long-term basis. One should never underestimate the size, power, social reach and capacity of the digital platforms involved, or their behaviour in an online universe.

In terms of **criticism**, the following comments are submitted:

1. the obvious point is "more, more, more".  
 We need a standing commitment to constantly studying and investigating the digital platforms, their practices and the impacts upon society. See for example, recent reports as to increasing formal FTC activity in this area.<sup>2</sup>
2. Why are we so slow to address such critically important social rights and issues?  
 For example, the concept that consumers *do not understand* the data collection and use practices of the platforms, is incontrovertible. Please see my thesis attached on this point, much less recent research by the ACCC, CPRC, and ACCAN.<sup>3</sup> We also await the AHRC report with interest.
3. It is time the Australian government addressed these issues, using EU research (and US where available). Australia is behind in a regulatory enforcement context and Australians are suffering potentially long-term data abuses as a result.
4. See numerous **other comments** in the attached submission.

### The author

I am an Australian consumer, legal practitioner and academic with an especial interest in the legal rights and protections afforded to my fellow Australian consumers in a burgeoning online universe. As a former corporate lawyer, I believe in the transformative effects of regulation and regulatory enforcement – when appropriately targeted and implemented.

**Thank you for this opportunity.**

---

<sup>2</sup> <https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology>. See e.g. tech commentary here: <https://www.theverge.com/2019/2/26/18241491/ftc-task-force-tech-monopolies-bureau-competition-online-platforms>

<sup>3</sup>

## Introduction

I have read and agree with the CPRC submission dated 15 February 2019, in its entirety. I have therefore followed that submission order below, but have added additional comments where necessary.

I wish to express some frustration that the European Commission (EU) has conducted extensive research and work into the issue of digital platform regulation, and in particular, issues pertaining to consumer data gathering, consent and privacy (as well as competition law). Given that **identical issues apply**, it is of concern that Australia has not rapidly adopted or (if necessary, rapidly repeated) that research in our context.

Without wishing to sound alarmist, I cannot emphasise how technology, data gathering, advertising, data (mis)use such as consumer profiling (and arguably online tracking), machine learning, artificial intelligence and potential discrimination against consumer - and human - rights are **inextricably connected**.

It is urgent, if appropriate consumer-protective moral and legal parameters are to be set, that legislators provide appropriate powers and that regulators take serious action on these issues NOW.

## Submission

For ease of reference, my submission follows that of the Consumer Policy Research Centre ('CPRC') with my variations, as follows:

1. The CPRC is correct to identify significant concern at the **fragmentation of digital platform/ data management inquiry** in this country. It is correct to identify a range of current, pressing, serious issues which should be considered together comprehensively, if this issue is to properly be evaluated and managed (see CPRC, page 4).

The two issues are inseparable. Data is THE "oil".

The Federal Government needs to allocate the broadest remit to the ACCC to review, monitor and investigate (as necessary) the digital platforms (obviously inclusive of apps, etc) from both competition and consumer law perspectives. Those perspectives include, from a data context, provision of clear, simple information and consent, data ownership (and potential recompense for use), data valuation, a clear understanding of data collection and use practices, and the long-term value (which may be significant).

2. The CPRC is correct to identify that tech leaders from *Microsoft* have acknowledged that regulation is required, particularly as to data gathering and artificial intelligence. Note also that (even) *Facebook* have acknowledged that regulation is required.
3. The CPRC is correct to identify that recent initiatives such as the consumer data right are important, but in the overall perspective, piecemeal. This requires redress.
4. The CPRC is correct to identify that the intersection between consumer, privacy and competition law has (in my terms) **collided**. I add that while the "levers" are held within the *Privacy Act*, the demonstrable failure of enforcement, has rendered the privacy regime frequently unobserved and ultimately, the Act ineffective. For example, the ACCC might review the enforcement as to data breach both pre and post the recent federal legislation.

I would further add that there are significant differences between the relevant (unenforceable) Guidelines, and the (enforceable) Privacy Principles, which require urgent reconciliation. The former is arguably very good practice; the latter does not reflect this, nor has been enforced in that way. A simple example is the recent *Grubb* case where ultimately, mobile phone location data was not found to be "personal information" despite the capacity (albeit with some systems-related difficulty) of the collector to discern who it was location tracking.<sup>4</sup>

5. **CPRC point (1) Increasing consumer comprehension and agency (CPRC page 4):** I reinforce that more information will not achieve this. Indeed, in my view, the ACCC or ACL should prescribe acceptable formats and

---

<sup>4</sup> For an optimistic take on the decision, see <https://www.oaic.gov.au/media-and-speeches/statements/privacy-commissioner-v-telstra-corporation-limited-federal-court-decision> I would argue the decision to be very wrong and very disappointing; as it fails to reflect international decisions as to location data constituting personal information, or to understand how an organization can or may in the future, merge data within its possession. In fact, court decisions go further in the EU and in the GDPR: see Art. 4(1).

approaches. In particular, dashboards and other graphic, “simpler” approaches are clearer to consumers. As it is, no one reads, as the reading is so difficult and incomprehensible an experience. Further, if all platforms enjoy the incomprehension, they are incentivised to continue the practice, which arguably, involves deception of consumers.

## 6. CPRC point (2), (3): agree (mostly)

Transparency is critical and is the most absent feature of terms. The fact is that terms are designed to lack transparency, and even lawyer-conducted reviews cannot understand what data is collected, how much, how to stop collection and how it is used/ transferred (etc). The recommendation that further (desktop) and Australian research might assist to ascertain how to improve this issue is sound. But, the reality is, based upon EU research, that something simpler and more transparent which actually incentivises collectors to sharply improve their practices, is required. In particular, third party uses are described by category, not name – how does this really disclose how many and to whom, data is realistically disclosed? It may be that (for example) a simple, publicised, legislated grading structure or independent third party scheme would be more effective – i.e. they don't use my data much so grade 1 is good; they must be cavalier as grade 4 is unacceptable.

The purpose of data collection is irrelevant. It is likely consumers will (generously) share more with non-commercial uses, but the disclosure requirements should be equal for whichever data use is intended – and also, significantly, as to future data uses. The CPRC is right to refer to (unexpected and undisclosed) data transfer, on-sale and sharing. For example, who would expect that a sex toy would collect and report its use identified to the user, and then send the data across US borders?<sup>5</sup> There are hundreds of not thousands of these outrageous examples. I do not agree with the CPRC that “primary purpose” is an adequate or appropriate indicia for coverage under any disclosure scheme. ANY use should activate disclosure and consent. I want to know if the Red Cross sells my data (collected for donation purposes) to an advertiser (a genetic platform for example) just as much as if it were their primary purpose of collection. It is not inconceivable that even Facebook might assert that data gathering is not their primary purpose – after all, as they say, they do not “sell” your data,

Strengthen consent requirements: privacy protective defaults are a must. So too, should be the requirement that ALL sharing with any entity be disclosed. It is not enough to disclose ‘with our ad agency’; which agenc(ies)? We should not remain complicit with this ejusdem generis style of disclosure: a descriptor should not supplant a NAME. Further, and equally significant, is the fact that consumers should NOT be obliged to provide one iota of data that is not required for provision of the service: how often have you downloaded an app which asks for your date of birth, when year alone – or nothing – would still enable provision of the service. The critical point is *necessity* (as opposed to data gathering invention or worse).

Nudges are unconscionable as they prey upon behavioural attributes of people, usually without their knowledge. The ACCC has shown itself to be effective in addressing some nudging in relation to the airlines; but more of this type of work is needed – especially in an online consent or data gathering context.

The CPRC is correct to contend that interest-based advertising or online behavioural advertising offends and shocks people. People do NOT understand cookies or other tracking devices. Numerous overseas studies have found this, as has the CPRC study. Functional cookies are okay; but what about tracking cookies when people may not understand how they work or the implications in terms of the ads they see, the profiling they suffer - and so on?

Erasure of personal information – and the right to be forgotten - is part of the GDPR. Let's protect consumers – and get with that program. We all realise that future uses are virtually unpredictable; and everyone should have the right to withdraw their data should they wish to do so. The question for regulators is how to enforce this right and how to ensure that data is truly (meaningfully) deleted – a mandatory reporting scheme may be necessary, as well as notifications to entities to whom data was shared (and to their sharing partners, etc etc).

The CPRC are correct to identify that children's data protection and reidentification/ deidentification are very serious issues. The latter cannot be guaranteed – ever it seems. There are innumerable examples of the reID of deID information – and of adverse consequences for consumers. Even the Australian Government has (with respect) promised that de-ID data is safe, only to find re-ID has occurred.<sup>6</sup> That those promises are made in the context of

<sup>5</sup> <https://www.afr.com/technology/web/security/wevibe-vibrators-maker-settles-data-collection-lawsuit-for-us375-million-20170315-guy8qy>

<sup>6</sup> <https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records>

data which is called “sensitive personal information” (i.e. health data) under the Privacy Act (and thus subject to more significant controls) is alarming. Consumers deserve better.

Privacy Act breaches should be as significant as those for ACL breaches. This is particularly so as data breach or misuse can often be irretrievable and its effects long-lasting; plus there is a clear need to incentivise improved compliance. Companies will respond - if significant penalties encourage them to. It is time that privacy became a valued Australian asset.

A direct consumer right of action is imperative.

*Expand OAIC Resourcing:* While expanding resourcing is imperative, I am not convinced that the OAIC has the culture or capacity to meet a very significant and arduous challenge. I would prefer to see the ACCC expand to take on this role, given its greater compliance and enforcement traditions. It should also be noted that frequently, there is a synergy or overlap between privacy and consumer/ competition law breach. **It would be more efficient, more effective and more likely immediately effective given its reputation and track record, to appoint the ACCC to oversee the privacy regime – in conjunction with its other responsibilities. Of course, this must be fully resourced to meet a big challenge and great compliance imperative.** Note this is not unusual as the US FTC undertakes both roles to a large extent.

*Proposed areas for future development 7:* Yes but note that there is already a Guidelines and Australian privacy principle obligation on this regard. But businesses are not (I strongly suspect) complying. This needs to be addressed.

*Proposed areas for future development 8:* Yes. There is a strong industry push that people like targeted advertising – but significant research to suggest the contrary. I am concerned about the filter bubble aspect of this as well as the wholesale lack of consent - and the fact that personally, I would prefer NOT to be tracked. Note that while there are search engines and other ways to avoid this type of tracking, the main platforms are not it, and most consumers would not understand what to do or how to do it. It is again, an argument for privacy-by-default.

The CPRC is correct to identify gaps in the Privacy Act application as to smaller businesses under \$3M etc. These were no doubt compromises at the time it was enacted, but the privacy challenge and regime the world-over has changed. The time has now come to elevate privacy given the increased risk and potential for breach across every data collector. Best practice should require **all data collectors** (whether incidental or not) be covered by and abide by the (revised, improved) *Privacy Act*.

*Proposed areas for future development 9:* Yes, yes, yes. The range of unfair practices besetting consumers online is significant. As is the range of arguably unconscionable terms, unfair terms etc. The levers we have are good but not enough – as evidenced by the lack of cases directly relevant to the areas pertaining to digital platforms.

\* \* \*

I trust that this submission is of assistance. I am available at any time to discuss the matters within the Inquiry at your convenience.

Thank you once again for the opportunity to make comment on your excellent report

Yours faithfully,

Dr Kate Mathews Hunt

**Honorary Adjunct Assistant Professor| Bond University**  
**Special Counsel| Mathews Hunt Legal**  
**SJD (Bond) LLM (Melb) LLB(Hons) BA(Hons) (Melb)**  
**Contact| 0412 307 023**  
**Email| kmathews@bond.edu.au**

Enc.



## **consumeR-IOT: where every thing collides**

**Promoting consumer internet of things  
protection in Australia**

**Kate Mathews-Hunt**

LLM LLB(Hons) BA(Hons) Uni Melb.

Submitted in final fulfilment of the requirements of the degree of  
Doctor of Legal Science (Research)

25 September 2017

Faculty of Law

Professor Dan Svantesson & Professor Brenda Marshall

*This research was supported by an Australian Government Research Training Program Scholarship.*

## Abstract

The ‘smart’(ly) disruptive world of the consumer internet of things (CIOT) is here. Australian consumers are poised to live in ‘smart’ homes, monitor their ‘smart’ selves and ride in ever- ‘smart’er cars, while smart(er) cities, transport and industrial IOT brilliance changes their world, and the world around them, irretrievably. This thesis both celebrates and exposes this radical, impending CIOT-driven disruption in all its consumer-abusive, privacy-intrusive glory. It posits that consumers and regulators do not yet understand the adverse implications of this new panopticon technology which surveys *everything* and blurs traditional understandings of human autonomy and privacy, nor has consumer law yet properly tackled the many adverse implications of an expanded big data universe: from ubiquitous collection to consumer profiling and analytics, anonymisation failures, data breach and so on. With the coming of the consumer IOT, there is a perfect consumer-adverse storm, in which multiple fast-paced and little-regulated technologies *collide* - seismically. As one of the first few legal studies of the consumer internet of things in Australia, this thesis partly fills a vast gap in scholarly literature by scoping the Australian CIOT and its stakes, identifying potential gaps in Australian consumer protective laws, and adapting the Australian *Consumer Law Policy Framework* (Framework) to the critical question of whether the CIOT exhibits consumer detriment sufficient to warrant regulatory action now, using the smart car, home and self contexts as rapidly-evolving reference-points. Informed by aspects of behavioural economics, regulatory theory and the first international CIOT cases and defect reports, this thesis is a confronting snapshot which concludes with a call for strategic policy and various regulatory and self-regulatory actions. It also proposes a simple series of draft principles for CIOT policy and regulation which synthesise established best practice by design and default, conform to the normative Framework values and offer an improved prospect of protecting and realising the indisputable public interest in a principled, morally-grounded<sup>1</sup> and trusted CIOT world.

**Key objectives** and the research outline are detailed in **Annex. A**.

**Key words:** Internet of things – IoT - consumer law – privacy law – smart - policy

---

<sup>1</sup> Accenture, ‘Connections with leading thinkers: Rebecca Schindler’ (2015 accessed 10 Jan 2016) [https://www.accenture.com/t20151105T110549\\_\\_w\\_/us-en/\\_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub\\_2/Accenture-Institute-Conversations-Rebecca-Schindler.pdf](https://www.accenture.com/t20151105T110549__w_/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_2/Accenture-Institute-Conversations-Rebecca-Schindler.pdf)> This proposition is accepted by policy-makers the world around; and is a cornerstone of the Australian IOT Alliance (IOTAA) approach – that consumer “trust” is essential.

## Author declaration

This minor thesis is submitted to Bond University in final fulfilment of the requirements of the Degree of Doctor of Legal Science (Research). This thesis represents my own work towards this research degree and contains no material which has been previously submitted for any degree or diploma at this University or any other institution, except where due acknowledgment is made.



Signed by Kathleen Anne Mathews Hunt  
21 June 2017 & 25 September 2017

## Research outputs and publications during candidature<sup>2</sup>

### Peer-reviewed publications

Mathews-Hunt, Kate, 'Gaming the system: fake online reviews v. consumer law' *Computer Law & Security Review*, 31 (1) (February 2015): 3-25

Mathews-Hunt, Kate. 'CloudConsumer: contracts, codes and the law' *Computer Law & Security Review* 31 (2015) 450- 477.

Mathews-Hunt, Kate, 'CookieConsumer: tracking online behavioural advertising in Australia' *Computer Law & Security Review* 32 (2016) 55- 90.

### Conference presentation (invited)

Mathews-Hunt, Kate, Presentation to the Consumer Consultative Committee, Australian Competition and Consumer Commission (23 June 2017) Melbourne, Australia.

---

<sup>2</sup> These outputs are derived from one coursework subject and two independent studies undertaken during the SJD degree. Publication copyright permissions do not apply.

## Acknowledgement

My work on this minor thesis would not have been possible without the wonderful support of my family and my supervisors, as well as the perpetually redefining innovation of the global technical community and the relentless courage of consumers as embracers of new technology the world around.

Firstly, to my family, my eternal love, admiration and thanks. As always in my life, they have provided unending support, encouragement and interest, touched with some amusement at my midlife scholarly endeavours. I look forward to the next chapter of our ever-interesting lives together.

Secondly, my warm thanks and respect to my supervisors, Professor Dan Svantesson and Professor Brenda Marshall. Both are talented teachers and researchers and they have been encouraging and kind to me throughout. Many thanks also to the interviewees who so generously spoke with me. They include Travis Hall of the US Department of Commerce, which is presently crafting US IOT policy at a time of great challenge, and Adam Thierer of George Mason University, who so energetically prosecutes the case for 'permissionless innovation' and to whom I am indebted for his invaluable CIOT-related work and a rather long Sunday night (his time) interview. Thanks also to Scott Peppet for his seminal US work on the consumer IOT which inspired my interest in contributing to an Australian perspective, as well as Mark Büniger of Lux Research. It is critical to any debate that all sides have intelligent and spirited advocates, who proactively elevate the public policy and consumer law interest, which is what these people do. Other interesting interviewees include ACCC Deputy Chair, Delia Rickard, Andrew Maurer of the Department of Communications, Karl Sullivan of the Insurance Council of Australia, as well as vibrant discussions with Frank Zeichner of the newly-formed Australian IOT Alliance and Alex Vulkanovski of NBN Co.

Finally, thanks to the extraordinarily imaginative and visionary people all around the world who make the internet, in all its incarnations, truly the most inspiring, challenging and fascinating area to research imaginable. These people recreate our world every day. Researching the IOT is a wonderfully multi-disciplinary, mind-expanding experience from an academic, public policy and legal perspective. It's like taking a glimpse into the creative ingenuity of our species, shadowed by its many future challenges. My greatest hope is that Australian lawyers, public policy-makers and regulators might seek out that panoramic technological view a little earlier and see it more clearly, more often, in the interests of proactive (not reactive) consumer protection and much 'smarter' technology regulation, so that the law may become a more profound influence and protective enabler of the future of our society - and our planet.

## Table of contents

<b>Title page</b>	i
<b>Abstract &amp; keywords</b>	ii
<b>Author declaration</b>	iii
<b>Research outputs</b>	iv
<b>Acknowledgement</b>	v
<b>Contents</b>	vi
<b>Lists</b>	ix
Tables	ix
Graphics	ix
Interviews	xi
<b>Research question</b>	xii
<b>Abbreviations &amp; acronyms</b>	xiii
<b>Terminology clarification</b>	xiv
<b>PART I LOCATING THE STATUS QUO</b>	<b>1</b>
<b>Prologue</b>	1
<b>Introduction</b>	2
Thesis structure	9
<b>Chapter 1: Scoping an Australian consumer internet of things</b>	<b>11</b>
1.1 What's in a name: the consumer 'internet of things'	11
1.2 Scope, scale, stakes	20
1.3 Status: consumer uptake and adoption	48
1.4 Consumer trust: ending before it begins?	52
1.5 Conclusion	56
<b>PART II A NORMATIVE FRAMEWORK TO IDENTIFY KEY ISSUES</b>	<b>57</b>
<b>Chapter 2: Adapting a policy framework</b>	<b>57</b>
2.1 Research question	57
2.2 Scope and smart category justification	57
2.3 ACPF objectives	58
2.4 Adapting a consumer policy framework approach	60
2.5 Applying the adapted Framework	61
2.6 Conclusion	68
<b>PART III CONSUMER LAW 'GAP' ANALYSIS</b>	<b>69</b>
<b>Chapter 3 CIOT 'complexity': an overview of (in)security, big(ger) data analytics, &amp; (artificial) intelligence</b>	<b>69</b>
3.1 (In)security is complex... and pressing	70
3.2 Big CIOT data uses and (ab)uses	90
3.3 Conclusion	100
<b>Chapter 4 ACL &amp; CIOT: an overview</b>	<b>101</b>
4.1 An introduction	103
4.2 Parts 2-1 & 3-1: misleading conduct and false representations	108
4.3 Part 2-2 Unconscionable conduct & unfair trading	117
4.4 Part 2-3 Unfair contract terms	121
4.5 Consumer guarantees	130
4.6 Product liability & safety	137

4.7	Other ACL CIOT 'gaps'	154
4.8	Conclusion	156
<b>Chapter 5 Privacy law &amp; CIOT: an overview</b>		158
5.1	Australian privacy law: a (brief) overview	159
5.2	Gap analysis	161
5.3	Other consumer privacy 'gaps'	180
5.4	(Un)smart privacy cases	186
5.5	OAIC privacy enforcement performance	190
5.6	Conclusion	193
<b>Chapter 6 Contracting and <i>imperfectly</i> rational consumers @CIOT</b>		196
6.1	CIOT contracting A, B, Cs...	198
6.2	Reading, reading, reading... the contract	200
6.3	Rational consumers & certain choices	207
6.4	But I own my own data... don't I?	215
6.5	Consumer liability: a new era?	222
6.6	Recommendations	225
6.7	Conclusion	226
<b>PART IV PROPOSAL FOR ACTION</b>		227
<b>Chapter 7 Regulating CIOT: policy recommendation</b>		227
7.1	Steps 1 & 2: Revisiting Ch. 2 CIOT 'problems'	228
7.2	Step 4 Set policy objectives, etc.	230
7.3	Step 5: Evaluate options, etc.	232
7.4	Conclusion	238
<b>Chapter 8 Recommendations &amp; draft principles</b>		239
8.1	Intended application	239
8.2	Recommendations	240
8.3	Draft CIOT principles	251
<b>CONCLUSION</b>		258
<b>BIBLIOGRAPHY</b>		260
<b>Table of Cases</b>		385
<b>Table of Legislation</b>		391
<b>ANNEXURES</b>		
<b>Schedules</b>		394
<b>Sched. 1 ACL unfair terms review</b>		394
1.1	Smart home	394
1.2	Smart self	406
<b>Sched. 2 Privacy</b>		416
2.1	Australian privacy principles	416
2.2	Global CIOT privacy sweep: results summary	417
<b>Sched. 3 Australian software-related recalls</b>		418

3.1	Vehicle recalls: 2014- 2016	418
3.2	Smart self recalls: 1998- 2016	420
	<b>Annexures</b>	421
	<b>Annex. A Thesis scope</b>	421
A1	Research outline	421
	A1.1 Research questions	421
	A1.2 Research purpose	421
	A1.3 Content scope and exclusions	421
	A1.4 Disclaimer	422
A2	Methodology & research design	423
	A2.1 Background research	423
	A2.2 Framing method	425
	A2.3 Theoretical perspectives	426
	A2.4 Additional validation	427
	A2.5 Legal analysis	427
	A2.6 Impact assessment	427
	<b>Annex. B Background</b>	429
B1	Literature review	429
	B1.1. Australia	430
	B1.2 International materials	437
	B1.3 Case law	443
	Conclusion	444
B2	Key stakeholder ID	445
	B2.1 Key sectoral players	445
	B2.2 Key Australian IOT stakeholders	447
	<b>Annex. C Consumer policy diagrams</b>	452
C1	OECD consumer policy toolkit process	452
C2	Productivity Commission consumer policy flowchart	453
	<b>Annex. D OWASP &amp; OTA consumer guidance</b>	454
D1	Online Trust Alliance CIOT Consumer Checklist	454
D2	OTA IOT Trust Framework minimum requirements	455
D3	OWASP Consumer IOT Security Guidance	456
	<b>Annex. E Glossary</b>	458

## List of tables

Table (i)	Interviewee list	xi
Table 2.1	Consumer ‘problem’ identification	62
Table 2.2	Financial & non-financial detriments	65
Table 2.3	ACPF steps	68
Table 4.1	ACL defences applied to certain facts	148
Table 4.2	Summary chapter 4	156
Table 5.1	Summary chapter 5	194
Table 7.1	Consumer problem definition & source	229

### Schedules

Table S1.1	Smart home: potentially applicable device terms	394
Table S1.2	Smart home selected terms review	395
Table S1.3	Smart self: potentially applicable device terms	406
Table S1.4	Smart self selected terms review	407
Table S2.1	Australian privacy principles – a summary for APP entities	416
Table S2.2	Global consumer internet of things privacy sweep	417
Table S3.1	Australian vehicle recalls: software defects 2014- 2016	418
Table S3.2	Australian smart self product recalls: software 1998- 2016	420

### Annexures

Table B1.1	Australian inquiries 2015- 2017	433
Table B2.1	Key sectoral players	445
Table B2.2	Key IOT Stakeholders	447
Table E	Glossary	458

## List of graphics

Graphic P.1	Jawbone data	1
Graphic 1.1	(C)IOT creates a “new dimension”	22
Graphic 1.2	Simple IOT data flow	25
Graphic 1.3	Projected new adoption 2015- 2019+	31
Graphic 1.4	Consumer & business IOT units globally	32
Graphic 1.5	Connected car data flows	36
Graphic 1.6	Levels of autonomous vehicles	43
Graphic 1.7	UK consumer smart home device ownership by category	49
Graphic 2.1	Six-Step process for Consumer policy-making	60
Graphic 3.1	‘Some Americans retained a sense of humour’	82
Graphic 3.2	Connected Car Attack Surface	85
Graphic 3.3	Waymo functional prototype self-driving car (2016)	98
Graphic 4.1	Consumer recalls: Australia & UK comparison	140
Graphic 4.2	Florida traffic crash report	143
Graphic 4.3	Limitations warning	145
Graphic 4.4	Tesla Australian website	146
Graphic 4.5	Tesla vehicle dialog box	151
Graphic 4.6	Tesla improved crash rates MY2014- 2016	152
Graphic 5.1	Foundational principles for Privacy by Design	168
Graphic 5.2	IOT ‘Privacy by Design’ Decision Tree	170

Graphic 6.1	Milo Champions™ webpage	204
Graphic 6.2	Traffic light	212
Graphic 6.3	Privacy dashboard	212
Graphic 6.4	Consumer preparedness to share car data	220
Graphic 6.5	Consumers (95%) want smart car user data protected by legislation	221
Graphic 7.1	Alliance approach	238
Graphic 7.2	ACCC Compliance and Enforcement	237
<b>Schedules</b>		
Graphic S2.1	Australian privacy principles – a summary for APP entities	416
Graphic S2.2	International consumer internet of things privacy sweep	417
<b>Annexures</b>		
Graphic C1.1	Consumer policy making steps (OECD)	452
Graphic C1.2	Identifying and evaluating policy instruments (OECD)	453
Graphic D1.1	Enhancing the Security, Privacy & Safety of Connected Devices (OTA)	454
Graphic D2.1	OTA IOT Trust framework	455
Graphic D3.1	OWASP Consumer IOT Security Guidance	456

## List of interviews

To verify the discussion as to regulatory posture, to gain additional insights and to validate the conclusions of this thesis, the author conducted a series of unstructured interviews with CIOT-relevant regulators, industry stakeholder experts, consumer groups, and Australian and international academics active in CIOT regulation and law. The interviewees are derived from stakeholders identified during the literature review (**Annex. B1**) and key stakeholder processes (**Annex. B2**).

Additional interviews were conducted under Chatham House Rules.<sup>3</sup>

Person	Organisation
<b>Stuart Comer</b>	Editor & technical journalist, Australian Internet of Things website
<b>Mario Filopovic</b>	Toyota Australia C-ITS expert
<b>Claire T Gartland</b>	EPIC Consumer Protection Counsel (email)
<b>Travis Hall</b>	Telecommunications Policy Analyst, NTIA, US Department of Commerce
<b>Andrew Maurer</b>	Department of Communications and the Arts, Australia
<b>Karl Sullivan</b>	General Manager Policy Risk & Disaster, Insurance Council of Australia
<b>Scott Peppet</b>	Professor, University of Colorado School of Law, USA (email)
<b>Stewart Plain</b>	Productivity Commission, Australia
<b>Delia Rickard</b>	Australian Competition and Consumer Commission, Australia
<b>Jacob Suidgest</b>	Office of the Australian Information Commissioner (email)
<b>Adam Thierer</b>	Academic, George Mason University, Washington DC
<b>Alex Vulkanovski</b>	NBN Co. former ACCAN Google intern
<b>Lesley Yates</b>	Australian Aftermarket Automobile Association
<b>Frank Zeichner</b>	Australian IOT Alliance & Communications Alliance

Table (i): Non-Chatham House interviews conducted

<sup>3</sup> That rule states: "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

## Research question

This research is designed to address the following question:

**How can Australian regulators and policy makers best fulfil the objectives of the Australian Consumer Policy Framework to improve consumer wellbeing through empowerment and protection, cognisant of Australian consumer laws and privacy principles, while fostering the twenty-first century consumer internet of things, as exemplified by smart cars, home and self?**

These sub-questions<sup>4</sup> are considered throughout:

1. What is the nature, potential and significance of the consumer internet of things (CIOT) for Australian consumers? \*
2. How does the consumer internet of things respond to analysis using the Australian Consumer Policy Framework; including the question of 'consumer detriment', such as:
  - a. What consumer data may be generated by the CIOT, who owns it and do consumers provide informed consent as to its collection and use? If not, what are the legal implications of this in Australia?
  - b. Is the CIOT (and consumer data generated by it) secured in a manner which is private and safe, and if not, what are the legal implications of this in Australia?
  - c. Can consumers understand their rights in the interactive, autonomous consumer CIOT context, based upon traditional (internet) assumptions as to rational choice, market forces and self-autonomy, or is a new paradigm necessary?
3. Are Australian consumer protection laws adequate to protect consumers in an CIOT context, and if not, what (if any) are the appropriate regulatory and policy responses to that?
4. Are there any principles or guidelines which might guide a public policy and regulatory approach to the CIOT in Australia?

Research scope & limitations are detailed in **Annex. A**.

---

<sup>4</sup> The Australian Consumer Policy Protection Framework is described in Ch. 2.

## Abbreviations & acronyms<sup>5</sup>

<b>ACCC</b>	<b>Australian Competition and Consumer Commission</b>
<b>ACL</b>	Australian Consumer Law
<b>ACMA</b>	Australian Communications and Media Authority
<b>ACPF</b>	Australian Consumer Law Policy Framework
<b>ADMA</b>	Association for Data-driven Marketing and Advertising
<b>APC</b>	Australian Privacy Commissioner
<b>ASIC</b>	Australian Securities and Investments Commission
<b>Auto Alliance</b>	Alliance of Automotive Manufacturers (US based)
<b>CAANZ</b>	Consumer Affairs Australia and New Zealand
<b>CAF</b>	COAG Legislative and Governance Forum on Consumer Affairs
<b>CCA</b>	<i>Competition and Consumer Act 2010</i> (Cth) which includes the ACL
<b>CIOT or consumer IOT</b>	consumer internet of things
<b>C-ITS</b>	Intelligent transport system (automobile)
<b>COAG</b>	Council of Australian Governments
<b>EC</b>	European Commission
<b>EDPS</b>	European Data Protection Supervisor
<b>ENISA</b>	European Network and information Security Agency
<b>EU</b>	European Union
<b>FCC</b>	Federal Communications Commission (US)
<b>FTC</b>	Federal Trade Commission (US)
<b>GDPR</b>	General Data Protection Regulation (EU) Reg No 2016/679
<b>GSMA</b>	Group Special Mobile Association
<b>ICO</b>	Information Commissioner's Office (UK)
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IOE or IoE</b>	Internet of Everything, often synonymous with IOT
<b>IOT</b>	Internet of things, including the industrial and consumer versions.
<b>IOTAA</b>	Internet of Things Alliance Australia
<b>ISO</b>	International Organization for Standardization
<b>ITU</b>	International Telecommunications Union (UN)
<b>M2M</b>	Machine to machine (communications and contracting)
<b>NHTSC</b>	US National Highway Traffic Safety Administration (US)
<b>NIST</b>	National Institute of Standards and Technology (US)
<b>NSTAC</b>	National Security Telecommunications Advisory Committee (US)
<b>NTC</b>	National Transport Commission (Australia).
<b>NTIA</b>	National Telecommunication and Information Agency (US)
<b>OECD</b>	Organisation for Economic Co-operation and Development
<b>OAIC</b>	Office of the Australian Information Commissioner inclusive of the APC
<b>PA</b>	<i>Privacy Act 1988</i> (Cth)
<b>PBD</b>	privacy by design (Ch. 5)
<b>PI/ SI</b>	Personal information/ sensitive information defined in the Privacy Act 1988 (Cth)
<b>UN</b>	United Nations
<b>WP29</b>	Article 29 Data Protection Working Party (EU)

---

<sup>5</sup> For a glossary, see **Annex. E**.

## Terminology clarification

Terminology in the internet of things is evolving.

This thesis uses certain recognised terms, acronyms or initialisms,<sup>6</sup> but in the interests of consistency, is selective and avoid others. To clarify, uses are explained below.

Term	Other(s)	Rationale
CIOT; consumer IOT	consumer IoT	preference: it is more usual to use upper case in an initialism, and it aids reading flow (if mentally read as the acronym, 'cyot') Consumer IOT is becoming a recognised IOT sub-category, differentiated from industrial IOT.
IOT	IoT	preference: it is more usual to use upper case in an initialism
data	data (plural); datum (singular)	preference: <sup>7</sup> the broad use has entered the lexicon because 'datum' (like <i>agendum</i> ) is now rarely used. The Oxford English Dictionary describes it as a plural and 'mass noun', like 'information'. The Wall Street Journal, The Guardian and other respected newspapers use it in the latter sense. Hence, the more modern, consumer-friendly form is preferred.
device	thing object	preference: allows legal 'thinghood' to be separated from the overall elements which make it smart which go beyond the 'object' itself. It is also more reflective of consumer language.
'smart' [device]	'connected' [device]	The term 'smart' is used to prefix and distinguish consumer internet of things products, devices and related services which form part of the CIOT. The rationale is that 'smart' is already analogously in the lexicon (for example, 'smartphones') and is more consumer friendly, but reminds consumers that these products are both revolutionary and qualitatively different.

---

<sup>6</sup> 'Acronyms' are abbreviations usually pronounced as a word. 'Initialisms' are often fully-capitalised abbreviations pronounced letter by letter.

<sup>7</sup> See Simon Rogers, 'Data are or data is?' *The Guardian* (8 July 2012 accessed 10 Feb 2017) <<https://www.theguardian.com/news/datablog/2010/jul/16/data-plural-singular>> The author apologises in advance to those who dislike this non-traditional usage.

## Part I LOCATING THE STATUS QUO

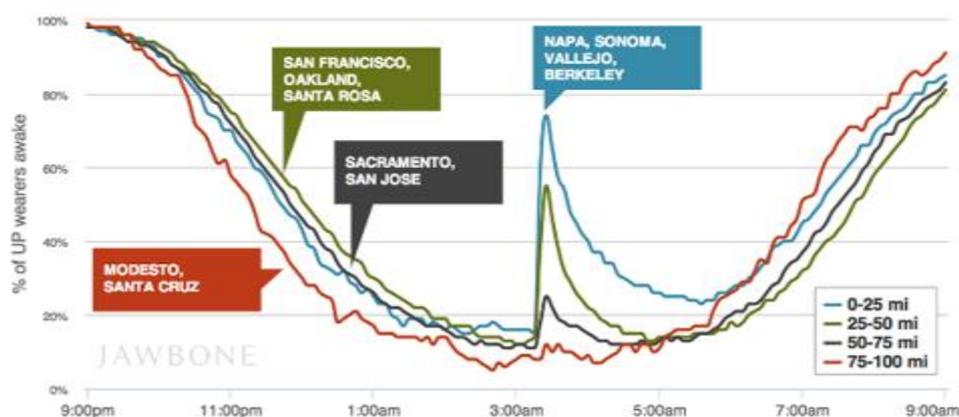
### Prologue

Seismic events happen, sometimes at the darkest hour, when people are unprepared.

Suddenly, people stir, and awaken... heavy heads lift from pillows, and sleepy eyes widen in awareness. Adrenalin surges. Heart rates lift. Pulses accelerate. And people move. So too, the bursting pulse of information surging from early morning Californian wrists to Aliphcom's massive always-on data centre. As an information-laden spike shot unusually, alarmingly north in the early hours, the corporation detected a suddenly wakeful population— and through simple analysis, could discern the very moment a magnitude 6.0 earthquake struck - at 3.20am. In the few following hours until dawn, the company also came to calculate the earthquake's epicenter to within a 15-mile radius, as biometric and geolocation data amassed, recording exactly how long each alert or anxious or possibly annoyed, data-generating person took, to finally, slip back to sleep.

Aliphcom make Jawbone; one of the world's most popular consumer smart fitness devices. The pulse of data they received that earthquake-night, enabled them to see, with insight, into the wee hours lives of their customers - and to know, precisely who woke up at that shaky moment, how each reacted physiologically, and where those reacting people lived – and if they chose, to speculate analytically upon the intimate personal traits revealed by the fact that only they came to know: that almost half of their customers within the epicentre, never went back to sleep at all.

Consumers 'wearing' the internet of things.



Graphic P.1 Jawbone data; Source: Jawbone Blog & The Economist<sup>8</sup>

<sup>8</sup> Eugene Mandel, 'How the Napa Earthquake affected Bay Area sleepers', *The Jawbone Blog* (25 Aug 2014 accessed 5 Jan 2016) <<https://jawbone.com/blog/napa-earthquake-effect-on-sleep/>> The earthquake struck Northern California on 24 August 2014.

## Introduction

On the cusp of the twenty-first century, Neil Gross imagined a poetically predictive analogy for the innately disruptive, technological organism known as the *Internet of Things* (IOT):

*In the next century, planet earth will don an electronic skin. It will use the Internet as a scaffold to support and transmit its sensations...stitched together [by] millions of embedded electronic measuring devices: thermostats... cameras, microphones.... These will probe and monitor ... our conversations, our bodies – even our dreams...<sup>9</sup>*

By 2016, the ‘smart’ world of IOT disruption is here.<sup>10</sup> No longer “science fiction”<sup>11</sup> or “scientific concept”,<sup>12</sup> it is “happening now”,<sup>13</sup> a revolutionary<sup>14</sup> “transformational shift”<sup>15</sup> which is “inevitable and inescapable”,<sup>16</sup> “on the rise”<sup>17</sup> and “here to stay”.<sup>18</sup> Dubbed the “second digital revolution”<sup>19</sup> or the “third”,<sup>20</sup> or “fourth”,<sup>21</sup>

---

<sup>9</sup> Neil Gross, ‘21 Ideas for the twentieth-first century’ *Businessweek Online* (30 Aug 1999 accessed 16 Mar 2016) <[http://www.businessweek.com/1999/99\\_35/b3644024.htm](http://www.businessweek.com/1999/99_35/b3644024.htm)>

<sup>10</sup> Karen Rose, Scott Eldrige, Lyman Chapin, ‘The Internet of Things: An Overview Understanding the issues and challenges of a more connected World’ *The Internet Society* (Oct 2015 accessed 18 Mar 2016): 3 <[https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014\\_0.pdf](https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf)>

<sup>11</sup> MSV Janakiram, ‘5 Companies that will Dominate Consumer IoT Market- Parts 1 and 2’ *Forbes* (26 May 2015 accessed 3 Apr 2016) <<http://www.forbes.com/sites/janakirammsv/2015/05/26/5-companies-that-will-dominate-consumer-iot-market-part-2/#6d22440c1930>>

<sup>12</sup> Ivan, ‘Things You Need to Know about Internet of Things’ *The Cloud Infographic* (7 Jan 2016) <<http://www.thecloudinfographic.com/2016/01/07/things-you-need-to-know-about-internet-of-things.html>>

<sup>13</sup> Cisco, ‘Embracing the Internet of Everything to Capture your Share of \$14.4 trillion’ *White Paper* (2013 accessed 11 Apr 2016): 2 <[http://www.cisco.com/c/dam/en\\_us/about/ac79/docs/innov/IoE\\_Economy.pdf](http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf)>; Rose, above n 10: 3.

<sup>14</sup> Charles Arthur, ‘The “things” are smart and will work for us’ in *Raconteur, ‘Internet of Things’ The Times* (30 Mar 2016 accessed 30 Mar 2016): 3 <<http://raconteur.net/internet-of-things>>

<sup>15</sup> Daniel Burris, a technology futurist, uses this term: Daniel Burris, ‘The Internet of Things is far bigger than anyone realises (Part 2)’ *WIRED* (Nov 2014 accessed 1 April 2016) <http://www.wired.com/insights/2014/11/iot-bigger-than-anyone-realizes-part-2/>. “Transformational is an overused word, but I do believe it properly applies to these technologies...”: David Petraeus, ‘Excerpts from Remarks Delivered by Director David H. Petraeus at the In-Q-Tel CEO Summit’ (1 Mar 2012 accessed 1 Apr 2016) <<https://www.cia.gov/news-information/speeches-testimony/2012-speeches-testimony/in-q-tel-summit-remarks.html>>

<sup>16</sup> Joel Lee, ‘What Is the Internet of Things & How Will It Affect Our Future [MakeUseOf Explains]’ (28 Jun 2013 accessed 18 Mar 2016) <<http://www.makeuseof.com/tag/what-is-the-internet-of-things-and-how-will-it-affect-our-future-makeuseof-explains/>>

<sup>17</sup> EC, ‘IoT Privacy and Security Workshop’ *AIOA* (13 Jan 2017 accessed 20 Feb 2016) <[https://europa.eu/newsroom/events/internet-things-%E2%80%93-privacy-and-security-workshop\\_en](https://europa.eu/newsroom/events/internet-things-%E2%80%93-privacy-and-security-workshop_en)>, and Report (10 Apr 2017 accessed 15 Apr 2017):1 <<https://ec.europa.eu/digital-single-market/en/news/internet-things-privacy-security-workshops-report>>

<sup>18</sup> International Conference of Data Protection and Privacy Commissioners, ‘Mauritius Declaration on the Internet of Things’ (14 Oct 2014 accessed 12 Apr 2015): 1 <<http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf>>; See also IDC & TXT, ‘Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination’ *European Commission* (13 May 2015 accessed 10 Feb 2016): 9 <<https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination>>

<sup>19</sup> (UK) Government Office for Science, ‘The Internet of Things: making the most of the Second Digital Revolution’ (18 Dec 2014 accessed 20 Apr 2016) <<https://www.gov.uk/government/publications/internet-of-things-blackett-review>> (Blackett Review)

<sup>20</sup> Theodore Forbath, ‘The third wave of computing’ *Forbes* (3 Oct 2015 accessed 25 Apr 2016) <<http://fortune.com/2013/13/1003/the-third-wave-of-computing/>>

<sup>21</sup> IDC, ‘The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things’ *EMC Digital Universe* (April 2014 accessed 29 Apr 2016) <<http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm>>

and fueled by “hype”,<sup>22</sup> Moore’s and several other ‘laws’,<sup>23</sup> and industry money, it expands the digital universe exponentially – into human life itself.<sup>24</sup> It is Gross’ big idea of a global connective electronic network, organically and systemically recording, processing, regulating and controlling almost infinite amounts of sensory and experiential data. Across the globe, billions of embedded IOT devices will metaphorically recreate the sensory capabilities of that skin, with an almost infinite capacity to probe, gauge, monitor, control, record and analyse a myriad of detectable, measurable, human ‘sensations’. An IOT world is one in which every physical, geographic and personal interaction or experience is translatable into data, and every conceivable human sensation is monitored, recorded, trackable, analysable, ‘advertise-able’ – and monetizable. For consumers, it is one in which the possibility of an intimately personal and digitally-noiseless moment – an unpredicted thought - becomes almost unimaginable.<sup>25</sup> But while the greater vision has Benthamite utopian potential, it is also potentially Orwellian<sup>26</sup> - spanning benign utilitarian oversight, to the dystopian extremity of institutionalized global surveillance. Such potential encapsulates the public policy and legal dilemma that is the consumer internet of things: how to appropriately control and human-centre a metastasizing technological organism, which by promise and threat, is a globally- ‘disruptive innovation’.<sup>27</sup>

---

<sup>22</sup> The term is often used; see for example: James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon, ‘The Internet of Things: Mapping the Value Beyond the Hype’ *McKinsey & Co* (June 2015 accessed 26 Nov 2015) <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>. Gartner graphs IOT at the “peak of overinflated expectations” in 2015: i.e., a “phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the technology is pushed to its limits. The only enterprises making money are conference organizers and magazine publishers”: Alfonso Velosa, W. Roy Schulte and Benoit J. L’Heureux, ‘Hype Cycle for the Internet of Things, 2015’ *Gartner* (21 Jul 2015 accessed 6 Mar 2016) < <https://www.gartner.com/doc/reprints?id=1-2M904VI&ct=150901&st=sb>>

<sup>23</sup> These are “rough empirical description”, not an immutable physical or scientific law. Moore’s Law came from Gordon Moore of Intel who observed that overall computer processing power doubles every two years or so. Metcalfe’s Law suggests that communications network value is proportional to user numbers, squared, but is criticised: Bob Briscoe, Andrew Odlyzko and Benjamin Tilly, ‘Metcalfe’s Law is Wrong’, *IEEE Spectrum* (1 Jul 2016 accessed 4 Feb 2016) <<http://spectrum.ieee.org/computing/networks/metcalfes-law-is-wrong>>

<sup>24</sup> Accenture Digital, ‘The Era of Living Services’ (2016 accessed 23 Mar 2016): 5 <<https://www.accenture.com/us-en/insight-living-services-from-accenture-digital.aspx>>

<sup>25</sup> This sounds hyperbolic; but the intrusion extends daily. For example, “connected sex tech” exists, including “pleasure chips”, “VR teledildonics” & “haptic deviants”. The smart condom detects “thrust velocity and pace, how many calories you’ve burned, skin temperature and girth”, position numbers adopted and sex frequency. App users upload data to share statistics with friends or the public: Conor Alison, This smart condom ring will track your sexual activity’ *WAREABLE* (3 March 2017 accessed 7 Mar 2017) <https://www.wearable.com/wearable-tech/smart-condom-sex-activity-tracker-4012> See also non-therapeutic ‘smart’ toilet analysis, menstrual cups, fertility monitors and so on.

<sup>26</sup> Lux Research, ‘The Internet of Everyone: Consumer Relationships in the Age of IoT’ (2015 accessed 15 May 2016). Bentham’s panopticon prison design enabled 360-degree surveillance to motivate prisoners to always do their best. The Orwell reference invokes the police state and human oppression critiqued in his sci-fi classic, ‘1984’.

<sup>27</sup> Clayton M. Christenson, *The Innovator’s Dilemma: The Revolutionary Book that will Change the Way You Do Business* (Collins Business Essentials) 2003. ‘Disruptive innovation’ means (simply) an innovation which helps to create new markets and value networks, but eventually disrupts the existing market and displaces the existing technology. The US National Intelligence Council lists IOT as one of six “Disruptive Civil Technologies” with prospective influences on US national power: Clinton Fernandes & Vijay Sivaraman, ‘It’s only the beginning: Metadata Retention laws and the Internet of Things’ *Australian Journal of Telecommunications and the Digital Economy*, 3(3) (2015)

Australian consumers are poised to live in 'smart' homes, monitor 'smart' selves and ride in ever - *smarter* cars. By 2020, analysts predict that globally, there will be 30 billion smart devices and one in five cars will be 'smart', with a global economic impact "up to" eleven trillion US dollars.<sup>28</sup> While Australia's CIOT market is small,<sup>29</sup> analysts claim that over 3.5 million Australians (14%) wear smart self devices today,<sup>30</sup> and predict that smart home spending will rise 66% to a projected \$383 million across 2015- 2016.<sup>31</sup> The growing consumer IOT market features a myriad of *smart self* 'wearables'<sup>32</sup> - fitness bands, jewellery, glasses, clothing and even "sex-tech"<sup>33</sup> - while *smart home*<sup>34</sup> devices are (slowly) appearing in-store, connecting smart TVs, whitegoods, security, thermostats, dog-feeders, baby monitors (etc.), and increasingly smart(er) cars<sup>35</sup> are connecting via GPS, C-ITS and telematics systems,<sup>36</sup> on road and in every showroom. Soon, more Australians will work in *smart buildings*, ride in *smart transport* directed by smart traffic management systems, through *smart cities*, and ride in smartly self-driving cars. And the rapidly evolving global market promises a myriad of other smart devices; driven by the world's largest

---

<<http://telsoc.org/ajtde/index.php/ajtde/article/view/21>> In 2017, the EC state: "the IoT is transforming and disrupting our daily lives faster than any other technology before": EC, above n 17.

<sup>28</sup> McKinsey & Co., 'The Internet of Things: Sizing up the Opportunity' (2014 accessed 2 Feb 2016)

<[http://www.mckinsey.com/insights/high\\_tech\\_telecoms\\_internet/the\\_internet\\_of\\_things\\_sizing\\_up\\_the\\_opportunity](http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_sizing_up_the_opportunity)>;

McKinsey & Co, 'The road to 2020 and beyond: What's driving the global automotive industry?'(2013 accessed 2 Feb 2016)

<[http://www.mckinsey.com/~media/mckinsey/dotcom/client\\_service/automotive%20and%20assembly/pdfs/mck\\_the\\_road\\_to\\_2020\\_and\\_beyond.ashx](http://www.mckinsey.com/~media/mckinsey/dotcom/client_service/automotive%20and%20assembly/pdfs/mck_the_road_to_2020_and_beyond.ashx)>; McKinsey & Co, 'Unlocking the Potential of the Internet of Things' (2015 accessed 2 Feb 2016) <[http://www.mckinsey.com/insights/business\\_technology/the\\_internet\\_of\\_things\\_the\\_value\\_of\\_digitizing\\_the\\_physical\\_world](http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world)>

<sup>29</sup> See Chapter 1 as to publicly-available Australian data. Some paid research exists but is inaccessible for cost reasons.

<sup>30</sup> Telsyte, 'Australian Smartphone & Wearable Devices Market Study 2016-2020' (6 Sept 2016 accessed 20 Sept 2016) <<https://www.telsyte.com.au/announcements/2016/9/6/smartwatch-market-gathering-steam-as-australians-turn-to-wearable-gadgets-amid-flat-smartphone-sales>>

<sup>31</sup> Telsyte, 'Australian IOT@ Home market to reach \$3.2 Billion by 2019 embedding smart technology into Everyday Life' (10 Aug 2015 accessed 22 Apr 2016) <<http://www.telsyte.com.au/announcements/2015/8/10/australian-iot-home-market-to-reach-32-billion-by-2019-embedding-smart-technology-into-everyday-life-1>>

<sup>32</sup> 'Smart Self' refers to devices attached to or implanted inside the human body – examples include devices which monitor human health and wellness, promote fitness, improve productivity and improve disease management and identification: McKinsey, above n 28: 3.

<sup>33</sup> Gareth May, 'The future of sex tech: Pleasure chips, VR teledildonics & haptic deviants' *WAREABLES* (30 Nov 2016 accessed 16 Jan 2017) <<https://www.wearable.com/wearable-tech/future-sex-tech-888>>

<sup>34</sup> A "smart home" is one "...fitted or equipped with a range of interconnected sensors to read external elements such as light, temperature, motion, moisture of systems such as heating, lighting, security; and of devices such as media devices and appliances, which can be automated, monitored and controlled through a computer or smart phone, including from outside the home, or via the Internet:: ENISA, 'Threat Landscape for Smart Home and Media Convergence' (9 Feb 2015 accessed 2 Nov 2015): 5 <<https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence>>

<sup>35</sup> 'Smart cars' is used here to collectively include automated, autonomous, self-driving and driverless vehicles. These entail a spectrum with increasing degrees of connectivity and autonomy. 'Connected' usually refers to C-ITS systems (traffic management and V2V communications) whereas 'autonomous' refers to on-board driving systems: EU, 'Research for TRAN Committee – Self-piloted cars: the future of road transport' (2016 accessed 2 Jul 2016): 19 <<http://www.europarl.europa.eu/supporting-analyses>>

<sup>36</sup> P. Lawson, 'The Connected Car: Who is in the Driver's Seat?' FIPA (2015 accessed Aug 2016) <<https://fipa.bc.ca/connected-car-download/>>

IT,<sup>37</sup> tech,<sup>38</sup> cloud,<sup>39</sup> manufacturing entities,<sup>40</sup> and the burgeoning data analytics industry<sup>41</sup> - right through to tiny crowd-funded, start-ups sustained by a smart idea, and a buy-out dream.<sup>42</sup> With powerful drivers, industry convergence<sup>43</sup> and international government support, CIOT will inevitably and irrevocably affect consumers, right around the globe. But the consumer protection implications of this smart technology may not legally, be so 'smart' right now,<sup>44</sup> much less into the future. Australian consumers and regulators are unprepared, and at 2016 end, seem unaware of the scope, scale and stakes<sup>45</sup> of a looming consumer IOT, much less envisaging regulatory responsiveness to diverse risks impacting consumer rights, privacy,<sup>46</sup> safety, data security, autonomy and "sovereignty".<sup>47</sup> While US authorities report that CIOT legal problems are "different in important aspects",<sup>48</sup> the EU finds many "novel liability aspects"<sup>49</sup> and

---

<sup>37</sup> E.g. Google, Amazon and Apple.

<sup>38</sup> E.g. IBM, Cisco and Intel.

<sup>39</sup> E.g. AT&T, GE, Microsoft and Oracle.

<sup>40</sup> E.g. Ford, Samsung, Bosch, Hitachi, GE and IBM. See IDG UK, '15 Most Powerful Internet of Things Companies 2016' *Computerworld UK* (16 Dec 2015 accessed 10 Mar 2016) <http://www.computerworlduk.com/galleries/data/12-most-powerful-internet-of-things-companies-3521713/#7>; Jacob Morgan, 'Which Companies Dominate the "Internet of Things?"' *CloudAve* (16 Jul 2014 accessed 2 Jan 2016) <<https://www.cloudave.com/35202/companies-dominate-internet-things/>>

<sup>41</sup> Executive Office of the President (EOP), 'Big Data: Seizing Opportunities, Preserving Values' Interim progress report (May 2014 accessed 10 May 2016) <

[https://www.whitehouse.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_may\\_1\\_2014.pdf](https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf)>; EOP, 'Big Data: a Report on Algorithmic Systems, Opportunity, and Civil Rights' (May 2016 accessed 10 May 2016)

<[https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016\\_0504\\_data\\_discrimination.pdf](https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf)>

<sup>42</sup> E.g. (Alphabet) Google bought out Nest, then later bought out Revolv home hub. Samsung brought out Smart things, which is now its principle smart home vehicle.

<sup>43</sup> GE CEO Jeff Immelt stated that GE would soon have to change its production and business model: "Every industrial company, will be a software company": Malcolm Turnbull, 'Opening Address to AIIA Summit: Navigating the Internet of Things' (26 Mar 2015 accessed 11 May 2016)

<[http://www.minister.communications.gov.au/malcolm\\_turnbull/speeches/internet\\_of\\_things\\_summit](http://www.minister.communications.gov.au/malcolm_turnbull/speeches/internet_of_things_summit)>

<sup>44</sup> Consumers International, 'Connection and Protection in the Digital Age: the Internet of things and challenges for consumer protection' (11 Apr 2016 accessed 18 Apr 2016)

<<http://www.consumersinternational.org/media/1657273/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf>> For a graphic depiction of the 'household name' corporations which have "lost" data, see: Information is Beautiful, 'World's Biggest Data Breaches: selected losses greater than 30,000 records' (updated 30th Mar 2015 accessed 2 Apr 2016) <<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>>

<sup>45</sup> Ch. 1 evidences this contention (largely) relying upon international studies.

<sup>46</sup> Boston Consulting Group, 'The Value of our Digital Identity' (Nov 2012 accessed 2 Feb 2016)

<[https://www.bcgperspectives.com/content/articles/digital\\_economy\\_consumer\\_insight\\_value\\_of\\_our\\_digital\\_identity/](https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/)>; Accenture, above n 24. Acquity Group, 'The Internet of Things: The Future of Consumer Adoption' (2014 accessed 3 Mar 2016) <<http://quantifiedself.com/docs/acquitygroup-2014.pdf>>

<sup>47</sup> Erik Laykin, Duff & Phelps digital forensics specialist cited in Rob Lever, 'Secrets from smart devices find path to US legal system' *PhysORG* (19 Mar 2017 accessed 15 April 2017) <https://phys.org/news/2017-03-secrets-smart-devices-path-legal.html> Note that this concept has multiple meanings depending upon one's philosophical bent:

<sup>48</sup> National Telecommunications and Information Commission (NTIA), 'Green Paper: Fostering the Advancement of the Internet of Things' (12 Jan 2017 accessed 15 Jan 2017): 3 <<https://www.ntia.doc.gov/other-publication/2017/green-paper-fostering-advancement-internet-things>>

<sup>49</sup> EU, Article 29 Data Protection Working Party, 'Opinion 8/2014 on Recent Developments on the Internet of Things' (16 Sept 2014 accessed 16 Mar 2016): 21 [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf); EC, 'Internet of Things Privacy & Security Workshop's Report' (10 Apr 2017 accessed 15 Apr 2017) <<https://ec.europa.eu/digital-single-market/en/news/internet-things-privacy-security-workshops-report>> c/f an early 2015 AIOA Report "...the rapid development of IoT technology may raise certain product compliance, product liability and insurance-related issues in the future. At present, we believe that these issues can be managed within the existing legal and regulatory framework. We propose that the emphasis should, in the main, be on the development of

Consumers International warn of both exacerbated and new legal contexts,<sup>50</sup> recent Australian enquiries largely ignore serious consumer-relevant CIOT challenges. This thesis snapshots the CIOT ecosystem and Australian consumer protection laws in 2016 and evidences international concerns, but within an Australian context. Absent pressing policy formulation informed by a national debate, consumer and privacy protections may struggle. That difficulty amplifies within the CIOT ecosystem: as traditional models of the rational consumer<sup>51</sup> and self-correcting systems<sup>52</sup> such as notice and choice-based consent<sup>53</sup> dismantle, freemium devices or apps disguise unconscious rights-sacrificial behaviours;<sup>54</sup> unfair contractual terms legitimise data (ab)use<sup>55</sup> and rights transfer; big data analytics and algorithms systematise consumer profiling, manipulation and discrimination; and artificial intelligence launches its predicted “unprecedented attack”.<sup>56</sup> But these fraught social and legal potentials seem abstractions when, at present, most consumer IOT devices seem over-hyped IT-hybrids, bearing hefty price tags, fancy packaging and (questionable)<sup>57</sup> consumer convenience, service and utility. What is less apparent in these ‘pretty products’, are systemic potentials for personal, cyber and financial consumer risk,<sup>58</sup> dire national security implications,<sup>59</sup> and an exponentially large and latent, surveillance-based, privacy intrusive, data-fuelled, backend value chain. Indeed, few consumers perceive ethicists’ and futurists’ warnings of data mining without duty, autonomy without control, surveillance without sanction, superintelligence without

---

policy solutions to these potential challenges”: AIOTA, ‘Report AIOTI Working Group 4 – Policy’ (15 Oct 2015 accessed 3 Mar 2016) <<https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf>>

<sup>50</sup> CI, above n 44.

<sup>51</sup> Charles Oren Bar-Gill, ‘Seduction by Contract: Law, Economics, and Psychology in Consumer Markets’, 2012 DOI:10.1093/acprof:oso/9780199663361.001.0001

<<http://www.oxfordscholarship.com.ezproxy.bond.edu.au/view/10.1093/acprof:oso/9780199663361.001.0001/acprof-9780199663361>>; M. W. Bailey, ‘Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things’ *Texas Law Review* (Apr 2016) 94(5): 1023-1054.

<sup>52</sup> European Commission (EC), ‘Europe’s policy options for a dynamic and trustworthy development of the IOT’ *Rand Corporation, SMART 2012/ 0053* (31 Dec 2012 accessed 12 Jul 2016)

<[http://www.rand.org/pubs/research\\_reports/RR356.html](http://www.rand.org/pubs/research_reports/RR356.html)>

<sup>53</sup> Chris Hoofnagle, Chris & Jennifer M Urban, ‘Alan Westin’s Privacy Homo Economicus’ (1 Jun 2014 accessed 5 Apr 2016) 49 *Wake Forest L. Rev.* 261 <<http://scholarship.law.berkeley.edu/facpubs/2395>>

<sup>54</sup> Bailey, above n 51: 1024

<sup>55</sup> Chris Hoofnagle and Jan Whittington, ‘Free: Accounting for the Costs of the Internet’s Most Popular Price’ (2013-2014) 61 *UCLA L. Rev.* 606 <<http://www.uclalawreview.org/pdf/61-3-2.pdf>>; Bailey, above n 51.

<sup>56</sup> James Barratt, ‘Why Stephen Hawking and Bill Gates Are Terrified of Artificial Intelligence’ *Huffington Post* (9 Sept 2015 accessed 25 May 2016) <[http://www.huffingtonpost.com/james-barratt/hawking-gates-artificial-intelligence\\_b\\_7008706.html](http://www.huffingtonpost.com/james-barratt/hawking-gates-artificial-intelligence_b_7008706.html)>

<sup>57</sup> As to smart self fatigue, see Aaron Pressman, ‘Why you probably won’t be getting a Fitbit this Christmas’ *Fortune.Com* (4 Nov 2016 accessed 4 Nov 2016) <<http://fortune.com/2016/11/04/probably-wont-fitbit-this-christmas/>>; Mike Feibus, ‘Face It, You’re Bored of the Smartwatch You Got last Christmas’ *Fortune* (10 Apr 2016 accessed 11 Apr 2016) <<http://fortune.com/2016/04/10/wearables-smartwatch/>>

<sup>58</sup> Health device and smart car hacks pose consumer danger: FTC, ‘Comments of the Staff of the FTC’s Bureau of Consumer Protection and Office of Policy Planning, ‘In the Matter of the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things’ *Docket No. 160331306-6306-01* (2 June 2016) 5- 6 <[https://www.ftc.gov/system/files/documents/advocacy\\_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf](https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf)>

<sup>59</sup> Widespread IOT hacking is a threat - from national infrastructure attacks, to smart (self driving) car(s) used as terrorist Trojan horses.

safeguard ... and even, the potential destruction of humanity.<sup>60</sup> It sounds over-dramatic, and that (final) end game aside, it is incontrovertible now that the CIOT offers transformational societal and individual benefits<sup>61</sup> if properly understood, enabled and controlled commensurate with social expectation and consumer-protective standards. But at this moment, it is difficult not to perceive a complex industry in hyperbolic money-making overdrive, threatening to run amok.

By 2016 end, the Australian government has no official IOT strategy, nor is it proactively developing one.<sup>62</sup> In 2015, the Prime Minister romantically proclaimed that IOT limitations lie solely within Australia's "imagination and vision", and that in its regulation, "less is better".<sup>63</sup> Contemporaneously, the US *National Security Advisory Committee* officially warned President Obama that the traditional pacing "gap"<sup>64</sup> between technological advance and effective policy development and governance - the *Collingridge* dilemma<sup>65</sup> - was turning into a "chasm".<sup>66</sup> NSTAC named 2019 as the tipping point for government IOT influence, warning that thereafter, regulatory policy could only effect "change at the margins".<sup>67</sup> But while European regulators are leading funding,<sup>68</sup> research,<sup>69</sup> and innovating privacy protection,<sup>70</sup> and American regulators are rushing to catch up,<sup>71</sup> the Australian government appears sanguine or at best, inactive.

---

<sup>60</sup> Giovanni Buttarelli, 'Ethics at the Root of Privacy and as the Future of Data Protection' *Presentation at Harvard & MIT* (19 April 2016 accessed 4 Sept 2016) <<https://secure.edps.europa.eu/edpsweb/Edps/Cache/Offonce/Edps/Ethics>>

<sup>61</sup> Examples are numerous: the capacity to better monitor and respond to health issues; improved energy management and use; efficient lower emissions transport – and so on. The industrial IOT promises infrastructure monitoring, vastly improved manufacturing efficiencies and so on.

<sup>62</sup> Communications Minister Mitch Fifield has attended Australian IOT Alliance (IOTAA) functions, the Communications Department, ACCC and OAIC attend IOTAA workstreams as observers. But the author finds little government lead or research investment.

<sup>63</sup> Angus Kidman, 'Malcolm Turnbull: The Internet Of Things relies on imagination, not regulation' *Lifehacker* (26 Mar 2015 accessed 11 May 2016) <<http://www.lifehacker.com.au/2015/03/malcolm-turnbull-the-internet-of-things-relies-on-imagination-not-regulation/>> He has put this view for some years: Turnbull, above n 43.

<sup>64</sup> The "pacing problem" or "gap" is identified in Gary E Merchant, Braden R Allenby and Joseph R Heckert (eds), *The Growing Gap between Emerging Technologies and Legal-Ethical oversight: The pacing problem* (Springer, 2011).

<sup>65</sup> Collingridge wrote: "When change is easy, the need for it cannot be foreseen; when the need for change is apparent, change has become expensive, difficult and time consuming.": David Collingridge, *The Social Control of Technology* (Pinter, 1980).

<sup>66</sup> National Security Telecommunications Advisory Committee (NSTAC), 'NSTAC Report to the President on the Internet of Things' (19 Nov 2014 accessed 7 Apr 2016) <<https://www.dhs.gov/publication/2014-nstac-publications>>

<sup>67</sup> *Ibid.* They referenced areas such as adoption, device design and technical use protocols.

<sup>68</sup> Funding includes €192 million from 2014 to 2017: European Commission, 'Digital Single Market, Research and Innovation' (9 Jun 2016 accessed 2 Mar 2017) <<https://ec.europa.eu/digital-single-market/en/research-innovation-iot>>

<sup>69</sup> The EU first recognised the need to address IOT regulatory issues by 2006, via its workshop 'From RFID to the Internet of Things' cited in Rolf H. Weber, 'Internet of things - Need for a new legal environment?' (2009 accessed 2 Jan 2016) 25:1 *Computer Law & Security Review* 522- 527: 523. Since that time the EU has led international policy and technical research – e.g. Commission Staff Working Document, 'Future Networks and the Internet- Early Challenges regarding the Internet of things' (2010) <[http://ec.europa.eu/information\\_society/eeurope/i2010/docs/future\\_internet/swp\\_internet\\_things.pdf](http://ec.europa.eu/information_society/eeurope/i2010/docs/future_internet/swp_internet_things.pdf)>

<sup>70</sup> EU General Data Protection Regulation (GDPR) 2016/679 (27 Apr 2016)

<sup>71</sup> US public policy work accelerated in 2015-6, with the FTC's enquiry and Congressional/ House hearings: see Mohana Ravindranath, 'Who's in charge of regulating the internet of things?' *Nextgov* (1 Sept 2016 accessed 16 Oct 2016) <http://www.nextgov.com/emerging-tech/2016/09/internet-things-regulating-charge/131208/>. In early 2017, the NTIA Green Paper is instigating national policy development: above n 48.

Aside from recent attack-driven attention to public cybersecurity and an industry-led push for public sector open data, there is no government-led IOT planning or focus. It is a policy 'gap' which industry has rushed to fill in the past twelve months through the Australian IOT Alliance – but unfunded volunteerism, even from specialist sectoral groups<sup>72</sup> - is no substitute for formal government-led democratic policy development processes and Australia remains well behind international approaches. Arguably, from a regulatory and policy perspective, the federal government is either unaware, or has assumed an ideologically-founded, non-interventionist posture, eschewing IOT strategy,<sup>73</sup> ignoring IOT risks<sup>74</sup> and presumably, assuming without justification, that Australian tech-neutral consumer laws are adequate to meet an undefined challenge. This thesis examines that assumption, identifies aspects of the challenge and seeks to evidence otherwise.

As one of few legal studies of the consumer internet of things in Australia, this work fills a gap in scholarly literature by analysing the Australian legal literature, selectively synthesising voluminous overseas materials, and applying the normative values of the Australian Consumer Law Policy Framework (Framework) to the important question of whether the CIOT evidences problems which warrant regulatory action, based upon the smart car, home and self contexts. In responding to this question, this thesis makes three assertions; each is fresh to Australian legal literature, timely in its contribution to a socio-legal debate growing in urgency, and important to future consumer law and policy making in this country:

- firstly, Australian consumers and regulators do not understand the adverse implications of this new panopticon technology<sup>75</sup> which surveys almost *everything* and blurs traditional understandings of human autonomy and privacy, nor do consumers understand the adverse implications of CIOT through its related intertwined technologies. As Australia is on the cusp of widespread adoption, time for an informed debate in Australia is pressing;
- secondly, Australian consumer and privacy law is inadequate to comprehensively address CIOT consumer detriments; and

---

<sup>72</sup> The IOTAA formed in May 2015 under Communications Alliance auspices. It became a separate not-for-profit entity in July 2016, and describes itself as “the primary IoT industry body in Australia with members being drawn from a wide cross-section of IoT service providers, vendors, consultants and suppliers as well as business, universities and consumer groups”: <<http://www.iot.org.au/>>

<sup>73</sup> Communications Alliance, ‘Internet of Things Think-Tank Highlights Need for National Strategy’ (May 2015 accessed 5 Mar 2016) <<http://www.commsalliance.com.au/about-us/newsroom/Internet-of-Things-Think-Tank-Highlights-Need-for-National-Strategy>>

<sup>74</sup> The 2016 Cybersecurity Strategy barely mentioned the IOT: *ComputerWorld ANZ*, ‘Cyber Threat looms large: is Australia doing enough to ensure cybersecurity?’ (July 2016 accessed 11 Jul 2016)

<[http://docs.media.bitpipe.com/io\\_13x/io\\_132733/item\\_1376580/ANZ\\_ISM\\_0716\\_ezine\\_FINAL.pdf](http://docs.media.bitpipe.com/io_13x/io_132733/item_1376580/ANZ_ISM_0716_ezine_FINAL.pdf)

<sup>75</sup> Lux, above n 26.

- thirdly, there are practical, risk-management-based approaches to address CIOT policy making and better shape industry practices, if responsive 'alliance-based' regulatory and self-regulatory positioning is adopted, and enforcement adequately funded and implemented.

Informed by aspects of behavioural economics, regulatory theory and the first emerging CIOT cases and product failure reports, this thesis concludes with a call for strategic policy and various regulatory and self-regulatory actions. It also proposes a series of draft principles for CIOT policy and regulation which synthesise established best practice by design, conform to the normative values expressed within the Framework and offer an improved prospect of protecting and realising the commercial and public interest in a principled, morally-grounded<sup>76</sup> and trusted CIOT world. Through this approach, the thesis both celebrates and exposes the IOT in all its privacy-intrusive, consumer-abusive glory, and cast in the light of ACPF norms, puts the fundamental question – how, if at all, to best regulate an Australian consumer IOT – to the test.

## Thesis Structure

The thesis has four parts, with eight chapters plus this introduction and conclusion.

**Part I** defines important concepts and briefly outlines a macro perspective of the Australia's CIOT economy; revealing the exponential projections which frame it as so economically attractive, and which may underlie less-interventionist political approaches to CIOT regulation. **Chapter 1** proposes and justifies a(nother) definition to focus upon consumer interests. It discusses the scale and scope of the CIOT including the 'monumental',<sup>77</sup> "mind boggling and ridiculous"<sup>78</sup> projections to assess its potential consumer impacts, and takes an Australian consumer awareness snapshot of current and projected adoption, risk perception and prevalence, and consumer trust. It also introduces smart car, home and self, as practical examples of CIOT adoption through which certain legal themes are later explored, including via the gap analysis in Part III. These 'smart' categories were chosen as they are contextually familiar, socially significant, and illustrate the phases of Australian consumer adoption (self), transitioning adoption (cars) and threshold adoption (homes). **Part II chapter 2** then adopts an analytical framework within which to consider the consumer IOT, which is used to explore and substantiate the evaluations in Part III and recommendations in Part IV. Following that framework, **Part III chapter 3** commences an

---

<sup>76</sup> Above n 1. This proposition is accepted by policy-makers the world around; and is a cornerstone of the IOTAA approach – that consumer "trust" is essential.

<sup>77</sup> Linklabs, '16 Ridiculous Internet of Things Statistics as we head into 2016' (2 Dec 2015 accessed 11 Apr 2016) <<http://www.link-labs.com/internet-of-things-statistics-2016/>>

<sup>78</sup> Ibid.

analysis of CIOT 'consumer detriment', including certain structural vulnerabilities and complexities, such as (in)security, and big data (mis)use and breach, and intertwined adverse attributes of algorithms, analytics, anonymisation, corporate acquisition and the cloud. **Chapters 4, 5 and 6** then address the efficacy of consumer law, privacy and contract consumer protection regimes against identified CIOT consumer detriments. **Chapter 4** tests the ACL against known but also in novel or nuanced CIOT contexts; for example, a smart car hypothetical adapts a real-life crash scenario to illustrate legal deficiencies and impending challenges. **Chapter 5** examines privacy in a similar vein, referencing recent cases, data breach occurrences and CIOT research; while **chapter 6** analyses the detriments implicit within online CIOT contracting, using behavioural economics as an explanatory prism. **Part IV** then concludes the Framework analysis in **chapter 7** to recommend a policy-making approach and **chapter 8** details recommendations designed to meet the policy objectives. It also proposes a simple set of draft principles, reflecting accepted CIOT best practice approaches, and which might inform any regulatory approach. Finally, in **conclusion**, the thesis recommends that Australian governments and regulators engage in the international debate actively, conduct the national policy debate as a priority, assess potential CIOT issues early, work with stakeholders closely, and embed industry best-practice-by-default across the Australian CIOT marketplace. As the great electronic skin expands around the globe, it is to be hoped that Australian policy-makers and regulators will seek to ensure that Australian consumers are wherever practically possible, protected, as well as educated and informed, before venturing forth into the vast, waiting CIOT universe.

## Chapter 1. Scoping an Australian consumer internet of things

*We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten. Don't let yourself be lulled into inaction. – Bill Gates<sup>79</sup>*

*There is a danger of trivialising the importance of the Internet of Things...<sup>80</sup>*

Capturing the Australian consumer internet of things (**consumer IOT** or **CIOT**) practically and conceptually, is not as easy as one might expect. There is no accepted IOT or CIOT definition internationally,<sup>81</sup> nor is there Australian-specific market research or studies, either as to overall status or future projection. Nevertheless, it is important to contextualize the CIOT from an Australian perspective to better understand its potential impacts: this chapter therefore briefly reviews selected IOT definitions and descriptions, proposes a more consumer-centric descriptive alternative, identifies CIOT scope, scale and stakes<sup>82</sup> and outlines a brief macro perspective of the potential Australian CIOT economy and its place in the digital world.

Its purpose is to define our terms as best we may, starting with the 'internet of things' to which the 'consumer' will be attached, whether they like it or not.

### 1.1 What's in a name: the consumer 'internet of things'

*The Nine Billion Names of God...<sup>83</sup>*

The internet of things<sup>84</sup> has multiple names,<sup>85</sup> a "global buzz"<sup>86</sup> and no accepted definition.<sup>87</sup> So too, its consumer incarnation, sold by its distinctive 'connectivity' and convenience. In this thesis, the terms IOT,

---

<sup>79</sup> Internet Society, 'Global Internet Report 2015' and 2016 (2016 accessed 2 Sept 2016): 9 <<https://www.internetsociety.org/globalinternetreport/2016/>>

<sup>80</sup> Blackett, above n 19: 6.

<sup>81</sup> This view is incontrovertible at present.

<sup>82</sup> This analytic approach is derived from the NTIA, above n 48.

<sup>83</sup> Arthur C. Clarke, 'The Nine Billion Names of God', *Star Science Fiction Stories* No.1 (1953).

<sup>84</sup> No one really knows who first coined the phrase 'Internet of things' although Kevin Ashton first used it in 1989, so is the default inventor: Kevin Ashton, 'That 'Internet of Things' thing' *RFID Journal* (22 Jun 1999 accessed 3 Apr 2016) <<http://www.rfidjournal.com/articles/view?4986>> Cisco's Chief Futurist prefers 'IOE' as it includes "people, process, data and things" - wearable/ health devices (people), systematisation or improved services (process), increased information capture (data) and greater internet connectivity via sensors (things): Dave Evans, 'The Internet of Things: Connected in Four Dimensions' *Huffington Post* (24 Sept 2014 accessed 2 Mar 2016) <[http://www.huffingtonpost.com/dave-evans/cisco-beyond-things-the-internet\\_b\\_3976104.html](http://www.huffingtonpost.com/dave-evans/cisco-beyond-things-the-internet_b_3976104.html)>

<sup>85</sup> Largely-synonymous terms include: industrial or physical or future internet, situated, pervasive or ubiquitous computing, cyber physical systems, ambient intelligence, Wireless Sensor Networks, smart object networking, machine-to-machine (M2M) communications, sensor-driven analytics, 'Everyware', the Web of Things, the 'Internet of Everything', 'Internet of Everyone', 'Living Services' and amusingly, "bar code on steroids".

<sup>86</sup> Rose, above n 10: 11

<sup>87</sup> Rolf H. Weber, 'Internet of things – Governance quo vadis?' *Computer Law & Security Review* 29 (2013) 341- 347 <<http://www.sciencedirect.com/science/article/pii/S0267364913001015>>; IEEE, 'Towards a definition of the Internet of things

CIOT, and 'smart' and 'data' are used as outlined in **Terminology** above. The author has sought consistency, reader ease of reference and consumer friendly terms over some which may otherwise, be more generally adopted in the literature. 'Smart' is adopted to prefix and distinguish consumer devices which form part of the CIOT; it is a term which locates them as connected akin to smartphones, is consumer friendly and both reflects and reminds consumers that these products, are both revolutionary and qualitatively different.

### 1.1.1 A simple description

It is easier to describe what the CIOT is, than to locate a useful consumer-focused definition in the literature. At its simplest, the consumer IOT may be described as an expanding network of everyday consumer devices which are internet-enabled,<sup>88</sup> and so are described as 'smart'.<sup>89</sup> A slightly more sophisticated version is used by the European Commission: "all-embracing heterogeneous networks of smart [consumer] devices hyper-connected with each other via the Internet".<sup>90</sup> Those networks consist of a constellation of inanimate consumer objects – such as smart cars, fridges, TVs and watches - designed with built-in wireless connectivity, so they may conveniently be linked, monitored and controlled via the internet by consumers (often) using a mobile app on a smartphone or tablet.<sup>91</sup> These devices are unique as they can record, collect, process, transfer and store consumer data continuously, unobtrusively and seamlessly,<sup>92</sup> while relaying information back to consumers, cloud-based applications and amongst devices, through design features such as ubiquitous connectivity,<sup>93</sup> intelligence, interactivity and autonomy,<sup>94</sup> and unique<sup>95</sup> internet-identification.<sup>96</sup> Collected 'data' may include anything sensate,

---

(IOT)' (27 May 2015 accessed 22 Mar 2016) <<http://IOTbusinessnews.com/download/white-papers/IEEE-IOT-Towards-Definition-Internet-Of-Things.pdf>>

<sup>88</sup> Christina Mercer, 'What is the Internet of Things? Everything you need to know about IOT' *Techworld* (7 Dec 2015 accessed 13 Mar 2016) <http://www.techworld.com/big-data-what-is-internet-of-things-361109/>; Note some IOT devices do not use IP or directly connect to the internet: Kayleen Manwaring and Roger Clarke, 'Surfing the third wave of computing: A framework for research into networked eObjects' *Computer Law and Security Review* 31 (2015) 186- 203 (accessed 9 Aug 2016) <<http://dx.doi.org/10.1016/j.clsr.2015.07.001>>

<sup>89</sup> Griffith Hack, 'The Internet of Things: Smart Objects, Not-So-Smart Users?' (16 May 2016 accessed 19 May 2016) <<http://griffithhack.com/ideas/insights/the-internet-of-things-smart-objects-not-so-smart-users/>>

<sup>90</sup> EC, above n 17: 2

<sup>91</sup> Walt Mossberg cited in Bonnie Cha, 'A Beginner's Guide to Understanding the Internet of Things' *recode* (15 Jan 2017 accessed 20 Jan 2017) <<https://www.recode.net/2015/1/15/11557782/a-beginners-guide-to-understanding-the-internet-of-things>>

<sup>92</sup> EU, above n 49.

<sup>93</sup> EC, 'Commission Staff Working Document: Advancing the Internet of Things in Europe' (19 Apr 2016 accessed 3 Jun 2016): 6 <<https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe>>

<sup>94</sup> Andy Mulholland, Constellation Research cited in Mercer, above n 88: 19.

<sup>95</sup> 'Unique identifiers' include RFID or (micro)processors embedded within products or on inventory by label and tracks products using radio waves. RFID will replace barcoding as it enables individual product identification- which vegemite jar amongst all the vegemite - for example: Ava Itzkovitch, 'The Internet of Things and the Mythical Smart Fridge' *UX Magazine* (18 September 2013 accessed 10 Jun 2016) <<http://uxmag.com/articles/the-internet-of-things-and-the-mythical-smart-fridge>>

<sup>96</sup> Mercer, above n 88.

measurable or detectable: from the temperature of a home, to how fast a driver drives or the (geo)locations where a runner likes to jog. In this way, CIOT devices are uniquely intrusive; operating within many hitherto private spheres and specifically designed 'always on' to collect a consumer's 'personal information'. That extends from geolocation, biometrics, personal habit markers, health or lifestyle information to detecting implicit 'signals' revelatory of preferences, interests, behaviours and inferable characteristics. In the simplest data flow, consumer data travels human-to-device- to-app-to-cloud, and provides the consumer with a service, such as automation or data in a conveniently analysed and quantified form.

Consumers provide personal 'consent' to data storage and uses by activating devices and/ or downloading apps subject to 'terms'; usually by 'accepting' often linked, legalistic and lengthy device and app terms and privacy statements. Like all data in a (very) big data world, those consents usually enable consumer information to be analysed, amalgamated, anonymised, used for predictive analytics, behavioural marketing or simply, shared, traded, on-sold or transferred, across corporations, countries or across the world, in a multitude of transactions and for a multitude of purposes. It is a highly monetized, opportunistic, backend process largely unknown to and likely, unimaginable by, the average Australian consumer.

### **1.1.2 A complex debate**

*Now we have one name but can't agree on what it means.*<sup>97</sup>

IOT seems to be the accepted 'name', although 'internet of everything' is gaining traction.<sup>98</sup> There is an encyclopedia<sup>99</sup> of "evolving, overlapping and inconsistent"<sup>100</sup> definitions for the IOT, each a stakeholder prism of the ".infrastructure of the information society".<sup>101</sup> The IEEE studied over fifty authoritative

---

<sup>97</sup> Bernard Cole, 'Namedropping: the Many Names of the Internet of Things' *EE Times* (20 Jan 2015 accessed 22 Mar 2016) <[http://www.eetimes.com/author.asp?section\\_id=36&doc\\_id=1325245](http://www.eetimes.com/author.asp?section_id=36&doc_id=1325245)>

<sup>98</sup> E.g. Terrell McSweeney, 'Consumer Protection in the Age of Connected Everything' *Keynote remarks, New York Law School* (3 February 2017 accessed 5 Feb 2017) <<https://www.ftc.gov/public-statements/2017/02/consumer-protection-age-connected-everything>>; Peter Leonard, 'The Internet of Things (aka The Internet of Everything): What Is It About and Who Should Care' (4 Aug 2016 accessed 8 Aug 2016) <<https://www.gtlaw.com.au/?q=internet-things-aka-internet-everything-what-it-about-and-who-should-care>>; Cisco, 'Internet of Everything: A \$4.6 trillion Public-Sector Opportunity' *White Paper* (2013 accessed 8 Apr 2016) <[http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe\\_public\\_sector\\_vas\\_white%20paper\\_121913final.pdf](http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf)>

<sup>99</sup> The IEEE recently cited fifty(+) authoritative definitions: IEEE, above n 87: 10.

<sup>100</sup> Manwaring, above n 88.

<sup>101</sup> The IEEE identify definition focus points: sensing and actuation capability, ubiquity, architectural principles, platform or infrastructure layer, connectivity, data, enabler technologies, structural aspects (protocols, security features), architectural aspects (domains and abstractions, standardization network and communications factors), and so on: above n 87: 90.

definitions- from the ITU,<sup>102</sup> EU Research Cluster,<sup>103</sup> NTIA,<sup>104</sup> IEFT,<sup>105</sup> to Cisco,<sup>106</sup> IBM,<sup>107</sup> (and so on) – and then carefully, wrote two more.<sup>108</sup> From the author’s review, it seems clear that each quite properly reflects stakeholder priority and ecosystem perspective, but few reflect consumer experience. Device technical attributes<sup>109</sup> or connectivity predominate: for example, the European Research Cluster’s oft-cited definition:

*A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communications protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.*<sup>110</sup>

While scrupulously accurate, the consumer-as-stakeholder or even as reader perspective seems particularly absent. Vodafone adds, “. that connects to smart things...”<sup>111</sup> after ‘protocols’, while other definitions insert elements such as security: “...the use of network intelligence, convergence,

---

<sup>102</sup> “A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communications technologies”: Global Standards Initiative on Internet of Things (IoT-GSI) ‘Recommendation ITU-T Y.2060’ (06/2012 accessed 2 Feb 2016) <http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx>

<sup>103</sup> Cited at n 110 supra: European Research Cluster on the Internet of things (IERC), ‘Internet of Things’ (2013 accessed 2 Jan 2016) <[http://www.internet-of-things-research.eu/about\\_iot.htm](http://www.internet-of-things-research.eu/about_iot.htm)>

<sup>104</sup> “...the connection of physical objects, infrastructure, and environments to various identifiers, sensors, networks, and/or computing capability...”: NTIA, above n 48.

<sup>105</sup> The “... basic idea is that IOT will connect objects around us... to provide seamless communication and contextual services”: cited in IEEE, above n 87.

<sup>106</sup> Its definition (reflecting its commercial interests) is: “...the use of network intelligence, convergence, orchestration, and analytics added to a secure connection between devices”: Cisco, ‘Connected Athlete’ (2013 accessed 17 Apr 2016) [http://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/white\\_paper\\_c11-711705.html](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/white_paper_c11-711705.html)

<sup>107</sup> IBM, ‘Submission to NTIA’ (2 June 2016 accessed 20 Mar 2017): 9

<[https://www.nist.gov/sites/default/files/documents/2016/09/16/ibm\\_rfi\\_response.pdf](https://www.nist.gov/sites/default/files/documents/2016/09/16/ibm_rfi_response.pdf)> cited in NTIA, above n 48.

<sup>108</sup> The IEEE adopted: “Large environment scenario: A self-configuring, adaptive, complex network that interconnects ‘things’ to the Internet through the use of standard communications protocols... things have physical or virtual representation in the digital world, sensing/ actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing’s identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything, taking security into consideration.” “Small environment scenario: An IoT is a network that connects uniquely identifiable “Things” to the internet... [which]... have a sensing/ actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the ‘thing’ can be collected and the state of the “Thing” can be changed from anywhere, anytime, by anything.”: IEEE, above n 87.

<sup>109</sup> “The set of physical objects embedded with sensors or actuators and connected to a network...” Center For Data Innovation, ‘NTIA Comment’ (13 Mar 2016 Accessed 15 Jan 2017) <https://www.ntia.doc.gov/files/ntia/publications/cdi-comments.pdf> at 8 <<https://www.ntia.doc.gov/files/ntia/publications/cdi-comments.pdf>>

<sup>110</sup> IERC, above n 103. This definition is adopted in Alexander Vulkanovski, “Home, Tweet Home”: Implications of the Connected Home, Human and Habitat for Australian Consumers’ ACCAN (Feb 2016 accessed 17 Apr 2016): 10

<sup>111</sup> As cited in NTIA, above n 48: 6.

orchestration, and analytics added to a secure connection between devices...<sup>112</sup> (Cisco) or identify the roles of software, big data and analytics (GSMA<sup>113</sup> and IBM):

*The growing range of internet-connected devices that capture or generate an enormous amount of data every day along with the applications and services used to interpret, analyse, predict and take actions based upon information received...<sup>114</sup>*

In Australia, the Communications Alliance adopts the ITU definition:<sup>115</sup>

***A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.***

*NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IOT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.*

*NOTE 2 – From a broader perspective, the IOT can be perceived as a vision with technological and societal implications.<sup>116</sup>*

This thesis acknowledges salient arguments against a non-sectoral<sup>117</sup> or indeed, any IOT definition altogether,<sup>118</sup> but given its nascent status in Australia, a definition is useful as an educative starting point, and this high-level definition allows for evolution, refined by important “qualifications”<sup>119</sup> as to data, security, privacy and societal implications reflective of current consumer law and policy concerns. Of course, this begs the question as to defining the ‘consumer’ IOT itself. As an internationally accepted IOT

---

<sup>112</sup> Cisco, above n 106.

<sup>113</sup> GSMA, ‘IoT Security Guidelines Overview Document’ (Feb 2016 accessed 2 Apr 2016):6 <<http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.11-v1.1.pdf>>

<sup>114</sup> IBM, above n 107: 9.

<sup>115</sup> “A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies”: ITU, above n 101.

<sup>116</sup> ITU, *Ibid*.

<sup>117</sup> Refined or sectoral definitions for CIOT categories such as smart home, self or cars (for example) may be more meaningful, given the diverse ecosystem of industries, devices, technologies and applications involved in each: the NTIA propose that policy is better directed at “categories’ of uses and/ or devices, rather than all of IoT”. NTIA, above n 48: 7.

<sup>118</sup> The caveat is (at least) twofold: firstly, ‘consumer’ meanings vary internationally and which defects/ people attract legal recourse. The FTC approach implies this view: they define IOT descriptively: “...day-to-day consumer products and services that connect to the internet”, and communicate with other devices, us or others...”: FTC, ‘Careful Connections: Building Security in the Internet of Things’ (Jan 2015 accessed 23 Feb 2016) <<https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things>>; their recent NTIA submission adds: “...the ability of everyday objects to connect to the Internet to send and receive data...”: FTC, ‘Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission before the Federal Communications Commission’ (27 May 2016 accessed 30 Jun 2016): 3 <<https://www.ftc.gov/policy/policy-actions/advocacy-filings/2016/05/comment-staff-bureau-consumer-protection-federal>> Secondly, device-based, use- based or other classification approaches are evolving. NIST’s 2017 ‘foundational science’ creates a composability ‘building-block’ model identifying IOT or network of things (NOT) via “...sensing, computing, communications and actuation” attributes. It defines the “primitives” injecting “thing” behaviours, rather than a definition: Jeffrey Voas, ‘Networks of ‘Things’” *NIST Special Publication 800- 183* (Jul 2016 accessed 2 Oct 2016) <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf>> See also Manwaring and Clarke, above n 88.

<sup>119</sup> Communications Alliance, ‘Enabling the Internet of Things in Australia’, Geof Heydon & Frank Zeichner (Oct 2015 accessed 3 Jan 2016): 116 <[http://www.commsalliance.com.au/\\_\\_data/assets/pdf\\_file/0007/51991/Enabling-the-Internet-of-Things-for-Australia.pdf](http://www.commsalliance.com.au/__data/assets/pdf_file/0007/51991/Enabling-the-Internet-of-Things-for-Australia.pdf)>

subset, deemed useful to distinguish differing industrial: consumer policy concerns,<sup>120</sup> the author thus proposes a simple descriptive snapshot definition:

**The consumer internet of things (CIOT) consists of day-to-day consumer devices connected to the internet which collect consumer information through sensors, often store that information in the cloud and provide analysed data to consumers on-device or through software apps, while enabling device and app providers to any of use, aggregate, anonymise, analyse, transfer or on-sell such information and data into the big data ecosystem for myriad purposes, subject only to applicable contractual and privacy terms, and consumer laws.**

The approach attempts to define consumer experience within the ecosystem and to identify consumer law access points within the current boundaries of the consumer IOT. Those points include four structural aspects: the tangible element (the device), its embedded software and related maintenance requirements; the supply of digital infrastructures or services (via long-term contracts) and finally, the capture and exploitation of consumer data.<sup>121</sup> Consumer law applies to CIOT by dissecting many of these elements or contractual layers:

[C]IOT is not itself a 'thing', device or product ... it is a conceptual structure consisting of tangible things (e.g. commercial and consumer goods containing sensors) ... plus intangibles (e.g. software and data), plus a range of services (e.g. transmission, development, access contracts, etc....)"<sup>122</sup>

This is assumed in this thesis,<sup>123</sup> at least until the Part III critique, when those boundaries may be practically challenged and the extent to which Australian consumer law offers CIOT protection, may be tested.

---

<sup>120</sup> NTIA stakeholder submissions support 'consumer IOT' as a category distinct from the industrial IOT for policy reasons, given differing concerns and implications over matters such as safety, privacy and security: NTIA, 'Comments on Fostering the Advancement of the Internet of Things' (15 Mar 2017 accessed 20 Mar 2017): 7 <<https://www.ntia.doc.gov/federal-register-notice/2017/comments-fostering-advancement-internet-things>>. See e.g. Association for Computing Machinery US Public Policy Council Comment at 3; Cisco Systems Comment at 25; CompTIA Comment at 5-6; State of Illinois Comment at 20; Bugcrowd Comment at 3; Motorola Solutions Comment at 5; Secure ID Coalition Comment at 2; BSA The Software Alliance Comment at 5; and CDI Comment, at 11-12.

<sup>121</sup> EC, above n 17: 3.

<sup>122</sup> American Bar Association Section of Science and Technology Law, Comment to NTIA: 15.

<sup>123</sup> Smart health evidences that the distinction is complicating; when does a consumer device become medical or vice versa. At law, therapeutic goods requirements should apply, but may require refinement as device complexity increases.

### 1.1.3 What's in a name: the 'consumer' in CIOT

'Consumer'<sup>124</sup> has many nuanced meanings internationally.<sup>125</sup> especially in the multiple-layered, horizontally and vertically-integrated, IOT context.<sup>126</sup> In this thesis, its meaning is drawn from colloquial usage and consumer law, as the context indicates. The principal legal definition derives from the Australian Consumer Law (**ACL**), with incarnations as 'consumer contract' in the Parts 2-3 unfair contracts terms regime,<sup>127</sup> 'consumer guarantee' in Part 3-2 consumer guarantees,<sup>128</sup> and in the 'consumer goods' definition in Parts 3-3 and 4-3 as to product safety standards.<sup>129</sup> Specifically, ACL section 3 presumes<sup>130</sup> an acquiring entity a "consumer" if the price<sup>131</sup> of goods or services acquired<sup>132</sup> is \$40,000 or less; or alternatively, the goods<sup>133</sup> or services<sup>134</sup> (objectively assessed)<sup>135</sup> are of a kind

---

<sup>124</sup> ACL section 3 (1)(a)(i) states a person is taken to have acquired goods as a 'consumer' if the price is \$40,000 or less, or where greater (b) the goods were of a kind ordinarily acquired for personal, domestic or household use or consumption; (c) ... consisted of a vehicle or trailer acquired for use principally in the transport of goods on public roads. The definition excludes acquisitions for the purpose of: (a) ...re-supply; (b) ... using them up or transforming them, in trade or commerce (as defined); or (i) in the course of a process of production or manufacture; or (ii) in the course of repairing or treating other goods or fixtures on land. Goods includes 'software': section 2(e) and 'consumer contracts' are defined in section 23(3). "Services" are acquired as a consumer if they cost \$40,000 or less, or are of a kind ordinarily acquired for 'personal, domestic or household use or consumption'

<sup>125</sup> Margus Kingisepp and Age Värvi, 'The Notion of Consumer in EU Consumer Acquis and the Consumer Rights Directive—a Significant Change of Paradigm?' *Juridica International* (2011) XVIII <<http://www.juridicainternational.eu/?id=14841>>; Martin Ebers 'The Notion of Consumer in Community Law' *Comparative Analysis* (n.d. accessed 10 Aug 2014) <[http://www.eu-consumer-law.org/consumerstudy\\_part3a\\_en.pdf](http://www.eu-consumer-law.org/consumerstudy_part3a_en.pdf)>; Waller, Weber, Brady, Acosta and Fair, 'Consumer Protection in the United States: An Overview' *European Journal of Consumer Law* (May 2011 accessed 20 Feb 2016) <<https://ssrn.com/abstract=1000226>>; CI, above n 44.

<sup>126</sup> CI, above n 44. This cites multiple tech factors which contribute to its pervasive consumer interaction.

<sup>127</sup> ACL section 23(3): "consumer contract" is a supply of goods or services ... "to an individual, whose acquisition... is [subjectively] wholly or predominantly for personal, domestic or household use or consumption". This now includes a 'small business' contract', for supplies of goods or services where one party employs less than 20 people and either the upfront price payable is \$300,000 or less or the contract lasts over a year with an upfront price payable of \$1 million or less: s 23(4).

<sup>128</sup> ACL consumer guarantees cover undisclosed securities (s. 53), acceptable quality (s. 54), fitness for any disclosed purpose (s. 55), supply of goods by description (s. 56), supply of goods by sample or demonstration (s. 57), repairs and spare parts (s. 58), express warranties (s. 59) and as to "services": due care and skill (s. 60), fitness for a particular purpose (s. 61), and reasonable time for supply (s. 62).

<sup>129</sup> ACL s. 2(1) provides that 'consumer goods' are those either intended to be used or likely to be used for personal domestic or household use or consumption, if a mandatory or voluntary recall notice has been issued for those goods.

<sup>130</sup> ACL section 3(10) imposes a rebuttable presumption that a person is a 'consumer' if it is asserted that goods or services are acquired in that capacity.

<sup>131</sup> Sections 3 (4)- (9) provide for calculation of the "amount paid or payable": acquisition not by purchase: ss (4); acquired together without allocation of amount: ss(5)- (8) and where credit is obtained in their regard: ss (9).

<sup>132</sup> The section refers to 'acquired' or 'to be acquired'.

<sup>133</sup> ACL section 3(1).

<sup>134</sup> ACL Section 3(3).

<sup>135</sup> The court's 'objective' assessment means that commercial grade carpet and insulation, and commercial alarm systems are consumer purchases, even where subjectively purchased by businesses for commercial uses or premises: see *Carpet Call v Chan* (1987) ASC 55- 553; (1987) ATPR (Digest) 46-025; *Bunnings v Laminex* [2006] FCA 682 and *Crawford v Mayne Nickless Ltd* (1992) ASC 56-144; (1992) ATPR(digest) 46-091, respectively. In that latter case, the court said that carpet does not lose its character as a personal, domestic or household item, due to any 'commercial' quality. Likewise, inherently commercial products or services do not become a consumer item just because their (subjective) use is of a personal domestic or household nature (e.g. a large tractor: *Atkinson v Hastings Deering (Qld) Pty Ltd* (1985) 8 FCR 481; 71 ALR 93).

ordinarily acquired for ‘...personal domestic or household use or consumption’,<sup>136</sup> subject only to limited use exceptions for goods<sup>137</sup> (ACL definition). The objective nature of the assessment is expansive:<sup>138</sup> ‘ordinarily acquired’ means commonly or regularly<sup>139</sup> acquired, not predominantly,<sup>140</sup> and the courts have found business purchases of carpet and insulation for commercial premises and uses are included. As such, the focus of the second limb, is on the objective nature of the good itself, not its acquirer or their subjective purpose.

While there is no industry definition of what comprises consumer IOT ‘goods’ or ‘services’,<sup>141</sup> one European survey found fourteen types,<sup>142</sup> of which the four most important are healthcare<sup>143</sup> (e.g. ‘smart’ wearables such as fitness bands), home (e.g. ‘smart’ home whitegoods, heating, lighting, watering and security devices), transportation (e.g. ‘smart’ cars) and personal/ social (e.g. smartphones, which through ‘apps’ become vital CIOT consumer control and information components). These are the CIOT exemplars used in this thesis. There seems little doubt that these devices are of the ‘kind’ of goods or services contemplated in the ACL definition: smart self and home devices such as fitness bands and smart fridges will usually fall within the price threshold, smart cars mostly will<sup>144</sup> or will fall under the objective ‘personal, domestic or household use’ limb.<sup>145</sup> ‘Goods’<sup>146</sup> also inclusively<sup>147</sup> mean software<sup>148</sup> which clarifies previous uncertainty as to whether ‘unboxed’ software internet downloads fall within the ACL,<sup>149</sup> and is important given the app- integration of most CIOT devices and the related information and

---

<sup>136</sup> Similar to that in section 4B of the *Competition and Consumer Act 2010* (Cth).

<sup>137</sup> Section 3 excludes certain acquisitions: above n 124. These are unlikely to be relevant to smart self, car or home, so are not examined further.

<sup>138</sup> It has been expansively interpreted by the courts: above n 135.

<sup>139</sup> *Bunnings Group Ltd v Laminex Group Ltd* [2006] FCA 682.

<sup>140</sup> *Crago v Multiquip Pty Ltd* [1998] ATPR 41-620.

<sup>141</sup> Bailey, above n 51: 1028.

<sup>142</sup> Pasi Pussinen and Hanna Okkonenm ‘Scenarios for IoT’ in Oleksiy Mazhelis et al (eds), *Internet of Things Market, Value networks and business models: State of the Art Report* (2013) 63, 64: cited in *Ibid*.

<sup>143</sup> As noted, healthcare may straddle the consumer ‘good’ divide; increasing device sophistication and reduced cost may mean medical profession purposes and personal domestic or household uses overlap - for example, a medical grade diagnostic smart self device versus smart self devices of increasing capability and accuracy.

<sup>144</sup> This assumes cars retain their present social role – questionable – given changing (shared or licensed) ownership models, and the proliferation of tangible goods embedded with manufacturer-owned licensed software.

<sup>145</sup> This includes a vehicle purchased for use principally in public road, goods transportation irrespective of price.

<sup>146</sup> ACL section 2 defines ‘services’ similarly to CCA section 4. As to ‘goods’, section 2 added computer software, second-hand goods and any component part or accessory to, goods.

<sup>147</sup> The definition supplements the ordinary meaning: *ASX Operations Pty Ltd v Pont Data Australia Pty Ltd* (No 1) (1990) 27 FCR 460, 468.

<sup>148</sup> Prior to the clarification, software supplied on a physical medium like a CD rom was a ‘good’: *Amlink Technologies Pty Ltd and the Australian Trade Commission* (2005) AATA 359 *c/f* digitally downloaded software: *Gammasonics Institute for Medical Research Pty Ltd v Comrad Medical Systems Pty Ltd* [2010] NSWSC 267. There is little consumer-protection rationale for this distinction: Jay Forder & Dan Svantesson, *Internet & Ecommerce Law* (Oxford University Press, 2010) [87]. *Valve* may have clarified the point with respect to software licensed and supplied online, overcoming *Gammasonics*.

<sup>149</sup> Prior to the clarification, there was doubt as to whether unboxed software would constitute a ‘good’: *Amlink Technologies Pty Ltd and the Australian Trade Commission* (2005) AATA 359. As pointed put by Forder & Svantesson, Forder, above n 148: [87] there can be little rationale for a consumer-protection distinction between software purchased from a shop and software purchased online.

other 'services' (in a non-ACL sense) they provide.<sup>150</sup> While the author speculated otherwise analogously,<sup>151</sup> the recently decided (but on appeal) *ACCC v Valve* case affirms that software retains the character of a 'good' despite multiple service-like attributes such as internet downloads, auto updates, cloud storage, ongoing provisioning and a plethora of other "service-like" deliverables.<sup>152</sup> This discussion continues in Ch. 4. So too, the legal point that many 'apps' are licensed free and are essentially, a license by subscription, which (despite no case authority on point) seems likely to mean that the inclusive ACL definition of "acquire"<sup>153</sup> is broad enough to include the latter concept, and even the former - where the mutual 'free' exchange is (effectively) commercially-valuable personal information or privacy-trading in nature. As this suggests, the CIOT acquisitions discussed will likely render the purchaser an ACL 'consumer', such that the consumer guarantees, and unfair terms provisions will apply to CIOT devices, apps and any 'services'. Further, consumers commonly use other ACL provisions – such as those proscribing provider misleading and deceptive conduct, unconscionability and false representations – even though not referred to specifically. As such, the ACL generally covers most individuals and SME businesses<sup>154</sup> across the range of CIOT contexts contemplated here. To summarize, this thesis adopts the ACL 'consumer' definition when referring to the ACL, but 'consumer' may be broader in other chapters, to mean any individual who may be exposed to or affected by the consumer IOT - for example, a person whose privacy is infringed, or one who uses non-consumer specific ACL clauses.<sup>155</sup> While most consumers and businesses acquiring CIOT devices and apps within the smart self, home and car categories are ACL 'consumers' as acquirers of 'goods',<sup>156</sup> others who ride in or alongside another's smart car, or visit or work in smart homes or who may borrow smart self devices, are all (colloquially) 'consumers' here too. Finally, reflecting that contextual, collective approach, the term 'provider' includes CIOT manufacturers, retailers, app suppliers, cloud and analytics services and other entities within the complex CIOT supply chain, unless the context requires more specific reference.

A corollary to the definitional dilemmas above is the underlying regulatory question: whether the consumer IOT poses novel consumer social or technological issues, or those different enough to warrant

---

<sup>150</sup> Most people experience apps, data analytics and downloads as 'services' – but only in the colloquial sense.

<sup>151</sup> See Kate Mathews-Hunt, 'CloudConsumer: contracts, codes and the law' *Computer Law & Security Review* 31 (2015) 450- 477 <http://dx.doi.org/10.1016/j.clsr.2015.05.006> The musing was in the context of cloud services: especially SaaS.

<sup>152</sup> ACL section 2: 'services' include rights, benefits or privileges or facilities to be provided, granted or conferred under "... a contract for or in relation to the performance of work ... whether with or without the supply of goods..."

<sup>153</sup> ACL section 2: 'acquire' includes (a) in relation to goods – acquire by way of purchase, exchange or taking on lease, on hire or hire purchase; and (b) in relation to services – accept. Under section 11 references to acquisition are broadly interpreted to include the acquisition of property in, or rights in relation to, goods pursuant to the supply and includes mixed acquisitions including goods, property and/ or services.

<sup>154</sup> SME is used in the sense of sole traders, unincorporated businesses, up to corporations which are unlisted.

<sup>155</sup> For example, ACL sections 18 and 29 may apply if a tenant sharing a smart home is misled or deceived over personal data collection, or via misleading manufacturer advertising.

<sup>156</sup> *Four Square Stores (Qld) Ltd v ABE Copiers Pty Ltd* [1981] ATPR 40-232.

specific policy and/ or regulatory attention. Put simply, is there anything unique about the CIOT necessitating response or is it just “old problems squared”.<sup>157</sup> This is considered next, as is the CIOT in its Australian context, to foreground the risk assessments in Part III and the regulatory responses proposed in Part IV.

## 1.2 Scope, scale, stakes

*[C]IOT poses qualitatively different opportunities and challenges from those that society has dealt with before... because existing opportunities and challenges of the internet are emerging in new contexts, with greater reach and impact...<sup>158</sup>*

It is often asserted that the IOT is evolutionary not revolutionary,<sup>159</sup> so at worst, may exacerbate existing legal and policy problems, but requires no government intervention or IOT-specific or even, regulatory change,<sup>160</sup> until serious consumer problems eventuate.<sup>161</sup> This justifies the ‘wait, innovate then regulate’ mantra<sup>162</sup> - one which is rapidly growing thin, as the wait lengthens, known problem amplification expands and innovation strains legal boundaries. A more moderate approach is the view that there is no need for IOT-specific regulation, but as risks change across differing sectors, problems (evidenced market failures) may require industry self-regulation or principles-based approaches.<sup>163</sup> This thesis argues that smart *consumer* IOT regulation needs both – and remedial legislative action - because the CIOT is revolutionary for multiple reasons: it is global, it is ‘here’ already<sup>164</sup> driven by provider industries and

---

<sup>157</sup> Amy Collins, Adam Fleisher, Reed Freeman & Alistair Maughan, ‘The Internet of Things: The Old Problem Squared’, *Morrison & Fleisher, Society for Computer & the Law* (24 Mar 2014 accessed 22 Apr 2016) <<https://www.scl.org/articles/3055-the-internet-of-things-the-old-problem-squared>>

<sup>158</sup> NTIA, above n 48.

<sup>159</sup> Steve Case, *The Third Wave* (Simon and Schuster, April 2016); For a manufacturer’s perspective, see Samsung, ‘Letter to the NTIA, US Department of Commerce On the Benefits, Challenges and Potential Roles for the Government in Fostering the Advancement of the Internet of Things’ (2 June 2016 accessed 26 Jun 2016)

<[https://www.ntia.doc.gov/files/ntia/publications/samsung\\_ntia\\_iot\\_letter\\_6-2-16-c1.pdf](https://www.ntia.doc.gov/files/ntia/publications/samsung_ntia_iot_letter_6-2-16-c1.pdf)>; Part 2

<<https://www.ntia.doc.gov/files/ntia/publications/vc-kwon-keynote-remarks-6-2116.pdf>> and Part 3 <

[https://www.ntia.doc.gov/files/ntia/publications/samsung\\_iot\\_framework\\_paper\\_july\\_2016.pdf](https://www.ntia.doc.gov/files/ntia/publications/samsung_iot_framework_paper_july_2016.pdf)>

<sup>160</sup> Vulkanovski, above n 110. He concludes that CIOT has a “synergetic effect”, so will not raise (m)any new consumer issues – which justifies his largely consumer-beware, permissionless innovation-style recommendations.

<sup>161</sup> See the comprehensive work of US academic, Adam Thierer: Adam Thierer, *Permissionless innovation: the Continuing Case for Comprehensive Technological Freedom*, (2016 accessed 5 Mar 2016)

<http://mercatus.org/publication/permissionless-innovation-continuing-case-comprehensive-technological-freedom>; Adam Thierer, ‘The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things’ Testimony Before the NTIA (1 Jun 2016 accessed 12 Jun 2016) <<http://mercatus.org/publication/benefits-challenges-and-potential-roles-government-fostering-advancement-internet-things>>; Adam Thierer, ‘15 Years On, President Clinton’s 5 Principles for Internet Policy Remain the Perfect Paradigm’ *Forbes Opinion* (12 Feb 2012 accessed 2 Feb 2016)

<http://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remain-the-perfect-paradigm/print/>>; Adam Thierer, ‘Technopanics, threat inflation and the danger of the precautionary principle’ 14 *Minn. J. L. Sci. & Tech.* 309 (2013) <<http://purl.umn.edu/144225>>

<sup>162</sup> *Ibid*; Vulkanovski, above n 110.

<sup>163</sup> AIOTA, above n 49: 4. “Any regulatory proposal targeting the IoT should address only well-defined market failures that cannot be addressed through existing law and self-regulatory measures.” In contrast, their 2017 workshop acknowledges that such failure is sufficiently evidenced by a range of ‘problems’: EC, above n 17.

<sup>164</sup> EC, above n 17: 1. In a consumer context, the IOT “will become reality within the next five years.”

almost before consumers or regulators have drawn breath, it is 'urgent' that it be acted upon to shape its future parameters and to protect the public interest, and it is contextually, qualitatively and quantitatively different in terms of its **scope, scale and stakes**.<sup>165</sup> Further, CIOT consumer risk, legal and policy problem 'exacerbation' is of itself so quantitatively significant, as to also justify the epithet revolutionary.

This section briefly considers these metrics - scope, scale and stakes - illustrating each by reference to smart self, home and car - to support the conclusion that the CIOT poses qualitatively and quantitatively different challenges, with greater reach and impact and in new contexts, from those which Australian consumer law has faced before.<sup>166</sup>

### 1.2.1 Scope

*In the near future, the IOT ultimately will touch nearly every economic sector and break every regulatory silo...*<sup>167</sup> - Samsung

The IOT entails convergence between the economy and ICT on a "grand scale",<sup>168</sup> via the integration of more systems, devices, sectors and technologies than ever before.<sup>169</sup> As the ITU suggest, the IOT has a unique capacity to "greatly integrate leading technologies" including those related to advanced M2M, data mining and decision-making, cloud computing,<sup>170</sup> privacy and security protections, as well as advanced sensing and actuation technologies.<sup>171</sup> To those one might specify fields such as artificial intelligence, automated contracting, and big data analytics. This complexity, both interdisciplinary and cross-sectoral in scope, is transformational: impacting government,<sup>172</sup> business, industry, consumers and civil society, nationally and internationally.<sup>173</sup> It promises consumers benefits of increased efficiency, safety, cost, comfort and convenience. It presupposes new **methods** of information and awareness,

---

<sup>165</sup> The criteria, not the analysis, are drawn from NTIA, above n 48 and Vulkanovski, above n 110.

<sup>166</sup> Australian data is used wherever affordably publicly available, but recourse to international studies is necessary.

<sup>167</sup> Samsung, 'Comment to NTIA' (13 Mar 2017 accessed 15 Mar 2017): 5

<[https://www.ntia.doc.gov/files/ntia/publications/samsung\\_commerce-iot\\_comments\\_2017-03-13-c1.pdf](https://www.ntia.doc.gov/files/ntia/publications/samsung_commerce-iot_comments_2017-03-13-c1.pdf)>

<sup>168</sup> OECD, Digital Economy Outlook, 2015 cited in Communications Alliance, above n 119.

<sup>169</sup> Four recent technical 'trends' are significant CIOT enablers: (1) cheaper, smaller semiconductors which enable complex data collection; (2) increased internet network capabilities from 3 billion users (2015) to some 340 trillion, trillion, trillion via IPv6 by 2050; (3) improved data management and increased storage using the cloud, open-source software and "commoditised hardware" to fuel "big(ger) data"; and (4) increasing data analytics capabilities, machine-learning and algorithms. Emerging CIOT-significant developments include artificial intelligence and dynamic human-bandwidth user interfaces – fingerprints, voice and facial recognition technologies. These rapidly-evolving technologies intersect with CIOT and increasingly intertwine within it, to create new forms of CIOT value and risk: Blackett, above n 19.

<sup>170</sup> Linking increasing data with the cloud "...makes the IoT so interesting.": Phillip Branch, 'Are we ready for a world even more connected to the internet of things' *The Conversation* (20 Nov 2015 accessed 3 Mar 2016)

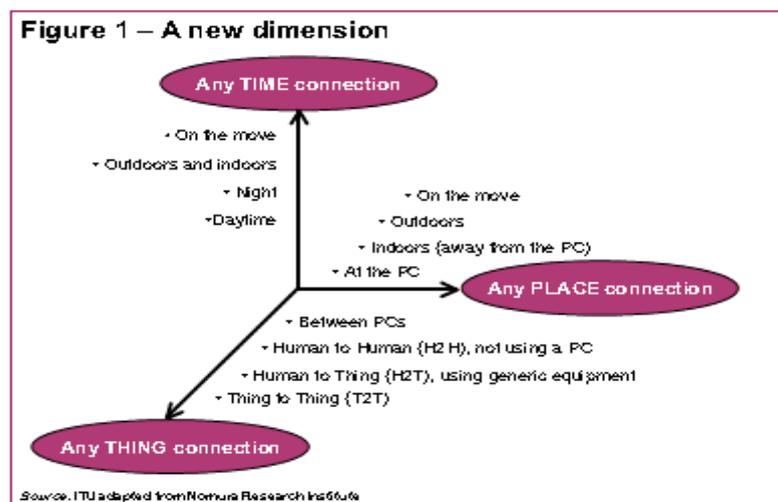
<<http://theconversation.com/are-we-ready-for-a-world-even-more-connected-in-the-internet-of-things-50889>>

<sup>171</sup> ITU, above n 101, Definition NOTE 2.

<sup>172</sup> Increased scope requires "new forms" of cross government, cross-sector knowledge-sharing, alignment and collaboration: NTIA, above n 48: 4.

<sup>173</sup> For example, agriculture efficiency and productivity increases affect domestic industry (with related economic flow-ons internally) but also, international inter-state trade, especially where one country has a more integrated IOT culture.

through ubiquitous consumer sensor and device data collection, sharing and analysis, via “... every mobile, every auto, every door, every room, every part, on every parts list, every sensor on every device in every bed, chair or bracelet in every home, office, building or hospital room in every city and village on Earth...”<sup>174</sup> Those methods enable far greater **reach** to intimate consumer data – inside home management and family habits, inside car driving ‘style’ and entertainment systems, and even, inside the human body. Its **nature** is pervasive, but also seamless and covert, such that consumers may never know - or may lose awareness - that sensitive personal information is collected at any time, by any thing and in any place”.<sup>175</sup>



Graphic 1.1 (C)IOT creates a new dimension  
Source: ITU-T<sup>176</sup>

CIOT’s contribution to (formerly) big data warrants special mention: from “3 V”<sup>177</sup> to “5 V”,<sup>178</sup> via vast volume, wide variety, variable veracity, high velocity and higher value.<sup>179</sup> By definition, ‘big data’ is “...any voluminous amount of data that has the potential to be mined for information...”,<sup>180</sup> involves “gigantic

<sup>174</sup> OASIS is a non-profit consortium which inter alia produces open international standards in areas such as the IOT, cloud computing and so on: IEEE, above n 87: 21.

<sup>175</sup> ITU-T, ‘Overview of the Internet of things’, ITU Former ITU-T Y.2060 renumbered as ITU-T Y.4000 on 2016-02-05 without further modification and without being republished. (2012) <<http://www.itu.int/rec/T-REC-Y.2060-201206-I>>

<sup>176</sup> Ibid.

<sup>177</sup> Data analyst, Doug Laney first named “3V”, that is, data that is large in volume, diverse in variety or moving with extreme velocity: Executive Office of the President, ‘Big Data’, above n 41 [4].

<sup>178</sup> Bernard Marr, ‘The 5V’s of Data’, (9 Apr 2015 accessed 10 Dec 2015) Data Science Central <<http://www.datasciencecentral.com/profiles/blogs/the-5-v-s-of-big-data-by-bernard-marr>>

<sup>179</sup> The world is becoming ‘datafied’, through vast data Volume, high data Velocity, wide data Variety, (variable) data Veracity – to create a (potentially high) Value data ecosystem, comprised of activity data, photo/ video/ image data, conversation data and sensor data: Ibid.

<sup>180</sup> Productivity Commission, ‘Data Availability and Use’ *Issues Paper* (April 2016 accessed 26 Apr 2016): 3 <<http://www.pc.gov.au/inquiries/current/data-access/issues>>

digital datasets”<sup>181</sup> and a “confluence” of near-ubiquitous collection, cheap storage and powerful new analytics capabilities – especially as to data fusion,<sup>182</sup> inferences and predictions. Data is” big business”<sup>183</sup> - the twenty-first century “oil” firing the combustion engine of data analytics.<sup>184</sup> And big data was indeed ‘big’<sup>185</sup> – until the IOT.<sup>186</sup> From 4 zettabytes<sup>187</sup> globally in 2013,<sup>188</sup> it will generate a predicted 44 zettabytes of data - annually.<sup>189</sup> CIOT adds a novel, accelerating<sup>190</sup> dimension: the capacity to detect functionally unknown, ‘dark’ personal information and to make it visible. From a consumer analytics, machine-learning<sup>191</sup> and marketing perspective, the ‘any time, any place, always-on’<sup>192</sup> CIOT, leveraging upon “open data”,<sup>193</sup> social media,<sup>194</sup> other platforms<sup>195</sup> and the internet, will be integral to harvesting more personal, hitherto private, consumer data than ever before. Big (projected) revenues support big player investment by Google, Amazon, Microsoft and Facebook,<sup>196</sup> as well as a raft of IT, automotive and

---

<sup>181</sup> Peter Hustinx, ‘Executive Summary of the Preliminary Opinion of the European Data Protection Supervisor on privacy and competitiveness in the age of big data’ (26 Mar 2014 accessed 6 Dec 2016) <[http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014XX0716\(01\)&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014XX0716(01)&from=EN)> citing the Art 29 WP, Opinion 03/2013: 35.

<sup>182</sup> Data “fusion” means combining data from two or more contemporaneous sources, to gain greater depth of insight – for example, combining smart home data with smart self and smart car data – plus public social media information (etc).

<sup>183</sup> OAIC, ‘Big data and privacy: a regulator’s perspective’ (10 Jun 2015 accessed 1 Sept 2015) <<https://www.oaic.gov.au/media-and-speeches/speeches/big-data-and-privacy-a-regulators-perspective>>

<sup>184</sup> Peter Sondengaard, Senior VP Gartner Research.

<sup>185</sup> Kate Mathews-Hunt, ‘CookieConsumer: Tracking online behavioural advertising in Australia’ *Computer Law & Security Review* 32(2016): 55- 90. Over 90% of global data has been generated since 2011, created by web behaviour, RFID data, location / geo data, environmental data, private/ public organisational operational data, user generated content, and research-based data: SINTEF. “Big Data, for better or worse: 90% of world’s data generated over last two years.” *ScienceDaily* (22 May 2013 accessed 2 Feb 2016) <[www.sciencedaily.com/releases/2013/05/130522085217.htm](http://www.sciencedaily.com/releases/2013/05/130522085217.htm)>

<sup>186</sup> Tom Krazit, ‘The Internet of Things Will Make Big Data Look Small’ *Forbes* (3 Mar 2-16 accessed 3 Mar 2-16) <http://fortune.com/2016/03/03/internet-data-structure/>

<sup>187</sup> A zettabyte is one sextillion bytes; that is equivalent to every person in the US taking a photo every second for a month or every letter in *War and Peace* multiplied 323 trillion times: EOP, ‘Big data’, above n 41 [2].

<sup>188</sup> This includes voluntarily-uploaded data such as over 500 million photos and 288,000 video hours uploaded daily: above n 41 [2]. Another estimate suggests 2.5 exabytes globally daily (or 30,000 times US Congress library content): TechAmerica ‘Mining the Big Data Gold Mine’ *Time News Group Advertising Feature* (2013 accessed 10 Apr 2015) <[http://www.timeincnewsgruopcustompub.com/sections/120409\\_CloudComputing.pdf](http://www.timeincnewsgruopcustompub.com/sections/120409_CloudComputing.pdf)>

<sup>189</sup> 44 zettabytes = 44 billion terabytes. The IOT will generate approximately twenty times the sum of all data existing in 2013: Verto, above n 45.

<sup>190</sup> Productivity Commission (PC), ‘Data Availability and Use’ *Draft Report* (October 2016 accessed 2 Nov 2016) <<http://www.pc.gov.au/inquiries/current/data-access/draft/data-access-draft.pdf>>

<sup>191</sup> Tesla receives real-time vehicle data flows as to driver, driving, vehicle and road information, which it uses to improve its software, improve autonomy and (anonymised) as a revenue-source.

<sup>192</sup> International Telecommunications Union -T (ITU), ‘Overview of the Internet of Things’ (15 Jun 2012 accessed 3 Mar 2016): 3 <<http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060>>

<sup>193</sup> The recent Australian Public Data Policy Statement, mandates “non-sensitive” government data is open by default; it has increased ‘discoverable resources’ from 500 to 20,000 since 2013: Malcolm Turnbull, ‘Australian Government Public Data Policy Statement’ (7 Dec 2015 accessed 30 May 2016) <<https://www.dpmc.gov.au/sites/default/files/publications/open-government-nap-consultation-print.pdf>> See also [www.opendata.gov.au](http://www.opendata.gov.au).

<sup>194</sup> In January 2015 alone, over 18 million Australians were online, viewing 28 billion webpages, over 39 million minutes. Social media use reveals 95% of Australians are amongst the 1.23 billion global users of Facebook, contributing to its 3.4 trillion tracked ‘likes’ and to the mass of ‘personal information’ shared every second around the world: above n 185.

<sup>195</sup> For example, software apps enable geolocation and other personal data collection.

<sup>196</sup> The “fifteen most powerful IOT companies” are Amazon Web Services, AT&T, Axeda, Cisco, Facebook, GE, Google, IBM, Intel, Microsoft, Oracle, SAP, Salesforce and Qualcomm: IDG UK, above n 40.

component suppliers. Like electricity,<sup>197</sup> the CIOT will be less visible but increasingly socially embedded, such that most human internet interaction will occur through “passive” smart device engagement.<sup>198</sup> Put simply, the CIOT is a data “goldmine.”<sup>199</sup>

There are no Australian statistics as to CIOT scope. But by mid-2016, 46.1%<sup>200</sup> of the world’s population and 85.1% of Australians are home internet users,<sup>201</sup> and 18.5 million cars are registered in Australia.<sup>202</sup> By inference, this represents a baseline CIOT smart home and smart car market, which can only expand with industry maturity, through improved devices, marketing and consumer value-definition. The smart sectors examined in this thesis are briefly introduced here by way of scope, to illustrate how each sector so significantly, expands the whole.

(a) *Scope: smart self*

Smart self wearables straddle two converging legal categories: fitness and therapeutic goods (smart health), but this paper focuses upon the former, which are not specifically regulated.<sup>203</sup> Devices such as watches, bands, jewellery and other ‘wearables’ collect human data as diverse as geolocation, daily steps taken, altitudinal (stair) data, heart rate, pulse, blood glucose levels, respiration, body temperature, galvanic skin response, REM, light and deep sleep quality and statistics, swim and bike tracking, kilojoules consumed and other physiological measures. Devices also seek manual inputs as to food consumption, mood, specific activities and personal goals, as well as create social-media networks via

---

<sup>197</sup> OECD, ‘Internet of Things: Seizing the Benefits and Addressing the Challenges’ (May 2016 accessed 2 Aug 2016): 5 <[http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP\(2015\)3/FINAL&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En)>

<sup>198</sup> Rose, above n 10.

<sup>199</sup> Kenneth Cukier cited in EuroActiv.com, ‘Economist editor: Big data is a goldmine for companies’ (6 May 2014 accessed 10 Apr 2015) <<http://www.euractiv.com/sections/eskills-growth/economist-editor-big-data-goldmine-companies-301933>>

<sup>200</sup> Population projection is 7.432 billion, with 3.424 billion defined as “internet users”.

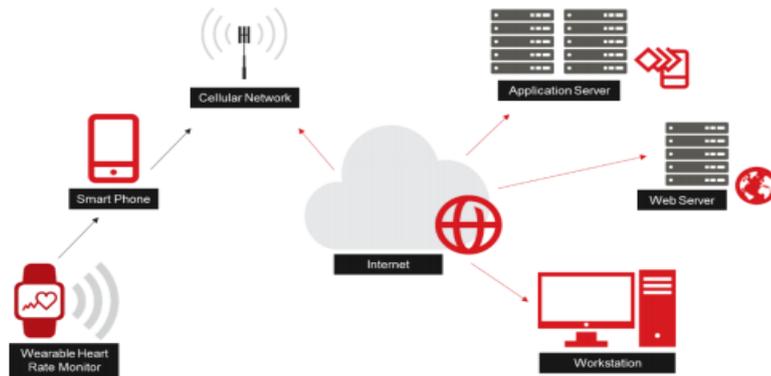
<sup>201</sup> ‘Internet users by country (2016) (accessed 10 May 2016) <http://www.internetlivestats.com/internet-users/> Note that the Sensis 2015 study showed 99% but that figure seems too high: Sensis, ‘Yellow Social Media Report’ (May 2015 accessed 29 Mar 2015) [11] <<https://www.sensis.com.au/learn/yellow-social-media-report-2014>> ABS statistics show that 12.7 million Australian internet subscribers by 2014 end: Australian Bureau of Statistics, ‘Internet Activity- Dec 2014’ <<http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/>>

<sup>202</sup> ABS, ‘9309.0 - Motor Vehicle Census, Australia’, (31 Jan 2016 accessed 2 Sept 2016) <<http://www.abs.gov.au/AUSSTATS/abs@.nsf/mf/9309.0>>

<sup>203</sup> Smart health devices are subject to therapeutic goods regulation – but smart self are not. The US FDA has an advisory: U.S. Department of Health and Human Services, Food and Drug Administration, ‘General Wellness: Policy for Low Risk Devices’ (2016 accessed 2 Nov 2016)

<<https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429674.pdf>> Such devices fall within a non-regulated Australian category at the time of writing.

social rankings, challenges and discussion.<sup>204</sup> This data is then (usually) subjected to the multiple provider transfers:<sup>205</sup>



Graphic 1.2 Simple IOT data flow  
Source: GSMA<sup>206</sup>

Smart self devices promise to revolutionise consumer health awareness by enabling continuous, real time health monitoring and analytics. Benefits include improved health outcomes through better consumer information., fitness and weight loss motivation and greater health status self- awareness and reduced life and health insurance premiums.<sup>207</sup> Device data can also through wider connectivity, provide medical information accessible by doctors and others or trigger alerts through analytics, to enable improved diagnostics and medical services.<sup>208</sup> In case of therapeutic apps, that data should be medically reliable; in contrast, smart fitness devices generally avoid that claim, though marketing representations and consumer expectation may differ. Recent cases on this issue are discussed in chapter 4.<sup>209</sup>

<sup>204</sup> Andrew Hilts, Christopher Parsons & Jeffrey Knockel, 'Every Step You Fake: A Comparative Analysis Of Fitness Tracker Privacy And Security', *Open Effect & Citizen Lab* (2 Feb 2-016 accessed 16 Aug 2016)

<[apo.org.au/files/Resource/every\\_step\\_you\\_fake.pdf](http://apo.org.au/files/Resource/every_step_you_fake.pdf)>

<sup>205</sup> As to apps, Fitbit is compatible with 37 different apps while Jawbone lists over 30: Thomas H. Davenport and John Lucker, 'Running on Data: activity trackers and the internet of things' *Deloitte Review* (26 Jan 2015 accessed 2 Apr 2016)16: 9 <<https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-16/internet-of-things-wearable-technology.html>>

<sup>206</sup> GSMA, above n 113.

<sup>207</sup> In Australia, Qantas 'Assure' offers health insurance via a third party provider which is allied to the Qantas fitness tracking program, and while premiums are not reduced, consumers are offered access to an incentivized points program, which includes recognition of their tracked success levels: <<https://www.qantaspoints.com/earn-points/qantas-assure>> In the US, one insurer provides a free Misfit flash tracker to consumers who receive health insurance discounts or credits if they meet daily fitness goals: Charles Orton-Jones, 'Ingenious ways wearables can enhance life and enterprise' *Raconteur Wearable Technology* (3 Sept 2015 accessed 2 Feb 2016) <<https://www.raconteur.net/wearable-technology>> Aside from brand enhancement and possibly commissions upon insurance sales, these schemes seem created to gather data.

<sup>208</sup> Australia has (arguably prematurely) established a national health database but controversially, has no resolved policy as to secondary use of health data and the National Digital Health Strategy is under review: Australian Digital Health Strategy, 'My Health Record' (accessed 20 Mar 2017) <<https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/content/home>>

<sup>209</sup> The most significant health data issues are security, accuracy and to whom it is accessible – discrimination is always a possibility. For example, consumers with device-detected, data-inferred health issues may face premium penalties or even

(b) *Scope: smart home*

Smart home devices promise to revolutionise consumer home management and monitoring by offering improved comfort, efficiency and security through automation, as well as increased consumer convenience, savings,<sup>210</sup> safety and sustainability.<sup>211</sup> Foreshadowing data-informed learning and AI-informed predictive capacities,<sup>212</sup> smart homes will soon “intuitively learn our habits, likes and dislikes and become tailored to our individual and changing needs...”<sup>213</sup> For the elderly or disabled, smart homes offer improved independent living, by automating home functioning, and monitoring and reporting upon occupant wellbeing. Smart homes are born by either integrated design or the gradual connection of interconnected components;<sup>214</sup> and hundreds, if not thousands, of smart home devices, are on the market,<sup>215</sup> from the banal to the eccentric.<sup>216</sup> Most are individually controlled via a smartphone-as-remote<sup>217</sup> or via branded device ‘hubs’.<sup>218</sup> For example, Google bought *Nest* for \$3.2 billion to establish its smart home ecosystem,<sup>219</sup> which is billed as self-learning, programmable and Wi-Fi enabled, operated remotely via its own and third party “Works with Nest”<sup>220</sup> smartphone apps. Interoperable *Nest* devices

---

be denied (private) health insurance. Even were health insurers not able to access such data, query whether mandatory policy disclosure obligations may (in some cases) oblige revelation of such data.

<sup>210</sup> “By 2020, the connected kitchen will contribute at least 15 percent savings in the food and beverage industry, while leveraging big data analytics”: Gartner, ‘Gartner Says by 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities’ (26 Jan 2015 accessed 3 Dec 2015)  
<<http://www.gartner.com/newsroom/id/2970017>

<sup>211</sup> Atlantic Council, ‘Smart Homes and The Internet of Things’ *Issue Brief* (30 Mar 2016 accessed 2 Jun 2016): 1  
<<http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the-internet-of-things>>

<sup>212</sup> “Living Services will intuitively learn our habits, likes and dislikes and become tailored to our individual and changing needs: Accenture, above n 24: 5.

<sup>213</sup> *Ibid.*

<sup>214</sup> ENISA, above n 34.

<sup>215</sup> Examples include smart TVs, security systems, thermostats, locks, smoke and CO2 detectors, lighting, home appliances<sup>215</sup> (fridges, washing machines, toasters, fans, blinds, dog feeders, etc), meters, wireless key finders, power outlets, wi-fi sprinklers, garage doors and scales, door locks, smart light bulbs, plant sensors and include many other electronic items. ‘Smart TVs’ run entertainment apps (such as web browsers, on-demand internet radio, video stream services) as well as stream media. TVs may include built-in video cameras, microphones and voice-gesture recognition technology: Office of the Privacy Commissioner of Canada, ‘An introduction to privacy issues with a focus on the retail and home environments’, *Research paper prepared by the Policy and Research Group* (February 2016 accessed 16 Aug 2016)  
<[https://www.priv.gc.ca/media/1808/iot\\_201602\\_e.pdf](https://www.priv.gc.ca/media/1808/iot_201602_e.pdf)>

<sup>216</sup> Postscapes, ‘Connected Home’ <<http://postscapes.com/connected-home>> For example, water filters, sofas, menstrual cups and umbrellas... readers may pick which if any, fit either category.

<sup>217</sup> Lux, above n 26.

<sup>218</sup> Hubs include (for example) Samsung’s SmartThings, Google’s Nest and (Apple’s new) HomeKit.

<sup>219</sup> Nest’s products consist of the Nest Learning thermostat, Nest protect and the Nest cam.

<sup>220</sup> This is an API or “app program interfaces” program, which is the technical method to make devices ‘talk’ to each other.

include electricity meters,<sup>221</sup> thermostats, alarm systems, appliances,<sup>222</sup> air fresheners, beds, fans, blinds, lighting, garage doors, locks, leak detectors, sprinklers, toys, baby monitors, showers, lawns,<sup>223</sup> *TrackR* for lost items, as well as offer syncing capacities with smart self devices and smart cars.<sup>224</sup> For example, smart fridges can order food,<sup>225</sup> and systems such as Amazon's *Dash* and *Echo* offer automated re-ordering systems,<sup>226</sup> where routine home purchases are approved via smartphone and made M2M.<sup>227</sup> Similarly, *Jawbone*, can tell *Nest* you are asleep so it turns down the heating, while *Mercedes* smart car geolocation can alert the oven,<sup>228</sup> lights and garage door when to operate, during the drive home. More recently, Amazon's *Echo*,<sup>229</sup> Apple's *HomeKit* and others deploy voice-enabled home assistants, but also record consumer voice communications to increase the collected data mix. For ease of operation, these devices seem likely to supersede non-voice devices in their direct consumer interaction capabilities.

(c) *Scope: smart car*

Smart cars enjoy substantial industry investment,<sup>230</sup> inter-industry partnerships and supply chains, hyperbolic market expectation and international government support. As Delphi comment:

---

<sup>221</sup> Smart metres have industry-changing potential: Victorian Government, 'Victoria's future industries new energy technologies', *Discussion Paper* (Dec 2016 accessed 2 Feb 2016) <[http://yoursay.business.vic.gov.au/futureindustries/application/files/8114/4823/4306/9186\\_dedjtr\\_vfi\\_document\\_new\\_energy\\_technologies\\_web.pdf](http://yoursay.business.vic.gov.au/futureindustries/application/files/8114/4823/4306/9186_dedjtr_vfi_document_new_energy_technologies_web.pdf)>

<sup>222</sup> For example, hot water heaters, fridges, kettles and washing machines.

<sup>223</sup> See for example, the Edyn soil sensor that claims to monitor and wirelessly stream data such as pH, nutrient content, temperature, moisture and humidity data to the cloud. The efficacy of such newer products often face very critical reviews; e.g. Michael Brown, 'Edyn smart garden probe review: A promising idea that needs time to blossom' *Techhive* (23 Jun 2015 accessed 13 Jun 2016) <<http://www.techhive.com/article/2939022/edyn-smart-garden-probe-review-a-promising-idea-that-falls-short-on-delivery.html>>. Others include Parrot's Flower Power, Rachio and Oso's PlantLink.

<sup>224</sup> BBC, 'Apple stops selling Nest products in its US stores' (24 Jul 2015 accessed 2 Jun 2016) <<http://www.bbc.com/news/technology-33655417>>

<sup>225</sup> Keith Wagstaff, 'Out of Milk? LG's new smart fridge will let you know' *NBC News* (7 May 2014 accessed 4 Mar 2016) <<http://www.nbcnews.com/tech/gift-guide/out-milk-lgs-new-smart-fridge-will-let-you-know-n99531>>

<sup>226</sup> <https://www.amazon.com/Dash-Buttons/b?ie=UTF8&node=10667898011>

<sup>227</sup> Note this is not M2M contracting; which involves no consumer involvement. But as consumer confidence grows, the transaction 'approval' step might be discarded; reflecting for example, current practices as to direct debiting bills.

<sup>228</sup> Interestingly, Australian regulation does not permit an oven being turned on remotely: Jennifer Dudley-Nicholson, 'The Internet of Things is coming to Australia: Samsung plans to launch SmartThings Down Under' *news.com.au* (23 Sept 2015 accessed 20 Mar 2016) <<http://www.news.com.au/technology/home-entertainment/the-internet-of-things-is-coming-to-australia-samsung-plans-to-launch-smarthings-down-under/news-story/4d85fb3c24d6446543f104df6f5abb3e>>

<sup>229</sup> <<https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E>> Alexa can play music from Prime Music, Spotify, Pandora, iHeartRadio, TuneIn, and more; answers questions, reads audiobooks and the news, reports traffic and weather, gives local business information, provides sports scores and schedules, (etc) using the Alexa Voice Service, controls lights, switches, and thermostats with compatible WeMo, Philips Hue, Samsung SmartThings, Wink, Insteon, Nest, and ecobee smart home devices. New features are added regularly.

<sup>230</sup> General Motors purchased a self-driving startup called Cruise for \$600M and spent half a billion dollars on ride-share company Lyft in January 2016: Alex Davies, 'The Startup that could help GM beat Google to the Self-driving car' *WIRED* (11 Aug 2015 accessed 13 Aug 2016) <<https://www.wired.com/2016/08/gm-cruise-automation-self-driving-vogt/>>

*"This trend is being driven by several factors, including regulators wanting fewer injuries and fatalities, city planners who want reduced congestion and reduced need for parking, and commuters want less traffic and the ability to more productively use their time during their commute."<sup>231</sup>*

Smart cars offer consumers safety, economic, environmental (energy), mobility and land use benefits.<sup>232</sup> Safety is their greatest public policy attraction:<sup>233</sup> globally, 1.25 million fatalities and 20- 50 million injuries occur annually.<sup>234</sup> In Australia, 600 thousand car accidents annually cost the economy \$27 billion,<sup>235</sup> 1200 Australians die and an estimated 32,500 people are seriously injured.<sup>236</sup> "Human error" is by far the dominant cause of accidents,<sup>237</sup> and fully autonomous smart cars will largely 'solve' this problem<sup>238</sup> - and more. Conventional driving entails driver costs,<sup>239</sup> and substantial negative externalities.<sup>240</sup> Smart car safety will increase with autonomy and C-ITS use,<sup>241</sup> as the fleet<sup>242</sup> changes over, and as road

---

<sup>231</sup> Andrew J. Hawkins, 'Delphi and Mobileye are teaming up to build a self-driving system by 2019' *The VERGE* (23 Aug 2016 accessed 15 Aug 2016) < <http://www.theverge.com/2016/8/23/12603624/delphi-mobileye-self-driving-autonomous-car-2019>>

<sup>232</sup> Rand Corporation, 'Autonomous vehicle technology: A Guide for Policymakers' by James M. Anderson, Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras, Oluwatobi A. Oluwatola, (accessed 2 Feb 2016) <[http://www.rand.org/content/dam/rand/pubs/research\\_reports/RR400/RR443-2/RAND\\_RR443-2.pdf](http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-2/RAND_RR443-2.pdf)>

<sup>233</sup> Car & Driver writes with some irony: "Brainless driving is closing in on us like a meteorite because of its potential to avoid accidents. Sadly, we are a nation of mediocre drivers, distracted ... and few of us are able to use the accident-avoidance capabilities built into every new car. Our driving errors cause crashes, injuries, and fatalities.": Don Sherman, 'Semi-Autonomous Cars Compared! Tesla Model S vs. BMW 750i, Infiniti Q50S, and Mercedes-Benz S65 AMG' *Car & Driver* (2 Feb 2016 accessed 3 Jun 2017) <<http://www.caranddriver.com/features/semi-autonomous-cars-compared-tesla-vs-bmw-mercedes-and-infiniti-feature>>

<sup>234</sup> WHO, 'Road Traffic injuries' (May 2016 accessed 10 Jun 2016) <<http://www.who.int/mediacentre/factsheets/fs358/en/>> Note that there are no clear global estimates of the costs of injury, but 2010 research suggests a 3% GNP cost, rising to 5% in certain lower and middle-income countries.

<sup>235</sup> Australian Automobile Association (AAA), 'Benchmarking the Performance of the National Road Safety Strategy June 2016' (July 2016 accessed 20 Aug 2016):5 <<http://www.aaa.asn.au/news-and-publications/reports/>> Crash reduction reduces the emotional toll and societal costs – fatalities, personal injury, medical and rehabilitation costs, work-days lost, property damage and so on, – that total \$billions lost annually.

<sup>236</sup> No statistics exist: Joshua Dowling, 'Australian road toll hits 69-year low but serious injuries from car crashes are rising' *news.com.au* (19 Jan 2015 accessed 20 Jul 2016) <<http://www.news.com.au/technology/innovation/motoring/australian-road-toll-hits-69year-low-but-serious-injuries-from-car-crashes-are-rising/news-story/24a1ad61b2bccea58af36384ee15ecb>>

<sup>237</sup> A MUARC Study identifies driver error - intoxication (13.5%), falling asleep (11.8%), fatigue (10.9%) as the dominant causation - the US Department of Transport claims (questionably) that 94% of accidents are attributable to driver error: Vanessa Beanland, Michael Fitzharris, Kristie L. Young, Michael G. Lenné, Corrigendum to "Driver inattention and driver distraction in serious casualty crashes: Data from the Australian National Crash In-depth Study" *Accid. Anal. Prev.* 54C (2013) 99–107 [626]. The remaining 6% are attributed to poor maintenance and environmental error. Product defects are the "unique cause" in less than 1% of accidents.

<sup>238</sup> Google research experience is that with a mixed fleet, baseline accidents will remain "unavoidable", due to human error causing accidents and challenging smart intelligence adaptability.

<sup>239</sup> For example, a Toyota Corolla costs \$152.79 per week and Holden Commodore costs 214.42 per week, or \$7,945 and \$11,149 per annum over 5 years: RACV, '2016 Motoring Cost Report', (2016 accessed 2 Aug 2016) <http://www.racv.com.au/wps/wcm/connect/racv/internet/primary/my+car/Operating+Costs> but in the UK, average car use is approximately only 5% daily: AA, *Motoring Costs, UK* (2014 accessed 2 Jan 2016) < <http://www.theaa.com/resources/Documents/pdf/motoring-advice/running-costs/diesel2014.pdf>>

<sup>240</sup> Rand, above n 232.

<sup>241</sup> These include V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) communications technology.

<sup>242</sup> This is currently at 10.2 years. As such there will be some 'changeover period' unless people are incentivized to adopt smart cars or if a 'bolt-on' system can be utilised.

infrastructure is upgraded. Other benefits include: improved driver convenience, services and entertainment, increased traffic efficiency, and increased car ownership and sharing economy value – a vehicle might independently uber-it by day until its owner wants it to leave work, for example. It also promises less congested<sup>243</sup> and greener traffic,<sup>244</sup> and reduced consumer insurance premiums as liability shifts to manufacturers.<sup>245</sup> The aged, disabled, young and immobile will enjoy improved quality of life. Aside from reducing the significant human and societal<sup>246</sup> road toll cost, all these factors offer substantial economic and social benefits, which address negative externalities and pressing public policy issues: from the environment, to reducing health costs, improving recall efficacy,<sup>247</sup> to improved transport and product safety. Further, there is concern that current safety strategies are flatlining: the 2011 target to reduce road deaths by 30%+ by 2020, sits at 6.1% by 2016 end.<sup>248</sup>

Consumer experience promises reduced driving stress, greater convenience - and information. Just-in-time data about vehicle safety, operation, maintenance, road systems, traffic; as well as a preference-driven car environment, much like one giant smartphone. Google's proprietary smart car algorithm is described as "...the connective tissue that combines the software, data, sensors and physical asset into

---

<sup>243</sup> Rand, above n 232.

<sup>244</sup> V2V and C-ITS will utilise real-time data analysis to reduce traffic congestion, lower carbon emissions and increase transport efficiency through route selection. Vehicle control systems which manage acceleration in traffic flow will reduce fuel consumption and congestion caused by accidents on-road, and consequently improve air quality and decrease emissions.

<sup>245</sup> Thatcham Research estimates that premiums could fall by 50% by 2025 and 80% by 2040. Although claims will fall, insurer revenues may shrink: Neha Jain, James O'Reilly & Nicholas Silk, 'Driverless Cars: Insurers Cannot be Asleep at the Wheel' *Bank Underground* (19 Jun 2015 accessed 2 Aug 2016) (<https://bankunderground.co.uk/2015/06/19/driverless-cars-insurers-cannot-be-asleep-at-the-wheel/>)

<sup>246</sup> The lead 2010 US National Highway Traffic Safety Administration study suggests that the societal costs significantly exceed the economic harm: societal harm totals \$836 billion, identifying 71% of that harm to be "lost quality of life" and 29% (\$242 billion), to be from more direct economic impacts. Economic impacts of 242 billion include lost productivity (\$77.4B) and costs such as: medical (\$23.4B), legal, court, emergency service costs, insurance costs, congestion impacts (\$28B), property damage (\$76.1B), and workplace losses. At page 9, the Report states "Most researchers agree that the value of fatal risk reduction falls in the range of \$5 to \$15 million per life saved" and evaluates comprehensive costs (e.g. economic impacts and lost quality-of-life) using the 2013 DOT risk reduction value guidance.: L. J. Blincoe, T.R. Miller, E. Zaloshnja, E., & B.A. Lawrence, 'The economic and societal impact of motor vehicle crashes, 2010' *NHTSA* (Revised May 2015) (Report No. DOT HS 812 013). Washington, DC <<https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812013>>

<sup>247</sup> The speed, convenience and reduced cost of over-the-air software updates will greatly increase recall success rates. Note however that more traditional product defects – a defective tyre for example, will still require the car to be physically rectified, subject to robotic repairs. The average Australian consumer goods recall return rate is only 56.75%. Of 10,000 recalls over 23 years, car recalls comprise 19%: ACCC, 'Review of the Australian product safety recalls system' (2010 accessed 3 Apr 2016): 16 <

<https://www.accc.gov.au/system/files/Review%20of%20the%20Australian%20product%20safety%20recalls%20system.pdf>>

<sup>248</sup> Ibid. In 2015-16 financial year, fatalities totalled 1,269. Australian figures (0.005% of the population) are dwarfed by US figures (0.012%): the US National Safety Council estimated 38,300 American fatalities in 2015 with 4.4 million "sustained injuries" resulting in medical consultations. The cost totalled \$412.1 billion: (US) National Safety Council, 'Motor Vehicle deaths Increase by largest Percent in 50 Years' (17 Feb 2016 accessed 5 May 2016)

<<http://www.nsc.org/Connect/NSCNewsReleases/Lists/Posts/Post.aspx?List=1f2e4535-5dc3-45d6-b190-9b49c7229931&ID=103&var=hppress&Web=36d1832e-7bc3-4029-98a1-317c5cd5c625>> The NSC believes an increase in miles driven of 3.5% is behind an 8% increase in fatalities year-to-year.

a true leap forward in transportation.”<sup>249</sup> That leap is already underway, despite some regulatory disarray: Tesla’s Model S is level 3- 4, and others are currently on-road,<sup>250</sup> and in test phase. In the US, Google have 58 cars driving 20,000 miles a week,<sup>251</sup> Uber are on-road in Pittsburgh,<sup>252</sup> and Tesla stream over one million miles of data every ten hours.<sup>253</sup> Software giants Baidu<sup>254</sup> and Apple<sup>255</sup> plan smart car releases by 2019, while Delphi and MobilEye plan an off-the-shelf self-driving system by 2019,<sup>256</sup> Google, Nissan and Mercedes plan for 2020,<sup>257</sup> with Ford and BMW for 2021.<sup>258</sup> Tesla wunderkind Elon Musk describes full autonomy as ‘problem- solved’,<sup>259</sup> and claims that subject to regulation, their Model X smart car will be on road between 2018- 2021.<sup>260</sup> It is a Goliath’s race to see who first puts a fully autonomous vehicle into the consumer marketplace, one which pits silicon valley against traditional ‘auto’ manufacturers, but which may ultimately, find its resolution in alliance over competition.<sup>261</sup>

## 1.2.2 Scale

*“Why the IOT heralds a new era of computing is a matter of math...”<sup>262</sup>*

<sup>249</sup> Peter Sondergaard, ‘Big Data Fades to the Algorithm Economy’ *Gartner Inc., Forbes* (14 Aug 2015 accessed 6 Dec 2015) <<http://www.forbes.com/sites/gartnergroup/2015/08/14/big-data-fades-to-the-algorithm-economy/print/>>

<sup>250</sup> Examples include the top range vehicles for most prestige marques, though there is no specific ‘level’ ranking: Sherman, above n 233.

<sup>251</sup> Waymo (formerly Alphabet/ Google autonomous vehicle project) drove 2 million autonomous miles by October 2016.

<sup>252</sup> Samuel Gibbs, ‘Uber riders to be able to hail self-driving cars for the first time’ *The Guardian* (19 Aug 2016 accessed 21 Aug 2016) <https://www.theguardian.com/technology/2016/aug/18/uber-riders-self-driving-cars;>

<sup>253</sup> Michael J. Koren, ‘Tesla has 780 million miles of driving data, and adds another million every 10 hours’ *Quartz* (May 28, 2016 accessed 20 Nov 2016) <<http://qz.com/694520/tesla-has-780-million-miles-of-driving-data-and-adds-another-million-every-10-hours/>> In May 2016, Tesla had driver data covering 780 million miles over 18 months.

<sup>254</sup> Baidu are a Chinese technology company. In March 2016, their plan was to put “commercial, self-driving cars on the roads by 2018”: Andrew Ng & Yuanqing Lin, ‘Self-driving Cars won’t work until we change our roads – and attitudes’ *WIRED* (15 Mar 2016 accessed 2 Aug 2016) < <https://www.wired.com/2016/03/self-driving-cars-wont-work-change-roads-attitudes/>>

<sup>255</sup> Alex Davies, ‘Apple better be ready for the mad world of Car Regulations’ *WIRED* (21 Sept 2015 accessed 2 Aug 2016) < <https://www.wired.com/2015/09/apple-better-ready-mad-world-car-regulations/>>

<sup>256</sup> The system is SAE level 4. The CSLP system is radar- and camera-centric, with LIDAR as a redundant sensor. Mobileye claim this will reduce costs to “only a few thousand dollars”: Hawkins, above n 231.

<sup>257</sup> Danny Yadron, ‘Two years until self-driving cars are on the road – is Elon Musk right?’ *The Guardian* (3 Jun 2016 accessed 5 Jun 2016) <<https://www.theguardian.com/technology/2016/jun/02/self-driving-car-elon-musk-tech-predictions-tesla-google>>

<sup>258</sup> Hawkins, above n 231.

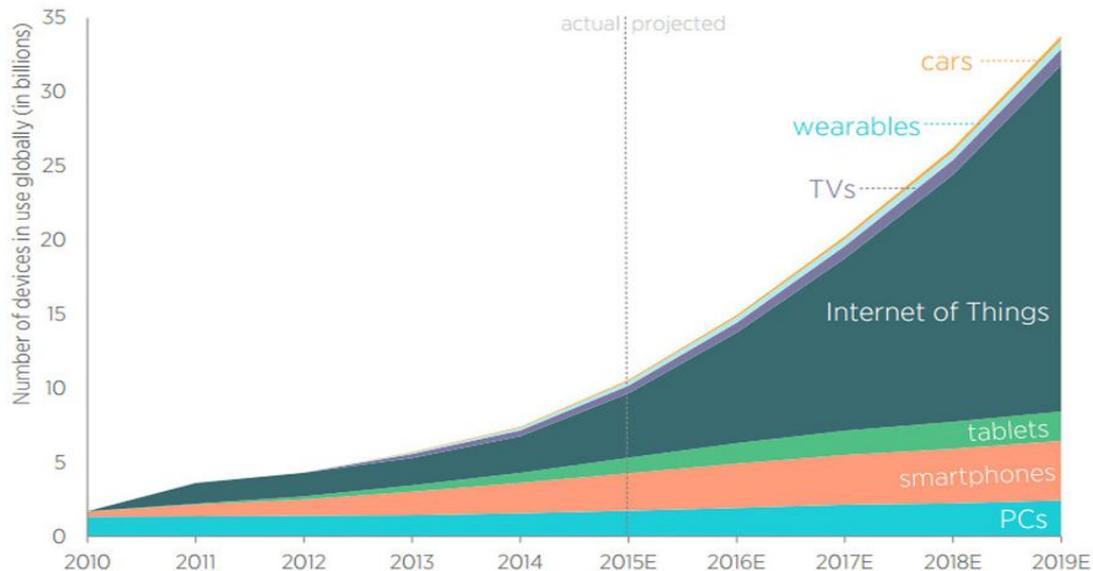
<sup>259</sup> Yadron, above n 257; Mike Ramsey, ‘Tesla’s Elon Musk says autonomous driving not all that hard to achieve’ *WSJ* (17 Mar 2015 accessed 2 Aug 2016) < <http://www.wsj.com/articles/teslas-elon-musk-says-autonomous-driving-not-all-that-hard-to-achieve-1426624848>>

<sup>260</sup> Elon Musk cited in Fred Lambert, ‘Tesla CEO Elon Musk drops his prediction of full autonomous driving from 3 years to just 2’ (21 Dec 2015 accessed 2 Aug 2015) <https://electrek.co/2015/12/21/tesla-ceo-elon-musk-drops-prediction-full-autonomous-driving-from-3-years-to-2/>; Danny Yadron, above n 257. By mid 2016, Ford predicted a five-year time frame for its fully autonomous fleet on road: Alex Davies, ‘Ford say’s it’ll have a fleet of fully autonomous cars in just 5 years’ *WIRED* (16 Aug 2016 accessed 20 Aug 2016) <<https://www.wired.com/2016/08/ford-autonomous-vehicles-2021/>>

<sup>261</sup> Recent Navigant research suggests that traditional manufacturers are ahead of IT companies as to autonomous vehicle development, see Alex Davies, ‘Detroit is stopping Silicon Valley in the self-driving car race’ *WIRED* (3 Apr 2017 accessed 4 Apr 2017) < [https://www.wired.com/2017/04/detroit-stomping-silicon-valley-self-driving-car-race/?mbid=nl\\_4317\\_p2&CNDID=>](https://www.wired.com/2017/04/detroit-stomping-silicon-valley-self-driving-car-race/?mbid=nl_4317_p2&CNDID=>)

<sup>262</sup> IDC, above n 21.

The number of connected devices in a rapidly expanding and changing international ecosystem poses significant challenges technically (infrastructure, stability, capacity, and resilience, etc.)<sup>263</sup> but also, in terms of policy, regulation and governance.<sup>264</sup> The scale is hitherto unimaginable: IOT projections are “monumental”,<sup>265</sup> “at the peak of inflated expectations”,<sup>266</sup> “staggering”,<sup>267</sup> and possibly, “ridiculous”.<sup>268</sup> From one connected toaster (1990),<sup>269</sup> to devices exceeding the global population (2017),<sup>270</sup> and somewhere between six to ten billion today,<sup>271</sup> the growth and future expectation, is exponential:



Source: John Greenough, “The Internet of Everything 2015,” *Business Insider Intelligence*. Produced by Adam Thierer and Andrea Castillo, Mercatus Center at George Mason University, 2015.

Graphic 1.3  
Source: Adam Thierer & Andre O’Sullivan<sup>272</sup>

<sup>263</sup> Communications Alliance, above n 119.

<sup>264</sup> For some important early articles, see Weber, above n 69; Weber, above n 87.

<sup>265</sup> Link Lab, ‘16 Ridiculous Internet of Things Statistics as we head into 2016’ (2 Dec 2015 accessed 11 Apr 2016) <<http://www.link-labs.com/internet-of-things-statistics-2016/>>

<sup>266</sup> Gartner, above n 22. This means that early publicity produces success stories — though often scores of failures.

<sup>267</sup> Syed Zaeem Hosain ‘Reality Check: 50B IoT devices connected by 2020 – beyond the hype and into reality’ *RCR Wireless News* (28 Jun 2016 accessed 2 Aug 2016) <<http://www.rcrwireless.com/20160628/opinion/reality-check-50b-iot-devices-connected-2020-beyond-hype-reality-tag10>>

<sup>268</sup> Link Lab, above n 265.

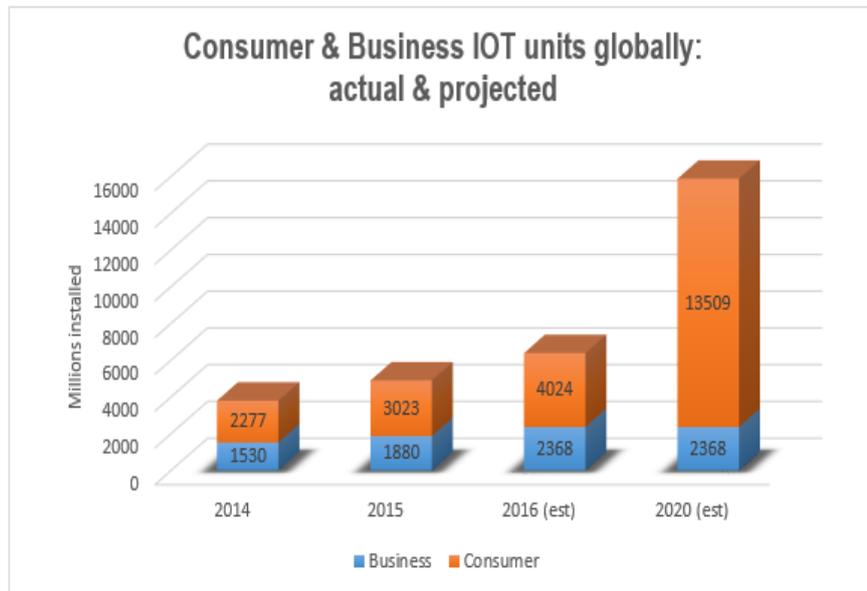
<sup>269</sup> Created by John Romkey, the toaster that could be turned on and off over the Internet.

<sup>270</sup> Gartner (2017) report 3.96 billion consumer devices in 2016 and a projected 5.2 billion in 2017. Total IOT devices are projected at 8.38 billion by year end: Liam Tung, ‘IoT devices will outnumber the world’s population this year for the first time’ *ZDNet* (7 Feb 2017 accessed 26 Feb 2017) <<http://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/>>

<sup>271</sup> ‘Internet of Everything Market Tracker’ in ABI Research, ‘The Internet of Things will drive Wireless Connected devices to 40.9 Billion in 2020’ Press Release (20 Aug 2014 accessed 26 Mar 2016) <<https://www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect/>>

<sup>272</sup> Adam Thierer & Andre O’Sullivan, ‘Projecting the Growth and Economic Impact of the Internet of Things’ *Mercatus Centre* (15 Jun 2015 accessed 25 September 2017) <<https://www.mercatus.org/publication/projecting-growth-and-economic-impact-internet-things>>

Respected analysts estimate between 15<sup>273</sup> and 75 billion<sup>274</sup> connected devices globally by 2020,<sup>275</sup> and Statista project a 30% CIOT growth rate to 13.5 billion devices globally by 2020.<sup>276</sup>



Graphic 1.4 Consumer & business IOT units globally  
Source: author using adapted Statista data<sup>277</sup>

<sup>273</sup> See Statista, 'Internet of things units installed base worldwide by category from 2014 to 2016 and in 2020 (in million units)' (2016 accessed 20 Jun 2016) < <http://www.statista.com/statistics/485203/iot-units-installed-base-by-category-worldwide/>>; Gartner are also commonly cited and predict 26B units by 2020: Gartner, 'Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020' (12 December 2013 accessed 3 Mar 2016) <<http://www.gartner.com/newsroom/id/2636073>

<sup>274</sup> Morgan Stanley cited in Hosain, above 267.

<sup>275</sup> Analysts use differing methodologies and definitions, which (partly) explains the disparities. For example: IBM (1 trillion by 2015), Ericsson (50B), Morgan Stanley (75B), Intel (31B), Cisco (40B), ABI Research (35B), IDC (31.8B), Gartner (19B excluding smartphones), Machine Research (7.2B M2M only), BII (23.3 B). Sources: ABI Research, above n 273; Irena Bojanova, 'IoT and the ever expanding web' *IEEE Computer Society* (14 Jul 2015 accessed 21 Mar 2016) < <https://www.computer.org/portal/web/sensing-iot/content?g=53926943&type=article&urlTitle=iot-and-the-ever-expanding-web->>>; Gartner, above n 273. This is thirty times the 0.9 billion installed in 2009, and as a result of their definitions, excludes a projected 7.3 billion market in PCs, tablets and smartphones; Intel, 'A Guide to the Internet of Things Infographic' (2014 accessed 11 Apr 2016) < <http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html>>. See also Adam Thierer and Andrea Castillo, 'Projecting the Growth and Economic Impact of the Internet of Things' *Mercatus Center* (15 Jun 2015 accessed 3 Mar 2016) <http://mercatus.org/print/1594637> and Hosain above n 267.

<sup>276</sup> There are no Australian CIOT projections; but taking smart meters as an example, 94 million were shipped worldwide in 2014, with projections to 1.1 billion by 2020: Statista, 'Smart Home' (2016 accessed 30 Jun 2016) <<https://www.statista.com/outlook/279/100/smart-home/worldwide#>>

<sup>277</sup> Statista, above n 273 and Ibid.

(a) *Scale: smart self:*

By March 2015, around 20.8 million people owned a Fitbit globally.<sup>278</sup> Telsyte estimate 14% or 3.5 million Australians wear a smart wearable device, and forecast growth to 37% by 2020.<sup>279</sup> Wearables (implantables and ingestibles) are by far the most visibly adopted, used, purchased and commercially successful CIOT devices: from smart fitness,<sup>280</sup> to smart watches, smart glasses, ‘hearables’, head-mounted displays,<sup>281</sup> smart jewellery<sup>282</sup> and smart clothes.<sup>283</sup> A *Fitbit* can track steps, kilojoules and sleep patterns, and leads a billion dollar industry of over fifty brands<sup>284</sup> tracking fitness and health data ranging from steps to heart rates, blood pressure,<sup>285</sup> temperature, haemoglobin levels,<sup>286</sup> blood alcohol levels,<sup>287</sup>

---

<sup>278</sup> “As of March 31, 2015, we have sold over 20.8 million devices since inception. According to The NPD Group, we held the leading position in the U.S. fitness activity tracker market, with a 68% share, by dollars, in 2014”: United States Securities and Exchange Commission, Fitbit Inc., Form S-1 Registration Statement (2015 accessed 31 Mar 216) (<<http://www.sec.gov/Archives/edgar/data/1447599/000119312515176980/d875679ds1.htm>>

<sup>279</sup> Telsyte, above n 30. Examples included “Adidas, Apple, Asus, Fitbit, Garmin, Huawei, Jawbone, LG, Microsoft, Motorola, Nike, Pebble, Samsung, Sony, TomTom and others.”

<sup>280</sup> Market range (with features in brackets) includes: Fitbit Blaze (Step tracking, sleep monitoring, 24/7 heart rate monitoring) or Alta, Garmin Vivosmart HR+ (Steps, sleep monitoring, 24/7 heart rate monitoring, GPS) , Garmin Vivoactive HR (Daily steps, 24/7 heart rate, GPS run/bike/golf tracking, notifications.), Jawbone UP2 (Step tracking, sleep monitoring, smart alarm) and UP3 (monitors bpm, respiration rate, body temperature and galvanic skin response, it can give you your REM, light and deep sleep stats - Heart rate, steps, sleep) , Misfit Shine 2 (Step tracking, sleep monitoring, smartphone notifications, swim tracking), Moov Now (Steps, sleep, advanced sports coaching, run/bike tracking); Xiaomi Mi Band Pulse (HR tracking, steps, sleep, smart alarms, incoming call alerts); Samsung Gear Fit2 ( Steps, sleep, GPS and optical heart rate). For fashionistas, the Misfit Swarovski Shine (Daily steps, sleep monitoring and calorie counting) is remarkable; and for smartwatches, Swiss watch manufacturers such as Mondaine Helventica No 1 Smart (Steps, sleep, long battery life) and Withings Activite Steel (Steps, sleep, calories, alarm) are traditional but smart. For those who dislike a wrist-worn tracker, there are a range of ‘clip-ons’ such as the Jawbone UP Move (Steps, sleep, basic sports tracking). See Wareable, ‘Fitness trackers’ <<http://www.wareable.com/fitness-trackers>>

<sup>281</sup> HMDs include virtual reality (gaming) devices such as Oculus Rift, HTC Vive, Sony PlayStation VR, and Microsoft HoloLens. HMD uses include equipment repair, inspections, maintenance; as well as viewing instructions and directions while performing a task hands free. The technology also enables car driving simulators, travel and retail experiences and any other application in which placing the consumer ‘there’ has a tangible impact. Lexus uses a driving simulator to test safety features: Orton-Jones, above n 207.

<sup>282</sup> ‘Leaf’ is a women’s health tracker which monitors activity (steps taken and calories burned), mindfulness (meditation), sleep (movement, duration, quality) and menstrual cycle (period tracker, fertility calendar) and has a six month battery: BellaBeat, ‘Leaf’ <<https://www.bellabeat.com/>>

<sup>283</sup> Examples include: the Mimo ‘smart onesie’ analyses a baby’s respiration rate, movement, temperature and sleep patterns: <http://shop.mimobaby.com/products/mimo-smart-baby-monitor>; Spinall towels and bikinis monitor sun exposure and remind users to reapply their sunscreen: Scott R. Peppet, ‘Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent’ *Texas Law Review* (2104) 93 (1) 85- 178: 88; Orton-Jones, above n 207: 5. Sensoree’s GER Mood Sweater measures galvanic skin response and depicts emotion via coloured lights - it is designed for Alzheimer patients to ‘verbalse’ their emotions and may improve care and carer workplace safety.

<sup>284</sup> This example is drawn from those on sale at the Rebel website on 18 April 2016: see <<http://www.rebelsport.com.au/store/heart-rate-monitors/heart-rate-monitors-watches/41201?page=1&pageSize=12&sort=-ProductSummaryViewsWeighted%2C-ProductSummaryViewsTotal>>

<sup>285</sup> Withings cuff will monitor and graph blood pressure: <<https://www.withings.com/eu/en/products/blood-pressure-monitor>>

<sup>286</sup> Scanadu Scout can measure temperature, heart rate and haemoglobin levels <<https://www.scanadu.com/devices.html>>

<sup>287</sup> Breathometer was withdrawn after an FTC action as to its (in)accuracy (discussed supra) so the company is focussing upon its smart toothbrush MINT: Jonah Comstock, ‘FTC: Shark Tank star Breathometer must offer full refunds for inaccurate smartphone breathalyzer’ *mobihealthnews* (24 Jan 2017 accessed 22 Feb 2017) <<http://www.mobihealthnews.com/content/ftc-shark-tank-star-breathometer-must-offer-full-refunds-inaccurate-smartphone-breathalyzer>>

oral health,<sup>288</sup> blood glucose levels,<sup>289</sup> offer GPS speed, distance and route tracking,<sup>290</sup> to women's fertility and PMS.<sup>291</sup> Training devices use real time "kinetic feedback"<sup>292</sup> to detect acceleration, jump height, speed, spin and ball strike point,<sup>293</sup> record work-out data, prescribe training plans, as well as calories and work-out intensity.<sup>294</sup> In 2016, Gartner forecast 18.4% growth in worldwide sales, to reach 274.6 million wearable electronic devices.<sup>295</sup> Forecast revenue is \$28.7 billion<sup>296</sup> and fitness wearables continue to increase in popularity due to growing smart watch sales and improving functionality.<sup>297</sup>

(b) *Scale: smart home*

In Australia, smart homes are on the cusp. So, there are no statistics<sup>298</sup> and few predictions, save for *Telsyte's* estimate for smart household device growth from 9<sup>299</sup> to 28.7 by 2020,<sup>300</sup> which roughly equates to 25 million smart home devices nationally in two short years.<sup>301</sup> Frost & Sullivan predict the smart home

---

<sup>288</sup> iBGStar <<http://www.bgstar.com.au/web/ibgstar>>

<sup>289</sup> Glow <<https://glowing.com/glow>>

<sup>290</sup> Adidas offer a miCoach Smart Watch Run with music, heart rate sensor, recorded work-out data, training plans together with for runners; C-Cell tracks heart rate, acceleration and jump height; their heart rate monitor measures calories and work-out intensity and their Smart Ball provides "instant feedback on the speed, spin and strike point of dead ball kicks".

<sup>291</sup> Glow monitors via thermometer devices and analytic apps. Kindara is another fertility app which is essentially a "smart" rhythm method via IOT thermometers, and are the second most downloaded apps on itunes.

<sup>292</sup> For example, Adidas Smart Ball provides "instant feedback on the speed, spin and strike point of dead ball kicks": Adidas, 'Fit Smart' (n.d. accessed 17 Apr 2016) <<http://www.adidas.com.au/micoach>> Others include LifeBEAM bike helmet which tracks blood flow, oxygen saturation and heart rate for cyclists. Sensors are now in shoes, racquets and golf clubs – which all measure and monitor performance: Stephen Pritchard, 'The Internet of things is revolutionizing the world of sport' *The Guardian* (2 Mar 2015 accessed 17 Apr 2016) <<https://www.theguardian.com/technology/2015/mar/02/internet-of-things-sport-six-nations>>

<sup>293</sup> Adidas miCoach Smart Watch Run.

<sup>294</sup> Adidas C-Cell tracks heart rate, acceleration and jump height; their heart rate monitor measures calories and work-out intensity

<sup>295</sup> Note this still lags behind smartphone sales which are projected to reach \$374 million in 2016: Gartner, "Gartner Says Worldwide Wearable Devices Sales to Grow 18.4 Percent in 2016" Press Release (2 Feb 2016 accessed 29 Mar 2016) <<http://www.gartner.com/newsroom/id/3198018>>

<sup>296</sup> Ibid.

<sup>297</sup> Gartner predict that smartwatch sales will overtake smart bands significantly 2016-17, subject to the latter developing mobile payments, safety, access, health and wellness, to increase their market penetration: Ibid.

<sup>298</sup> As previously noted, there may be paid reports including such data unavailable to the author.

<sup>299</sup> The figures exclude: home computers (1.9), smartphones (1.9) and tablets (1.3), but include game consoles (0.7), smart TV (0.3), toys (0.2), smart appliances (0.1) and other (1.6). For contrast, in the US, *Altimeter* found that 75% of Americans own a smartphone containing 7- 14 sensors, and 70% own at least one other CIOT device, with 87% owning three or fewer such devices - including smart game consoles (28%), smart TV (23%), wearables (7%), connected car or appliance (4%), home automation (3%) and other 'smart' product (15%).

<sup>300</sup> Telsyte, 'Internet Uninterrupted Australian households of the Digital Future' (2015 accessed 3 Dec 2015):

<http://www.nbnco.com.au/content/dam/nbnco2/documents/Internet%20Uninterrupted%20Australian%20Households%20of%20the%20Connected%20Future.pdf>>

<sup>301</sup> The calculation uses ABS statistics as to household numbers (9.2 in 2016 to 10.1M in 2021) multiplied by 24: ABS, 'Household projections' (2015 accessed 2 Jun 2016) <

<http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/3236.0Main%20Features42011%20to%202036?opendocument&abname=Summary&prodno=3236.0&issue=2011%20to%202036&num=&view=>>. Telsyte predict that value chain vendors will include manufacturers, retailers, ISPs, cloud software providers, utilities, electricians and security consultants.

market will reach \$200 million by 2020,<sup>302</sup> while Telsyte add (broad) value-chain ‘services’ to predict growth to \$3.2 billion by 2019.<sup>303</sup> In scale, Australia’s market is nascent: *SmartThings* and *Google Nest* will launch in 2017, bringing more of a global smart home industry projected to reach US\$53.45 billion in 2022.<sup>304</sup> Voice assistants are the latest trend, with a recent report predicting 33 million in US homes by 2017 end.<sup>305</sup>

(c) *Scale: smart car*

Valued at \$18 billion in 2012, the smart car market is predicted to triple by 2018. Predictions are that 20% of cars will be internet-connected by 2020,<sup>306</sup> and by 2025, all new cars will exhibit IOT connectivity through the ‘black box’ Event Data Recorder (EDR), C-ITS and/ or telematics.<sup>307</sup> There are no ‘smart car’ statistics for Australia yet: though most new models exhibit connectivity and premium marques have level 3 and (possibly) 4 autonomous vehicles on road. Estimates suggest 583- 600 Tesla vehicles were on-road in Australia by January 2016,<sup>308</sup> with around 150,000 sold internationally at 2016 end.<sup>309</sup> Smart car connectivity is also an important feature as to scale: these systems record vehicle data, “talk” together, alert drivers to accidents, communicate with road infrastructure such as traffic lights as to traffic updates and re-routing alerts – as well as monitor the driving and vehicle function, communicate with the

---

<sup>302</sup> Stuart Corner, ‘Aussie IoT in the home spend tipped to top \$200m in 2020’ (6 November 2015 accessed 2 Feb 2016) <https://www.iotaustralia.org.au/2015/11/06/iot-facts-and-forecasts/aussie-iot-in-the-home-spend-tipped-to-top-200m-in-2020/> citing Frost & Sullivan study.

<sup>303</sup> Telsyte, above n 300. ‘The CIOT value chain includes ISPs, manufacturers, retailers, (cloud) software-as-a-service providers, utilities, tradespeople and consultants.

<sup>304</sup> 14.5% CAGR between 2017- 2022: Zion Market Research, ‘Smart Home Market (Smart Kitchen, Security & Access Control, Lighting Control, Home Healthcare, HVAC Control and Others): Global Industry Perspective, Comprehensive Analysis and Forecast, 2016-2022’, (18 Jan 2017 accessed 2 Mar 2017) <https://www.zionmarketresearch.com/report/smart-home-market>

<sup>305</sup> Voicelabs, ‘The 2017 Voice Report’ (15 Jan 2017 accessed 2 Mar 2017) <http://voicelabs.co/2017/01/15/the-2017-voice-report/>

<sup>306</sup> This is 20% of the fleet: Gartner, above n 210, cited in *BusinessWire*, ‘Automotive Industry Adopts GSMA Embedded Sim Specification To Accelerate Connected Car Market’ (10 Feb 2016 accessed 3 Mar 2016)

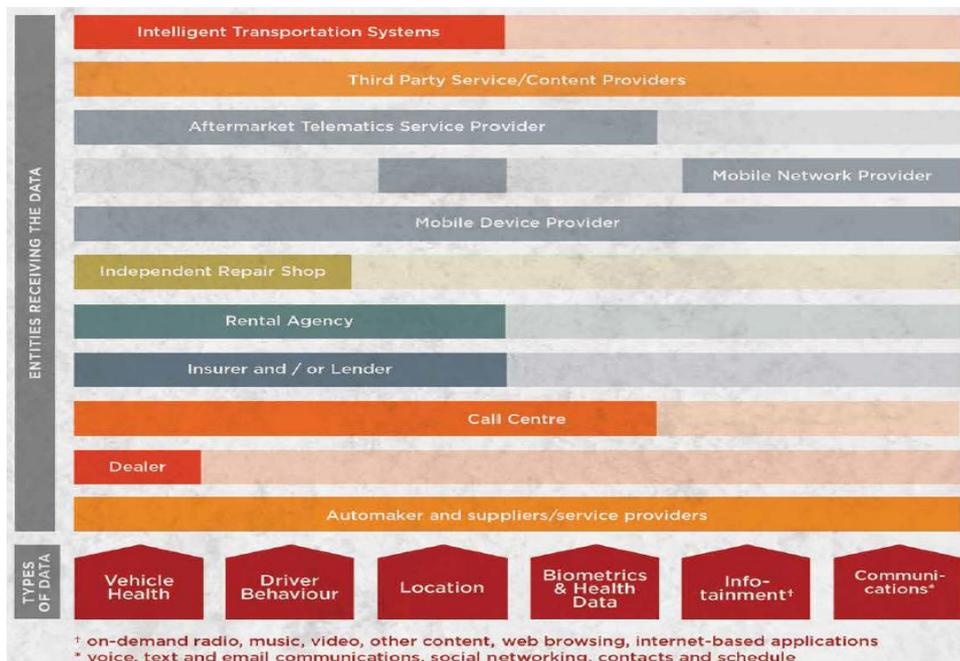
<http://www.businesswire.com/news/home/20160210005587/en/Automotive-Industry-Adopts-GSMA-Embedded-SIM-Specification> > *Machina Research* predict over 693 million car connections by 2020: *Machina Research*, <https://machinaresearch.com/> cited in *BusinessWire*, ‘Automotive Industry Adopts GSMA Embedded Sim Specification to Accelerate Connected Car Market’ (10 Feb 2016 accessed 3 Mar 2016) < <http://www.businesswire.com/news/home/20160210005587/en/Automotive-Industry-Adopts-GSMA-Embedded-SIM-Specification> >

<sup>307</sup> GSMA, ‘Connected Car Forecast: Global Connected Car Market to Grow Threefold Within Five Years’ (3 Feb 2013 accessed 10 Dec 2015) [https://www.gsma.com/iot/wp-content/uploads/2013/06/cl\\_ma\\_forecast\\_06\\_13.pdf](https://www.gsma.com/iot/wp-content/uploads/2013/06/cl_ma_forecast_06_13.pdf)

<sup>308</sup> Harry Trucker, ‘This is how many Tesla cars are in Australia’ *The Australian Business Review* (4 Jan 2016 accessed 22 Jan 2017) <https://www.businessinsider.com.au/this-is-how-many-tesla-cars-are-in-australia-2016-1>

<sup>309</sup> There are no VFACTS figures for Tesla’s Australia sales as it does not participate, but electric vehicle sales are generally low due to insufficient charging infrastructure (beyond NSW and Victoria) and price.

manufacturer, and to the vast smart world beyond. Lawson’s fine analysis depicts the scale of this information ecosystem as follows:



Graphic 1.5 Connected car data flows  
 Source: P. Lawson<sup>310</sup>

In other words, smart car scale, influence and systems are extensive. Complex data flows and supply chain interactions allow important data as to car systems, driver style (e.g. braking severity, response times etc.) and functioning, geolocation, and driver smartphone information such as social media and contacts, to flow seamlessly to car manufacturers, dealers (retailers) and others. Where it goes thereafter remains technically, subject to contracts, consents and voluntary industry practice.

(d) Scale: on the money...

<sup>310</sup> Lawson, above n 36. Graphic licensed to the public through a Creative Commons Attribution NonCommercial 2.5 Canada license (CC BY-NC 2.5 CA) < <https://creativecommons.org/licenses/by-nc/2.5/ca/>>

Overall CIOT economic projections are exponential, but also conflicting.<sup>311</sup> Internationally, Verizon predicts \$1.3 trillion (2019),<sup>312</sup> Gartner \$1.9 trillion (2020)<sup>313</sup> and McKinsey \$11.1 trillion (2025) or 11% of the global economy.<sup>314</sup> The expected EU market value exceeds one trillion euros in 2020.<sup>315</sup> As no useful Australian data exists,<sup>316</sup> a rather questionable adaption of international projections<sup>317</sup> yields a \$165 billion benefit by 2022<sup>318</sup> and a total potential annual impact of \$45 - 116 billion by 2025.<sup>319</sup> Of this, CIOT value across only three settings is \$9.5 – 39 billion: the smart home (\$3- 5 billion),<sup>320</sup> smart (autonomous) vehicles (\$4 – 10 billion) and smart health and fitness (\$2.5 – 24 billion).<sup>321</sup> Communications Alliance report that consumers may gain most, and infers “a potentially realizable \$100 billion” benefit to the Australian economy by 2025.<sup>322</sup> Today, that represents almost 10% of Australian

---

<sup>311</sup> Put simply, these depend on multiple factors including how the analyst defines the IOT and economic value, as a start. Note also that Metcalfe’s Law is said to apply to IOT “value”; that is, that the telecommunications network value is proportional to the square of the number of connected users of the system; so IOT’s connectivity presages its value.

<sup>312</sup> Figures are based upon an estimated compound annual growth rate of 17%. See Verizon, ‘2016: ready, set, go for the Internet of things’ (2016 accessed 11 Apr 2016) < <http://www.verizonenterprise.com/verizon-insights/state-of-market-internet-of-things/2016/>>; Verizon, ‘Impact of the Internet of things on Consumers’ Insights podcast with Ohad Zeira (2016 accessed 11 April 2016) <http://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf>; Verizon, ‘Value of IoT: The next step for IoT is predictive and prescriptive data analytics’ Insights podcast with Ashok Srivastava (2016 accessed 11 April 2016) < <http://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf>>; Verizon, ‘State of the Market: Internet of Things 2016’ (2016 accessed 11 April 2016) <<http://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf>>

<sup>313</sup> Gartner also include “incremental value”, “value adds” and “value at stake”, whereby IOT product and services will generate over \$300 billion in incremental value. Of the \$1.9T, sectoral breakdown includes manufacturing (15%), healthcare (15%) or insurance (11%) as the leading “verticals”: Gartner, above n 273. For businesses, benefits will include increased efficiency (82%), product quality (49%) and customer satisfaction (45%): Verizon, above n 312.

<sup>314</sup> McKinsey, above n 22 and 28.

<sup>315</sup> IDC Italia S.r.L and TXT e-solutions S.P.A., Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination (13 May 2015 accessed 2 Feb 2016) <<https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination>>

<sup>316</sup> Recent Australian Government Asia-Pacific figures project that by 2030, “disruptive business models” including the IOT, could collectively create up to \$625 billion pa, or 12% of total regional GDP: Australian Government, ‘Australia’s Cyber Security Strategy’ (2016 accessed 22 Apr 2016): 8 <<https://cybersecuritystrategy.dpmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf>>

<sup>317</sup> Assumptions include using McKinsey estimates and a GDP of 1.15%: Communications Alliance, above n 119: 67.

<sup>318</sup> Cisco cite five main values which fuel the \$14.4 trillion figure: asset utilization/ cost reduction (\$2.5 trillion); employee productivity/ labour efficiency (\$2.5 trillion); eliminating waste in supply chain and logistics (\$2.7 trillion), customer increase (\$3.7 trillion) and innovation(n.d.): Cisco, above n 13: 68.

<sup>319</sup> Using a nine-industry sectoral view: vehicles (autonomous vehicles and condition-based maintenance), home (chore automation and security), offices (security and energy), factories operations and equipment optimization), retail environments (automated checkouts), worksites (operations optimization and health and safety), human (health and fitness), outside (logistics and navigation) and cities (public health and transport): Ibid 67.

<sup>320</sup> Telsyte forecast that by 2019, Australian home spend will grow from \$289 million to \$3.2 billion, driven by new products and services – and reflecting the increasing “bake in” of new device connectivity: Telsyte, above n 31. Telsyte identify five key home market segments: smart lifestyle (appliances, gardening) – \$1.2B, smart home services (installation, management and cloud services) - \$812M, smart security (alarms, cameras, sensors, smart locks) - \$416M, smart energy (sensors, outlets, light bulbs) - \$658M and smart hubs (such as Google’s Nest) - \$64M. To put the \$3.2B in context, Australia’s overall retail spend in 2014 was \$275 billion: Ferrier Hodgson, ‘Australian retail 2015: Welcome to the Hunger Games!’ (Feb 2015 accessed 26 Apr 2016): 6.

<sup>321</sup> Ibid.

<sup>322</sup> Observation 22, Ibid 68. Note that the Report makes it clear these are estimates and does not suggest they are anything other than the best they can do, absent an Australian economic study.

GDP.<sup>323</sup> In summary, most if not all analysts agree that there will be billions of CIOT devices by 2020, yielding billions in revenue across the globe; and it seems that most discrepancies in how many billions relate to how each analyst defines the IOT, CIOT or economic value,<sup>324</sup> - not whether or not, those billions will exist.

### 1.2.3 Stakes

*50 billion connected things by 2020 means 50 billion data collection points, attack platforms, vulnerabilities, and opportunities...*<sup>325</sup>

From a consumer perspective, the CIOT ecosystem more than amplifies internet problems and stakes.<sup>326</sup> The NHTSA finds "... unprecedented effects":<sup>327</sup> the NTIA finds a "qualitative change" in connectivity, the "inextricable mixture of [connected] hardware, software, data and service"<sup>328</sup> poses new legal issues, and greater personal data volume, retention, accessibility and processing adds to greater granularity as to individual and collective behaviours, analysed and manipulated via big data and emerging technologies analysis. While collectively 'synergetic',<sup>329</sup> these factors combine with rapidly growing connectivity to create new potentials for consumer physical and financial harms through device malfunction or analytic error, data breach or national security attacks, and shift the privacy and security paradigm. Legally, the EU Article 29 Working Party locate many "novel liability aspects":<sup>330</sup>

- systemic dependence upon the cloud, with its known vulnerabilities;<sup>331</sup>
- wi-fi/ Bluetooth and apps with their associated vulnerabilities,<sup>332</sup>

---

<sup>323</sup> Trading Economics, 'Australia Economic Forecasts 2016-2020 Outlook' (2016 accessed 10 Nov 2016) <<http://www.tradingeconomics.com/australia/forecast>>

<sup>324</sup> For example, Gartner excludes PCs, tablets and smartphones from its definition. See the discussion as to defining the IOT above.

<sup>325</sup> Alexander Vulkanovski, "Presentation to ACCAN Conference, Connecting the Future Consumer" (2016 accessed 2 Oct 2016) Email to author.

<sup>326</sup> Collins, above n 157.

<sup>327</sup> NHTSA, 'Federal Automated Vehicles Policy: Accelerating the Next Revolution in Road Safety' (Sept 2016 accessed 22 Nov 2016): ES-3 <<https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf>>

<sup>328</sup> Guido Noto La Diega & Ian Walden, 'Contracting for the 'Internet of Things': Looking into the Nest', *Queen Mary University of London, School of Law, Legal Studies Research Paper No. 219/2016* (1 Feb 2016 accessed 3 Mar 2016) <SSRN:<http://ssrn.com/abstract=2725913>>

<sup>329</sup> Vulkanovski, above n 110: 5. He used a five-tier analysis: scale, reach, method, nature, and depth, but concludes the effect is issue amplification only. More recent reports and this author differ from that conclusion.

<sup>330</sup> EU's Article 29 Working Party (WP29) consists of 28 national data protection authorities formed for the 'protection of individuals with regard to the processing of personal data': Art 29 WP, above n 49: 22.

<sup>331</sup> See Mathews-Hunt, above n 151.

<sup>332</sup> Ibid.

- a complex liability chain involving multiple international actors;
- multiple hybrid goods/ services with dispersed responsibility;
- doubts as to ongoing product safety, maintenance issues, update capacities, and causation generally; and
- complexity little clarified by a long supply chain involving extensive contractual arrangements.

While exhibiting those aspects above, different CIOT market segments entail differing consumer risk profiles and attributes, as follows:

(a) *Stakes: smart self*

Smart self devices exhibit unsustainable consumer use patterns<sup>333</sup> and device use issues – most measure a limited number of activities, many lack accuracy,<sup>334</sup> most are technically challenging to operate, many provide limited interpretative analytics, and most lack integration with important health devices or resources.<sup>335</sup> Critics also warn that allowing employers<sup>336</sup> or health insurers<sup>337</sup> to monitor or access health data, even for overall economic<sup>338</sup> or financial incentives<sup>339</sup> such as reduced premiums or employment benefits, is privacy intrusive<sup>340</sup> and potentially, invites geo-fenced and behavioural advertising,<sup>341</sup> consumer discrimination<sup>342</sup> and may create long-lasting (in)accurate datasets as to changeable personal

---

<sup>333</sup> Endeavour Partners, 'Wearables abandonment rates are not improving materially' (May 2015 accessed 26 Mar 2016) <<http://endeavourpartners.net/wearables-abandonment-rates-are-not-improving-materially/>>

<sup>334</sup> See US cases impugning device data accuracy in Ch. 4. For similar Australian findings, see Tony Ibrahim, 'Flatlining Monitors' 'testing fitness trackers with heart rate monitors – what we found' *CHOICE* (8 Sept 2016 accessed 20 Sept 2016) <<https://www.choice.com.au/health-and-body/diet-and-fitness/sportswear-and-shoes/articles/fitness-trackers-with-heart-rate-monitors-what-we-found>>

<sup>335</sup> Davenport, above n 205: 5- 6.

<sup>336</sup> Mark Burdon and Paul Harpur, 'Re-conceptualising Privacy and Discrimination in an Age of Talent Analytics' (2014) 37 *UNSWLJ* 679 <<http://www.austlii.edu.au/au/journals/UNSWLawJl/2014/26.html#fn1>>

<sup>337</sup> Peppet, above n 283. In Australia, GIO seeks access to consumer health data, usually for 'flybuys' style consumer incentive programmes.

<sup>338</sup> RJ Krawiec, Jessica Nadler et al, 'No appointment necessary: How the IoT and patient-generated data can unlock health care value' *Deloitte University Press* (27 Aug 2015 accessed 25 Apr 2016) <[http://d27n205i7rookf.cloudfront.net/wp-content/uploads/2015/08/DUP-885\\_IoT\\_PatientGeneratedData\\_MASTER\\_082715.pdf](http://d27n205i7rookf.cloudfront.net/wp-content/uploads/2015/08/DUP-885_IoT_PatientGeneratedData_MASTER_082715.pdf)>

<sup>339</sup> Issie Lapowski, 'The Insurance Company That Pays People to Stay Fit', *WIRED* (8 Dec 2014 accessed 12 Jul 2016) <<http://www.wired.com/2014/12/oscar-misfit/>>; Rosalind McNamara, 'Insurance tracker apps: good for the consumer?' *CHOICE* (6 Oct 2016 accessed 8 Oct 2016) <<https://www.choice.com.au/electronics-and-technology/phones/mobile-phones/articles/insurance-tracker-apps>>

<sup>340</sup> Office of the Privacy Commissioner of Canada, "Wearable Computing — Challenges and opportunities for privacy protection" (Jan 2014 accessed 4 Apr 2016) <[https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc\\_201401/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc_201401/)>; Jennifer Elias, '6 Ways to Protect Your Data in the Age of Wearables' 1.0' (15 Dec 2015 accessed 10 Apr 2016) <<http://www.forbes.com/sites/jenniferelias/2015/12/15/6-ways-to-protect-your-data-in-the-age-of-wearables-1-0/#3c10b0b74405>>

<sup>341</sup> Office of the Privacy Commissioner of Canada, 'The Internet of Things', Policy & Research Group (Feb 2016 accessed 12 Apr 2016): 11 <[https://www.priv.gc.ca/information/research-recherche/2016/iot\\_201602\\_e.pdf](https://www.priv.gc.ca/information/research-recherche/2016/iot_201602_e.pdf)>

<sup>342</sup> Peppet, above n 283.



privacy, fusion-based discrimination potentials<sup>353</sup> and consent issues.<sup>354</sup> Many smart device markets are “embryonic”, entailing limited product choice, high costs and ill-defined consumer value.<sup>355</sup> Others like smart TVs are already market-ingrained, despite questionable surveillance attributes,<sup>356</sup> analogous to smart voice recognition and assistant technologies. ENISA identify a range of partial legal gaps requiring resolution:

- liability for consumer injury or damage;
- data breach liability;
- the time within which vulnerabilities are required to be fixed or software updated; and
- liability for failures to do so.<sup>357</sup> Some form of safe harbour scheme for security researchers to foster disclosure and redress of vulnerabilities, as well as disclosure for failure to do so.

Consumer inconvenience will arise if devices are defective, go offline or ‘rogue’. Smart homes innately collect and store extensive personal information, which may not occur with data subject consent,<sup>358</sup> unless deemed ‘implied’ by entry. Non-consenting persons may include visitors, tradespeople, passers-by or employees; and includes real time covert surveillance like the ‘nanny cam’ and ‘peep-hole camera’,<sup>359</sup> both of which produce remotely stream-able images. Critics also point to profiling and discrimination which may arise from home data analysis, including home insurance premiums, which already (un-controversially) offer lower rates for smart homes security.<sup>360</sup> Detriment questions arise if employers, health insurers or others seek home data access, even if consumers consent inspired by

---

<sup>353</sup> Peppet, above n 283.

<sup>354</sup> Diega, above n 328.

<sup>355</sup> Above n 340, 334.

<sup>356</sup> Samsung and Vizio TVs have been especially criticised (Ch.4 and 5). EPIC allege: “When the voice recognition feature is enabled, everything a user says in front of the Samsung SmartTV is recorded and transmitted over the internet to a third party regardless of whether it is related to the provision of the service”: EPIC, ‘Samsung Smart TV Complaint’ (24 Feb 2015 accessed 11 Aug 2016) <<https://www.epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf>> and commentary <<https://epic.org/privacy/internet/ftc/samsung/>>; California has enacted laws to address smart TV privacy and disclosures: Assembly Bill No. 1116, 2015-16, <[https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\\_id=201520160AB1116](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1116)> c/f Samsung deny the accusation: Samsung, ‘Samsung Smart TVs Do Not Monitor Living Room Conversations’ *Press Release* (10 Feb 2015 accessed 10 May 2016) <<https://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-conversations>>

<sup>357</sup> ENISA, ‘Security and Resilience of Smart Home Environments: Good practices and recommendations’ (Dec 2015 accessed 2 Apr 2016) <<https://www.enisa.europa.eu/publications/security-resilience-good.../at.../fullReport>>

<sup>358</sup> Most systems do not seek consents after the initial set-up stage and then, only that person is likely to be aware of them.

<sup>359</sup> Alexandra Gibbs, ‘Internet of Things: Peep-hole tells you who’s at the door’ CNBC (13 Jan 2015 accessed 28 Jan 2016) <<http://www.cnn.com/2015/01/13/internet-of-things-peep-hole-tells-you-whos-at-the-door.html>> > These devices attach a small camera inside a front door peephole, and take an image when anyone knocks, sending it via the home Wi-Fi system to the owner’s smartphone.

<sup>360</sup> Association of British Insurers, ‘How data makes insurance work better for you’ (2015 accessed 2 Jul 2016) <<https://www.abi.org.uk/~media/Files/Documents/Publications/Public/2015/Data/How%20data%20makes%20insurance%20work%20better%20for%20you.pdf>>

financial incentives.<sup>361</sup> As for smart self, smart home data potentially, fuels consumer discrimination<sup>362</sup> and may create long-lasting (in)accurate datasets as to infinitely changeable personal behaviours.<sup>363</sup> Smart home device data and profiled inferences are also starting to appear in court.<sup>364</sup> Competitive industry behaviours have emerged which may not promote consumer interests: for example, Google 'bricked' Revolv leaving consumers with a 'dumb' device and Apple stopped selling Nest once *HomeKit* launched - claiming its privacy was superior.<sup>365</sup> Questions as to manufacturer and cloud provider data management (collection, storage, processing and sharing), as well as third party disclosure practices and risks remain open: for example, while Samsung claims that consumers retain their data ownership, their terms reserve extensive use rights to themselves.<sup>366</sup> Finally, CIOT "data-veillance" may ultimately affect individual will, as discussed above.

(c) *Stakes: smart car*

*"The automotive industry views driverless cars as the evolution of cars leveraging computers. The computer industry views driverless cars as computers with wheels..."<sup>367</sup>*

*Connected cars will be the ultimate Internet of Things. They will collect and make sense of massive amounts of data from a huge array of sources... Cars will talk to other cars, exchanging data and alerting drivers to potential collisions. They'll talk to sensors on signs on stoplights, bus stops, even ones embedded in the roads to get traffic updates and rerouting alerts. And they'll communicate with your house, office, and smart devices, acting as a digital assistant, gathering information you need to go about your day."<sup>368</sup>*

---

<sup>361</sup> Lapowski, above n 339; McNamara, above n 339.

<sup>362</sup> Peppet, above n 283.

<sup>363</sup> McNamara, above n 339.

<sup>364</sup> There appears to be no evidence yet of smart home data use yet in court, but police routinely examine home security cameras and other home devices should it be relevant to their enquiries.

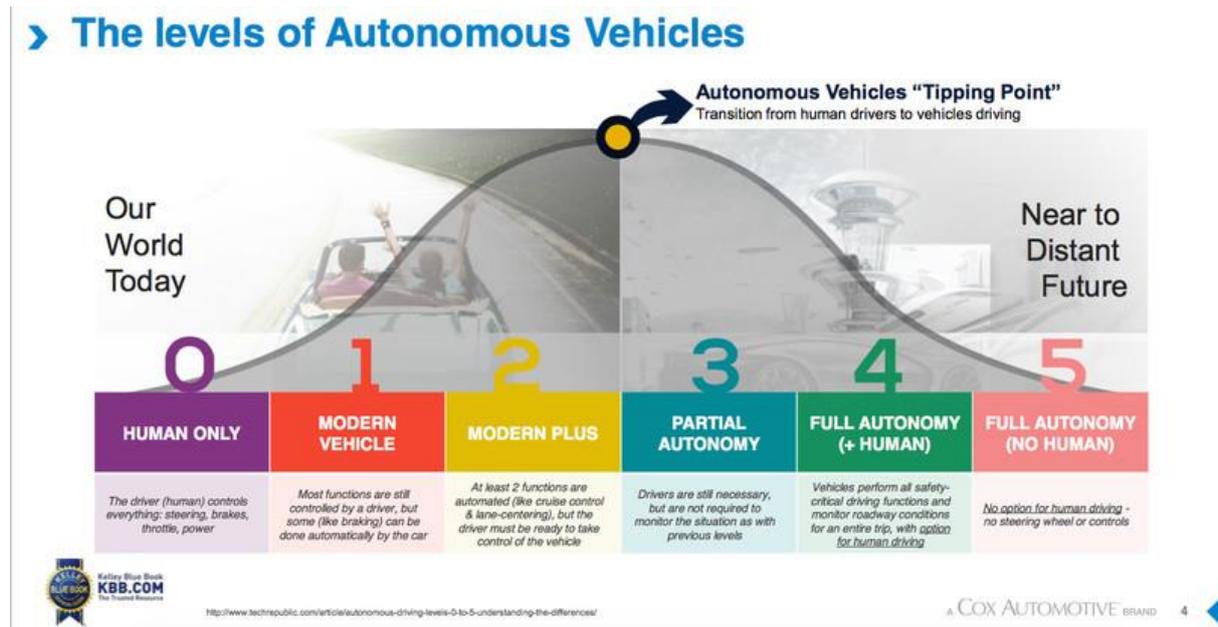
<sup>365</sup> "HomeKit introduces a new way for you to control supported devices in your home... and we've taken great care to make sure that the convenience... doesn't come at the expense of your privacy..."

<sup>366</sup> Consumers may retain data 'ownership': W.P. Hong, 'Samsung shows that the internet of things is now "in sync with real life' Samsung Newsroom (8 Jan 2016 accessed 11 May 2016) <<https://www.news.samsung.com/global/Samsung-shows-that-the-internet-of-things-is-now-in-sync-with-real-life>> but Samsung reserve extensive 'use' rights: see Sched. 1: Samsung, 'Samsung Smart Home Terms of Service (Aust)' (n.d. accessed 2 Aug 2016) <<https://account.samsung.com/membership/etc/specialTC.do?fileName=smarthome.html>>

<sup>367</sup> Chunka Mui, '28 Primers on Driverless Car Innovation and Disruption' *Forbes* (updated 5 Apr 2016 accessed 26 May 2016) <<http://www.forbes.com/sites/chunkamui/2016/03/10/primers-on-driverless/print/>>

<sup>368</sup> IBM's Dirk Wollschlaeger, "What's Next? V2V (Vehicle-to-Vehicle) Communication with Connected Cars" (9 Oct 2014) <<https://www.wired.com/insights/2014/09/connected-cars/>> cited in Lawson, above n 36.

The auto industry is “on the brink of a revolution...”<sup>369</sup>, and the smart car future is a highly disruptive<sup>370</sup> inevitability. A typical modern smart(ish) car now contains over 100 million lines of code – more than a Boeing 787 (6.5M) or F-22 jet fighter (1.7M).<sup>371</sup> With such complexity, potentials for software error and vulnerabilities increase. “Smart” is a relative concept, spanning a spectrum of increasingly-autonomous technologies,<sup>372</sup> from human control to self-driving vehicles,<sup>373</sup> across SAE’s six automation levels<sup>374</sup> below:



Graphic 1.6 Levels of autonomous vehicles  
Source: Kelley Blue Book (2016)<sup>375</sup>

<sup>369</sup> Simon Ninan, Bharath Gangula, Matthias von Alten & Brenna Sniderman, ‘Who owns the road’ *Deloitte* (2015 accessed 5 Apr 2016) <<http://dupress.com/articles/internet-of-things-iot-in-automotive-industry/?id=us:2em:3na:dup1161:eng:dup:060816>>

<sup>370</sup> It smashes the traditional auto industry model – towards software-driven, data-gathering products, which conceivably, may disrupt traditional car self-ownership models towards a more sharing economy approach. It is not difficult to imagine a system of efficiently autonomous drones, collecting and depositing passengers seamlessly on demand, parking themselves and skilfully avoiding traffic, human error and through V2V communications, each other.

<sup>371</sup> A Boeing 787 passenger aircraft contains 6.5 million lines of code, and an F-22 U.S. Air Force jet fighter contains 1.7 million lines: U.S. Gov’t Accountability Office, GAO-16-350, ‘Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack 8–9’ (Mar. 2016 accessed 11 May 2016) <<http://www.gao.gov/assets/680/676064.pdf>>

<sup>372</sup> Expert Missy Cummings cites GPS position information, internal navigation maps, outward-facing cameras, and laser (and other) range-finding systems, form a part of autonomy: M.L. Cummings, M.L. & J.C. Ryan, ‘Who is in Charge? Promises and Pitfalls of Driverless Cars’, *TR News* (May-June 2014 accessed 20 Mar 2016) <<http://hal.pratt.duke.edu/sites/hal.pratt.duke.edu/files/u7/TR%20news%20Cummings%20MAR14.pdf>>

<sup>373</sup> Note that some reports distinguish between connected cars and autonomous technology, but the industry reality is that these technologies coexist in most new models. See for example, Rand, above n 232.

<sup>374</sup> There are: none (level 0), driver assistance (1), partial automation (2), conditional automation (3), high automation (4) and full automation (level 5).

<sup>375</sup> Kelley Blue Book, ‘Future Autonomous Driver Study’ (Sept 2016 accessed 25 Sept 2016) <<http://mediaroom.kbb.com/future-autonomous-vehicle-driver-study>>; & Standard: SAE International, ‘Automated Driving’ (2014 accessed 5 Aug 2016) <[https://www.sae.org/misc/pdfs/automated\\_driving.pdf](https://www.sae.org/misc/pdfs/automated_driving.pdf)>

The control “tipping point” – or “no man’s land”<sup>376</sup> - spans levels 2 to 4, through which humans are variously expected to drive and/ or ‘monitor’ the dynamic driving task,<sup>377</sup> and to respond promptly to system ‘requests to intervene’,<sup>378</sup> or if necessary, to override the system itself. The question of “proper control” between car ‘driver’ and manufacturer, is a liability controversy which remains unresolved by Australian regulators.<sup>379</sup> While liability might shift with ‘control’ – in practice, that ‘shift’ is less clear until full autonomy is reached; especially where vehicle systems require an alert driver to override their actions. This issue, manufacturers’ liability and ‘state of the art’ is explored further in chapter 4.

Smart cars also present potentially unquantifiable external costs, involving economic and social disruption:<sup>380</sup> adverse effects on public transport use and investment,<sup>381</sup> road congestion, urban sprawl; vehicle size,<sup>382</sup> reduced ‘car’<sup>383</sup> and ‘crash’ industry employment;<sup>384</sup> disruption to insurance<sup>385</sup> and related industries;<sup>386</sup> parking revenue decline<sup>387</sup> and increased road infrastructure costs.<sup>388</sup> Social equity issues

---

<sup>376</sup> Keith Naughton and Dana Hull, ‘Ford Plans Leap from Driver’s Seat with Autonomous Car by 2021’ *Bloomberg Technology* (17 Aug 2016 accessed 18 Aug 2016): <<http://www.bloomberg.com/news/articles/2016-08-16/ford-aims-to-offer-fully-autonomous-ride-sharing-vehicle-by-2021>>

<sup>377</sup> ‘Dynamic driving task’ includes the operational (steering, braking, accelerating, monitoring the vehicle and roadway) and tactical (responding to events, determining when to change lanes, turn, use signals. etc) aspects of the driving task, but not the strategic (determining destinations and waypoints) aspect of the driving task: SAE International, ‘Automated Driving International Standard J3016’.

<sup>378</sup> ‘Request to intervene’ is notification by the automated driving system to a human driver that s/he should promptly begin or resume performance of the dynamic driving task: Ibid.

<sup>379</sup> The NTC is conducting further consultation in Australia on the question of ‘proper control’, though seems likely to resolve via national enforcement guidelines that cars remain under human control until they are designated fully autonomous. One of the reasons for this is simplicity, as well as keeping the onus upon drivers to remain alert. NTC, ‘NTC seeks feedback on proposal for drivers to allow hands off the wheel in some automated vehicles’ (12 April 2017 accessed 13 Apr 2017) <<https://www.ntc.gov.au/about-ntc/news/media-releases/ntc-seeks-feedback-on-proposal-for-drivers-to-allow-hands-off-the-wheel-in-some-automated-vehicles/>>

<sup>380</sup> As this non-comprehensive list suggests, the many uncertainties raise multiple unknowns, justifying additional research as to the nature and potential magnitude of costs and benefits of smart cars, especially during the fleet transitional phase.

<sup>381</sup> These may adversely impact public transport utilization, reduce fare income leading to reduced services or increased fares, and perpetuate transport inequities, in favour of “our individualistic car-centred society”: Rand, above n 232: 39.

<sup>382</sup> Some speculate vehicles will become more of a “living space”.

<sup>383</sup> Employment disruption may occur in fields like emergency services, car servicing, taxi, parking and chauffeuring services: Allison Arieff, ‘Driving Sideways’ *The New York Times Opinionator* (23 Jul 2013 accessed 3 Mar 2016) <<https://opinionator.blogs.nytimes.com/2013/07/23/driving-sideways/#more-146616>>

<sup>384</sup> Driving-related jobs, employment in public transport, logistics, insurance, etc; and in the “crash-related” economy (emergency services personnel, doctors and other health professionals, hospitals, investigators and lawyers, automotive sales and repair industry, etc) may be affected.

<sup>385</sup> The insurance industry will (ultimately) be significantly affected through reduced premiums as costs for accidents (and possibly theft) decline. But car manufacturers and suppliers will change their insurance profiles as crash liability shifts to them, and costs will be passed on to consumers. Tesla self-insures its cars as do many other manufacturers (at least indirectly). Insurers will find themselves dealing with vehicle manufacturers, rather than drivers, as accident liability shifts: James Titcomb, ‘Motor insurers form alliance to tackle driverless cars’ *The Telegraph* (18 Jan 2016 accessed 26 Mar 2016) <<http://www.telegraph.co.uk/technology/news/12106757/Motor-insurers-form-alliance-to-tackle-driverless-cars.html>>

<sup>386</sup> Adverse impacts upon insurance, health and other sectors (together with their investment practices) will potentially affect markets and shareholders.

<sup>387</sup> Declining municipal parking and fine-related revenue may occur as smart cars can park further away, in smaller spaces.

<sup>388</sup> Smart cars require better and more standardised road infrastructure to ensure C-ITS operation and so they can for example ‘read’ the road signs (etc) consistently. This poses cost problems for large countries such as Australia and the US,

will (initially) be exacerbated – poverty may increase an individual’s accident risk, and public transport may become more expensive. Culturally, people may miss driving.<sup>389</sup> Of course, the worst ‘known’ detriment is that consumers will die in smart cars,<sup>390</sup> due to inadequate road infrastructure, product liability (design or software defects, mechanical or systems failures), hacking (deliberate or accidental security breach or terrorism) and human error (via the perils of transitioning autonomy, instructional or maintenance failures, and a mixed road fleet). Hackers have demonstrated significant software vulnerabilities,<sup>391</sup> and in a worst-case software update defect scenario, for example, an entire model may literally, suddenly, ‘crash’.<sup>392</sup> Current systems ‘limitations’ already disclaim smart car flaws as common road-use scenarios, such as ‘bright light’ or ‘bad weather’, policemen’s hand signals and minor programming glitches, can confuse current technology.<sup>393</sup> Further, inexpensive equipment can threaten system integrity: researchers have shown jammers can cause GPS navigation problems and cheap laser devices can deceive systems into seeing false objects. Experts also suggest that other road users – drivers, cyclists and pedestrians – may behaviorally ‘game’ smart car technology, just for fun or to exploit predictable vehicle behavior, like giving way.<sup>394</sup> Conversely, subtle human road user signals<sup>395</sup> (nods, waves etc.) will need to be ‘unlearned’. Inter-disciplinary studies reveal human physical, psychological and behavioral attributes which affect safety-systems design efficacy: driver distractibility, technology over-confidence, reaction time, attention span and so on,<sup>396</sup> all of which should influence both design practice

---

with significant rural populations and large road networks. This may confine smart car use to specific geographic locations – such as cities – until such time as the cars become sufficiently ‘smart’ to cope beyond.

<sup>389</sup> They refer to lost personal autonomy and enjoyment of car driving plus lost cultural motifs such as the ‘road trip’ adventure: Rand, above n 232: 40.

<sup>390</sup> Professor Missy Cummings critiques as “utilitarian” the argument that smart cars will save lives as demonstrating “an insensitivity to a deontological perspective that causes many people to be uncomfortable with such a significant shift in responsibility and accountability to computers... A deontological approach could assert that machines should not be allowed to take the lives of humans under any circumstances, which is similar to one of Asimov’s three laws governing robots.” Cummings, above n 372: 1. See also n 394 supra.

<sup>391</sup> For example, see Mark Anderson, ‘Black Hat 2014: Hacking the Smart Car,’ *IEEE Spectrum* (6 Aug 2014 accessed 16 Mar 2016)

<<http://spectrum.ieee.org/cars-that-think/transportation/systems/black-hat-2014-hacking-the-smart-car>

<sup>392</sup> Rand, above n 232: 6. It is however likely that recalls will be more effective due to the ease with which software updates are implemented over the traditional requirement that consumers bring cars into dealers for recall-related fixes.

<sup>393</sup> Other commonly cited ‘limitations’ include poor road markings, standing water, sudden downpours and snow; all of which are commonly expected motor vehicle uses.

<sup>394</sup> Testimony of Mary Cummings, ‘Hands Off: the Future of Self-Driving Cars’ (15 Mar 2016 accessed 20 Mar 2016)

<<https://governmentrelations.duke.edu/wp-content/uploads/Cummings-Senate-testimony-2016.pdf>>; M.L. Cummings & J.C. Ryan, ‘Who is in Charge? Promises and Pitfalls of driverless Cars’, *TR News* (May-June 2014 accessed 20 Mar 2016) 292

<<http://hal.pratt.duke.edu/sites/hal.pratt.duke.edu/files/u7/TR%20news%20Cummings%20MAR14.pdf>> UK trials will be conducted using unmarked cars, for fears that drivers will ‘game’ them on-road: Julia Kollewe, ‘Volvo to seek volunteers for self-driving car trial in UK’ *The Guardian* (2 Feb 2017 accessed 7 Feb 2017)

<<https://www.theguardian.com/business/2017/feb/02/volvo-seeks-volunteers-for-self-driving-car-trial-in-west-london-public-roads>>

<sup>395</sup> Most drivers are familiar with pedestrians who show an interest in crossing the road and may use eye-contact to ‘okay’ that manoeuvre, and vice versa, drivers may gesture to pedestrians to cross, even where there is no strict legal right to do so. These are to some extent an extra-legal etiquette of road use.

<sup>396</sup> Cummings, above n 394: 1- 2.

and legal considerations as to what is reasonable 'warning' in a safety context. But while many safety issues may decline as the fleet, technology and experience matures and road infrastructure improves, shorter term risks as to consumer (lack of) adaptability, the tipping point and fleet changeover delays, pose unique challenges for consumer welfare. Further, information asymmetry risk - such as consumer instructional conflicts between voluminous manuals, systems, in-car prompts versus smart car sales, marketing and risk perception - will take time to resolve. Aside from design and driving context issues,<sup>397</sup> Australia's state-based fault and no-fault personal injury compensation schemes, may be unworkable without legislative reform.<sup>398</sup>

Smart car issues common to CIOT generally include voluminous vehicle data collation and privacy policy issues a lack of mandatory international data use standards,<sup>399</sup> software security flaws,<sup>400</sup> anti-competitive third party data access,<sup>401</sup> 'data-veillance',<sup>402</sup> data discrimination potentials<sup>403</sup> and questionable consumer consents.<sup>404</sup> Further, in-car data collection consent is complicated by different drivers and passengers, or may be deemed 'implied' by vehicle entry. Even if passenger identity is not initially discernible, geolocation alone can constitute personal information:<sup>405</sup> for example, a car which regularly visits a cancer treatment clinic may generate certain health information inferences.<sup>406</sup> Profiling and discrimination may arise from other car data analysis; while car insurers already offer lower rates or

---

<sup>397</sup> NTC, 'Regulatory Options for Automated Vehicles' *Discussion Paper* (May 2016 accessed 30 May 2016) <[https://www.ntc.gov.au/Media/Reports/\(049B1ED1-5761-44D5-9E3C-814A9195285D\).pdf](https://www.ntc.gov.au/Media/Reports/(049B1ED1-5761-44D5-9E3C-814A9195285D).pdf)>

<sup>398</sup> Kieran Tranter, 'The Challenges of Autonomous Motor Vehicles for Queensland Road and Criminal Laws' 16:2 (2016) *QUT Law Review* 59- 81 <<https://lr.law.qut.edu.au/article/view/626/591>>

<sup>399</sup> Note the US-based global car manufacturers have released certain approaches to privacy and security, which are lower than Australian Privacy Act 1988 (Cth) standards: Alliance of Automobile Manufacturers Inc., and Association of Global Automakers, Inc. (Auto Alliance), 'Consumer Privacy Protection Principles', (12 November 2014 accessed 16 Mar 2016) <http://www.autoalliance.org/index.cfm?objectid=CC629950-6A96-11E4-866D000C296BA163>>; and 'Framework for Automotive Cybersecurity Best Practices' (19 Jan 2016 accessed 2 Mar 2016) <<http://www.autoalliance.org/index.cfm?objectid=1E518FB0-BEC3-11E5-9500000C296BA163>>

<sup>400</sup> Mark Anderson, above n 391; Andy Greenberg, 'Hackers reveal Nasty New Car Attacks - with me behind the Wheel' *Forbes* (24 Jul 2013 accessed 3 Mar 2016) < <http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#6741c6765bf2>>; Andy Greenberg, 'The Jeep Hackers are back to prove car hacking can get much worse' *WIRED* (1 Aug 2016 accessed 2 Aug 2016) < <https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/>>; Andy Greenberg, 'A New Wireless Hack can Unlock 100 Million Volkswagens' *WIRED* (10 Aug 2016 accessed 12 Aug 2016) <https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/>>

<sup>401</sup> Australian Automobile Aftermarket Association, (AAAA) 'AAAA Demands Better Consumer Law Protection for Car Owners' (15 July 2016 accessed 30 June 2016) <<https://www.aaaa.com.au/news.asp?id=242>> Without data access, aftermarket repair and maintenance if hindered, reducing competition in that industry

<sup>402</sup> Lawson, above n 36.

<sup>403</sup> Peppet, above n 283.

<sup>404</sup> Lawson, above n 36.

<sup>405</sup> Article 29 WP, above n 346.

<sup>406</sup> Mason Hayes and Curran, above n 346; Data Protection Commissioner (Ireland), above n 336. In contrast, the NTC recommended no change to the *Privacy Act 1988* (Cth) including as to geolocation data: NTC, 'Cooperative Intelligent Transport Systems Policy Paper' (December 2013 accessed 2 Jan 2016):17 <[https://www.ntc.gov.au/Media/Reports/\(55AFE902-73F4-073B-E6ED-AE684E3BE595\).pdf](https://www.ntc.gov.au/Media/Reports/(55AFE902-73F4-073B-E6ED-AE684E3BE595).pdf)>

incentives for drivers who allow insurers 'black box' data access,<sup>407</sup> such data may reveal vehicle direction, date, time, latitude, longitude and speed, is accessible upon any court order and may cumulatively create long-lasting (in)accurate datasets as to often-changeable personal behaviours.<sup>408</sup> Car use and location data, accident data and profiled inferences are currently used by law enforcement and accident investigation agencies and may soon become commonplace in court.<sup>409</sup> Finally, questions as to data management (collection, storage, processing and sharing) approaches of manufacturers and their cloud providers, as well as third party disclosure practices and risks have largely been left to the manufacturers to resolve within privacy legislation, but arguably reflect a commercial interest in data exploitation potentials.

## Conclusion

CIOT exacerbates multiple 'known' issues and tendencies, but its scope, scale and role in integrating a raft of rapidly-emerging technologies, and consumer reach, represents a qualitative and quantitative change. That change will affect many previously 'known' tech-related issues such as: privacy, data use and abuse, breach or hacking, security, anonymisation, disclosure and transparency; the 'notice and choice' consent fallacy; complex liability chains and product/ data internationalisation; as well as lesser known issues surrounding tech lock-in to products and systems, interoperability, hybrid device/ software products, erosion of ownership norms;<sup>410</sup> emerging industry-frustrating technical constraints<sup>411</sup> and evolving consumer smart device (M2M) contracting. As these complex 'knowns' evolve and expand in concert with CIOT, they foreground a myriad of "unknowns" as the technology permeates society,

---

<sup>407</sup> Car insurers offer consumers a chance to reduce premiums though monitoring their driving patterns. Australian examples include comprehensive (only) policies from GIO, Progressive and 'Insurance Box' (underwritten by QBE): the latter requires consumers to 'rent' a black box, records speed, braking, acceleration and night driving, ranks these over time (via a dashboard consumers can access to modify their behaviour) and premiums "settle once driver rating data 'settles'. The related app privacy documents states "our App will record the direction you are heading, date, time, latitude, longitude and speed and that this information is collected and stored by us or by third parties on our behalf. You understand that by using our App it is possible to identify your location and the speed at which you are travelling: Insurance Box, 'Journey data privacy policy' <<http://insurancebox.com.au/documents/privacy-promise.pdf>> See also Association of British Insurers, above n 360; Jain, above n 245.

<sup>408</sup> McNamara, above n 339.

<sup>409</sup> For example, Tesla data was used by the NHTSA investigation. Location data can be used to place suspects at the scene of a crime or corroborate other factors circumstantially.

<sup>410</sup> Kyle Weins, 'We Can't Let John Deere Destroy the Very Idea of Ownership' *WIRED* (21 Apr 2015 accessed 2 Apr 2016) <<http://www.wired.com/2015/04/dmca-ownership-john-deere/>> The manufacturer asserted tractor owners did not 'own' their vehicle; rather they were licensed to use it for its life cycle only.

<sup>411</sup> Issues commonly cited by technical experts include spectrum availability, network coverage, standardisation and interoperability: Communications Alliance, above n 119: 14.

vulnerabilities emerge and error informs trial. Combined, industry analysts confirm that these ‘problems’ will require regulatory involvement on an ongoing basis.<sup>412</sup>

In this turbulent social and legal environment, consumers are reportedly exhibiting CIOT security overconfidence<sup>413</sup> while experiencing a trust crisis,<sup>414</sup> as well as facing disruptive social impacts upon transport, home, health, education, and the workforce. Combined, the consumer stakes appear significant and long-lasting. Against those stakes, the next question is to examine the current baseline: to what extent are Australians adopting the consumer IOT and does it inspire consumer trust?

### 1.3 Status: consumer uptake & adoption

*...apart from wearable devices and the odd car with a mobile app ... it hasn't been something which consumers have not picked up on...*<sup>415</sup>

*IOT will only take off once consumers understand what it means on a basic, emotive level...*<sup>416</sup>

Australians are generally “early [tech] adopters”<sup>417</sup> and adoption is “inevitable”,<sup>418</sup> but there are no Australian studies as to consumer IOT awareness levels, market participation or current spend as at 2016

---

<sup>412</sup> McKinsey, above n 22 and 28; Verizon, above n 312 and Cisco, above n 98: 13, all of which are pro-CIOT but recommend that regulatory change will be required. McKinsey argue that the digitization of physical systems will require both updating and strengthening of privacy and property policy, to regulate entirely new “forms of activity in the public sphere” (such as autonomous vehicles), privacy security, data ownership and sharing regulations require review and to be “updated” and governments will need to coordinate efforts to create interoperability standards, incentivized policy settings (eg in health), and to balance privacy, data protection, IP with national security imperatives. Cisco likewise contends that government retains a policy and regulatory role with respect to IOT, “governments will need to help ensure the safety and security of the systems themselves, whilst also protecting users’ personal information and privacy”, together with ensuring “social cohesion and inclusion”. Verizon has called for greater technology-expertise amongst regulators to cope with increasing IOT products and services, whilst consumer-focused academics have called for specific regulation and soft law. UK’s Blackett Report recommends regulation to “anticipate and respond to new challenges” as well as to support privacy and other regulatory objectives (though recommends it be “kept to a minimum”): Blackett, above n 19.

<sup>413</sup> A 2016 ISACA study found a major confidence gap as to the security of connected devices between the average Australian consumer and cybersecurity IT professionals: ISACA, ‘ISACA Survey: Wide Gap between Australian Consumers and Global IT Professionals on Internet of Things Security’ *Press Release* (14 Oct 2015 accessed 3 Jan 2016) <<http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/ISACA-Survey-Wide-Gap-between-Australian-Consumers-and-Global-IT-Professionals-on-Internet-of-Things-Security.aspx>>

<sup>414</sup> ‘Hacking’ is used in this paper to mean any person who without authorisation, breaks into a computer or software system. It includes those who do so for personal amusement, research or criminal purposes such as terrorism, data theft, attack or denial of service. The important point, when considering CIOT security, is that the system can be breached, rather than the intent of the person involved. Sead Fadilpašić, ‘Consumers do not trust Internet of Things’ *betanews* (April 2016 accessed 11 May 2016) <<http://betanews.com/2016/04/08/internet-of-things-consumer-trust/>>

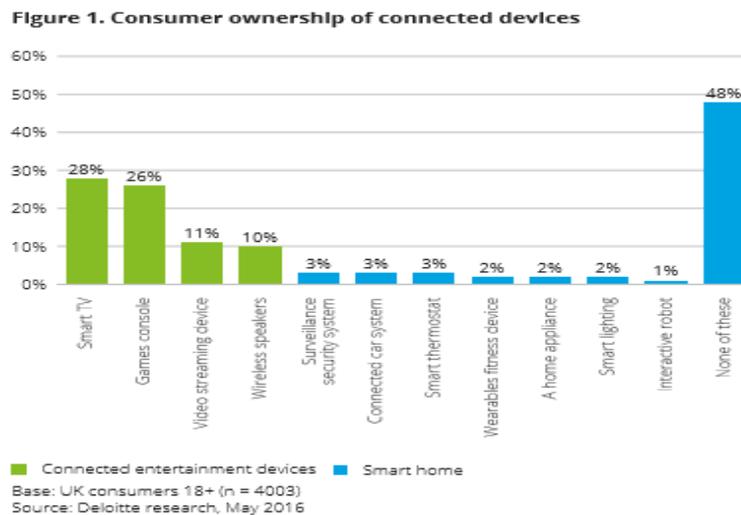
<sup>415</sup> Alex Talevski, ‘Why people don’t care about the internet of things’ *The Australian* (26 Apr 2016 accessed 29 Apr 2016) <<http://www.theaustralian.com.au/business/technology/why-people-dont-care-about-the-internet-of-things/news-story/2670ec1d7c9bc4017e10e632d1a8f90c>>

<sup>416</sup> *Ibid.*

<sup>417</sup> Telsyte, ‘Internet Uninterrupted Australian households of the Digital Future’ *Research Paper* (2015 accessed 3 Dec 2015) <http://www.nbnco.com.au/content/dam/nbnco2/documents/Internet%20Uninterrupted%20Australian%20Households%20of%20the%20Connected%20Future.pdf>

<sup>418</sup> Accenture, ‘The Internet of Things: The Future of Consumer Adoption’ (2014 accessed 23 Mar 2016) <[https://www.accenture.com/t00010101T000000\\_\\_w\\_/au-en/\\_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology\\_9/Accenture-Internet-Things.ashx#zoom=50](https://www.accenture.com/t00010101T000000__w_/au-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Internet-Things.ashx#zoom=50)>

end. Recent US and UK studies may be indicative, though their markets are more advanced.<sup>419</sup> These conclude that consumer awareness is low: two years ago, 87% of US consumers had not heard of the internet of things.<sup>420</sup> Of those, 64% were unaware of the smart device market, and 7% or less owned a smart self or home device.<sup>421</sup> One year later, only 16% of US adults knew what the consumer IOT is, though 48% had “heard of it”,<sup>422</sup> which confirms European findings.<sup>423</sup> By mid-2016, Deloitte found that smart home awareness and interest was improving, but that people did not understand device operation or capabilities, and purchase disinterest (70%) remained high.<sup>424</sup> Further, consumer awareness was clustered in traditional entertainment categories (in green below), with few owning newer ‘smart’ home devices and most not planning a ‘smart’ purchase 2016- 2017. This suggests that baked-in connectivity (where all new devices are built ‘smart’) and natural replacement cycles are likely to be significant market drivers in the evolution of smarter homes, rather than consumer demand, at least initially.



Graphic 1.7 UK consumer smart home device ownership by category  
 Source: Deloitte 2016<sup>425</sup>

<sup>419</sup> This reflects the draw of larger consumer markets for manufacturers. Several smart home manufacturers have indicated 2017 will be their Australian ‘launch’ year.

<sup>420</sup> Altimeter’s study concluded that IOT is an industry term of art, and that there is a high degree of consumer ignorance as to the IOT generally: Accenture, above n 418.

<sup>421</sup> 40% did not know what ‘wearables’ were. Of the 13% who were IOT-aware, reasons not to buy-in included due to a lack of perceived value (36%), privacy (23%) and price (23%): Ibid. See also Bernard Marr, ‘17 Internet of Things Facts Everyone Should Read’ *Forbes* (27 Oct 2015 accessed 10 Mar 2016) <http://www.forbes.com/sites/bernardmarr/2015/10/27/17-mind-blowing-internet-of-things-facts-everyone-should-read/#6381e8161a7a>

<sup>422</sup> To the question “Do you know what the IOT is?”, 36% responded No and only 13% said Yes. Verto, above n 45.

<sup>423</sup> Statista report that 12% of German consumers are ‘aware’ of the Internet of Things as at June 2015: Statista, ‘Share of consumers who are aware of the Internet of Things in Germany in June 2015’ (2015 accessed 6 Aug 2016) <<https://www.statista.com/statistics/458159/consumers-awareness-of-the-internet-of-things-in-germany/>>

<sup>424</sup> Deloitte, ‘Switch on to the connected home’ *The Deloitte Consumer Review* (May 2016 accessed 10 Oct 2017) 5-8 <<https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-16.pdf>> Respondents indicated that smart devices “had the potential’ to make their lives easier and Deloitte conclude retailers need to demonstrate the value proposition more clearly – demonstrate how it works and what it will do for people, for example. Note interest diminished with age: 18- 24 yo (91%), 37% (65 years +).

<sup>425</sup> Deloitte, above n 424: 6

Current global trends also reveal the market is underperforming expectation. Sales are “sluggish”<sup>426</sup> and device demand is “not growing fast enough”<sup>427</sup> to meet 2020 predictions.<sup>428</sup> Consumers complain that devices are too expensive (62%), insecure (47%) and confusing (17%),<sup>429</sup> and identify purchase barriers:<sup>430</sup> known security problems (67%) made consumers more cautious (27%), stopped device use (18%), and postponed purchase (14%).<sup>431</sup> International research largely concurs: globally, 60% of consumers ‘worry’ about CIOT technology, citing trust (62%), security (54%) and physical safety (27%). Accenture warn:

*The consumer technology industry does not have the fundamentals in place – and the consumer trust established – to push into more personalised and sensitive areas ...*<sup>432</sup>

Speculatively, these figures may suggest that many consumers do not understand CIOT terminology, or how it works and thus, mistrust persists: consumers may perceive risk but not understand why (see 1.4 below). This perception, and BE factors such as ‘overconfidence’ (Ch. 6) may explain why consumers buy-in to some CIOT devices (smart fitness for example) but resist others – such as smart car autonomy. Critics also explain slow adoption as an industry failure to market to things consumers “actually care about”<sup>433</sup> – and rampant information asymmetry. As to smart cars for example, most consumers (51%) do not know what an ‘autonomous’ vehicle is, but 79% recognise ‘self-driving’;<sup>434</sup> most (62%) believe full

---

<sup>426</sup> Deloitte, above n 424: 5. Note the potential role of ‘baked-in’ connectivity with the entertainment devices: it is harder to buy a non-smart TV or games console etc. these days. This situation will inevitably flow on into whitegoods as models change over.

<sup>427</sup> Accenture, ‘Igniting Growth in Consumer Technology’ 2016 Accenture Digital Consumer Survey (2016 accessed 24 Mar 2016): 5 < [https://www.accenture.com/\\_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf](https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf)>

Accenture predict that the consumer technology industry’s decade-long unprecedented growth is coming to an end, pointing to (relatively) sluggish growth across all traditional categories such as smartphones, laptops, tablets etc. The study involved thousands of consumers in 28 countries.

<sup>428</sup> This survey involved 28,000 participants across 28 countries (including Australia). Accenture say it reveals a healthy but static market; with growth static on fitness monitors (13%), home surveillance cameras (11%) and home thermostats (0%).

<sup>429</sup> Ibid: 2. The survey identified “prices, security and ease of use”, lack of a “compelling value proposition”, ease of use or experience concerns and product abandonment due to security concerns.

<sup>430</sup> Ibid: 2.

<sup>431</sup> Security also features in terms of price: over five years in the fitness wearables/ smartwatch category, there is a US\$7.4 billion price differential between what consumers who value security want to pay versus those who do not want to pay: Ibid: 9.

<sup>432</sup> Accenture, above n 427: 7.

<sup>433</sup> For example, ‘fitness’ not ‘wearables’; car ‘safety’ over ‘autonomy’. See Talevski, above n 415.

<sup>434</sup> Kelley, above n 375: 11.

autonomy lies beyond their lifetime,<sup>435</sup> would not buy a level 5 smart car (84%),<sup>436</sup> and 80% still want to drive - which suggests a serious disconnect between industry and consumers.<sup>437</sup>

In summary, CIOT is unlikely to live up to its 2020 hype. Aside from technical viability issues,<sup>438</sup> it suffers from four fundamental problems: over optimistic industry-led rather than consumer value perceptions,<sup>439</sup> industry failure to design products consistent with consumer wants (price, security, functionality, etc.),<sup>440</sup> a failure to identify and explain consumer product value,<sup>441</sup> and a brittle assumption that exponential predictions are accurate, regardless.<sup>442</sup> Despite these (and other)<sup>443</sup> concerns, most consumers (90%)

---

<sup>435</sup> Ibid: 12. While this varies with generations, all over 16 agreed. This suggests consumers know little about smart car development or industry progress.

<sup>436</sup> Andrew J. Hawkins, 'Self-driving cars will have to pry the steering wheel from our cold, dead hands, poll says' (28 Sept 2016 accessed 2 Oct 2016) < <http://www.theverge.com/2016/9/28/13076948/self-driving-car-poll-autonomy-kelley-blue-book>>

<sup>437</sup> Accenture identify a lack of "well-articulated consumer solutions so far..." and say technology-led innovation should be driven by "core consumer needs", and respond to "primal human needs". To improve industry 'value', Verto point to creating "consumer-ready" devices and connecting scalable CIOT populations, while Accenture highlight expanding data use and exploitation to increase industry value. Accenture, above n 427: 6. Deloitte argue that IOT technology is predominantly for business or industrial application – rather than consumer use. They suggest that much technology (citing large-screen smartphones, tablets, faster telecommunications network-capability, VOIP and desktop video-conferencing) was driven by consumer-led demands, as opposed to enterprise-led innovation. They suggest that this may explain why IOT innovation has not proceeded as rapidly as initially predicted: Deloitte, 'The Internet of Things ecosystem: Unlocking the Business Value of Connected Devices' (2014 accessed 8 Mar 2016) <[www2.deloitte.com/global/en/..internet-of-things-ecosystem.html](http://www2.deloitte.com/global/en/..internet-of-things-ecosystem.html)> Note as to improving manufacturer returns, Verto, above n 45. See also Accenture, above n 427: 10.

<sup>438</sup> Unless resolved, these will adversely impact upon consumer experience. For example, spectrum availability and licensing, IP address availability requires IPv6, standards and interoperability, which are key to device compatibility, convenience and efficiency - yet are not a practical reality in a presently fractured CIOT marketplace. Finally, the lucrative question as to which software platform will (eventually) be the one upon which all vertical applications of the IOT will be built remains unknown. None of these uncertainties are resolved, though the industry is incentivized to do so as each may constrain CIOT uptake, benefits and value for consumers into the future. Zeichner et al, above n 119 :80. The report observed: "IoT policy areas under review or development coalesce around a few areas, which are: spectrum management, personal privacy, use of IPv6, network resilience and security, open Government data, interoperability and national innovation and competitiveness." ; "Australia is quite behind in take-up and deployment of IPv6 compared to rest of world...": Zeichner, above n 119: 99; The question is well-posed in Matt Turck, 'Making Sense of the Internet of Things' *TechCrunch* (25 May 2013 accessed 8 Feb 2016) < <http://techcrunch.com/2013/05/25/making-sense-of-the-internet-of-things/>>

<sup>439</sup> Critics also explain adoption issues by suggesting that the CIOT industry needs to start marketing its products to things consumers "actually care about" - 'fitness' rather than "wearables", for example: Talevski, above n 408.

<sup>440</sup> Accenture identify a lack of "well-articulated consumer solutions so far..." and say technology-led innovation should be driven by "core consumer needs" and respond to "primal human needs": Accenture, above n 427: 6.

<sup>441</sup> Ibid.

<sup>442</sup> Consumer information seems deficient: 51% of consumers do not know what an 'autonomous' vehicle is, but 79% recognise 'self-driving'. When explained, most consumers (62%) do not believe they will see full autonomy in their lifetime, would not purchase a fully smart car (84%), and 80% still want the option to drive: Kelley, above n 375: 11 – 12. It all suggests information asymmetry and an industry well ahead of consumer markets: Hawkins, above n 436.

<sup>443</sup> The technical challenges remain significant and substantially unresolved, which is a dampener to increased consumer adoption. Issues of consumer inconvenience, cost and confusion prevail. Evans refers to the "fractured" consumer experience created by product silos or individual apps controlling disparate devices, the costs incurred as a result of separate device ecosystems and an "alphabet soup of [competing] protocols": Dave Evans, 'We Need to get the Internet of Things right' *TechCrunch* (19 Apr 2015 accessed 11 Apr 2016) <http://techcrunch.com/2015/04/19/we-need-to-get-the-internet-of-things-right/>

can see 'potential' benefits,<sup>444</sup> and a "future" purchase (65%).<sup>445</sup> Indeed, both metrics considered - consumer intent and actual purchase - suggest that CIOT devices, pushed by industry, will continue to increase in prevalence. If industry can build consumer trust.

#### 1.4 Consumer Trust: ending before it begins?

*... risks to privacy and security undermine consumer trust. And that trust is as important to the widespread consumer adoption of new IOT products and services as a network connection is to the functionality of an IOT device...*<sup>446</sup>

If "...trust in the internet is over",<sup>447</sup> it is questionable if trust in the consumer IOT has even begun. As a critical enabler identified by industry,<sup>448</sup> regulators<sup>449</sup> and analysts alike, a lack of consumer trust or confidence will hinder adoption and threaten future success. Research suggests that consumer confidence is decreasingly<sup>450</sup> "low",<sup>451</sup> privacy and security are a "top barrier" and data-use practices make consumers "uneasy".<sup>452</sup> Analysts predict a looming "privacy class divide",<sup>453</sup> describe current security models as "obsolete"<sup>454</sup> and report that consumers perceive, though do not yet fully understand, the risk and threat implications of a smart world.<sup>455</sup> Further, as consumer awareness increases, other trust-barriers may emerge. For example, ACMA identify three main cloud-industry trust-related barriers: privacy, security and data management, interoperability, vendor lock-in and cross-service portability with

---

<sup>444</sup> Mobile Ecosystem Forum (MEF), 'The Impact of Trust on IoT' Global Consumer Survey (2016 accessed 11 May 2016) <[http://www.mobileecosystemforum.com/wp-content/uploads/2016/04/IoT\\_Exec\\_Summary.pdf](http://www.mobileecosystemforum.com/wp-content/uploads/2016/04/IoT_Exec_Summary.pdf)>

<sup>445</sup> Accenture, above n 427. Perhaps seeking a positive, they perceive an overall consumer perception shift, a newfound openness to adoption and that CIOT will have major B2B and B2C implications by 2020.

<sup>446</sup> Edith Ramirez, 'Opening remarks to the International Consumer Electronics Show' (6 Jan 2015 accessed 5 Jan 2016) <<https://www.ftc.gov/public-statements/2015/01/privacy-iot-navigating-policy-issues-opening-remarks-ftc-chairwoman-edith>>; See also ICDPPC, above n 18; J. Brill, 'The Internet of Things: Building Trust and Maximizing Benefits through Consumer Control' *Fordham Law Review* (2014) 83: 1 205- 217 (26 Feb 2014 accessed 28 Feb 2016) <[https://www.ftc.gov/system/files/documents/public\\_statements/289531/140314fordhamprivacyspeech.pdf](https://www.ftc.gov/system/files/documents/public_statements/289531/140314fordhamprivacyspeech.pdf)>

<sup>447</sup> Paul Brody and Veena Pureswaran, 'Device Democracy Saving the Future of the Internet of things' *IBM Institute for Business Value, Executive Report* (2015 accessed 23 Mar 2016) <<http://iotbusinessnews.com/download/white-papers/IBM-Saving-the-future-of-IoT.pdf>>

<sup>448</sup> The Australian IOT Alliance is very conscious of the trust imperative: see <http://www.iiot.org.au/>

<sup>449</sup> Edith Ramirez, above n 446; FTC, Internet of Things Privacy and Security in a Connected World, *Staff Report* (Jan 2015 accessed 26 Nov 2015) <<https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iortpt.pdf>>

<sup>450</sup> 42% of Americans were more concerned than in the previous year:

<sup>451</sup> J. Groopman and Susan Etlinger, 'Consumer Perceptions of Privacy in the Internet of Things' *Altimeter* (June 2015 accessed 12 Apr 2016): 8 <<http://www.altimetergroup.com/pdf/reports/Consumer-Perceptions-Privacy-IoT-Altimeter-Group.pdf>> Altimeter's 2016 survey received 6900 responses across 24 countries, including Australia (500).

<sup>452</sup> Jeff Evans, 'The Opt-Out Challenge' *Black & Veatch* (March/April 2012) *Electric Light & Power* <<http://bv.com/docs/articles/the-opt-out-challenge.pdf>>

<sup>453</sup> Mark Thompson cited in KPMG, 'Creepy or cool? Staying on the right side of the consumer privacy line' (Nov 2016 accessed 9 Nov 2016) <<https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2016/advisory/creepy-or-cool.pdf>>

<sup>454</sup> Brody, above n 447.

<sup>455</sup> A 2016 MEF survey showed that 60% of consumers have concerns about the "perceived risks and threats" of a connected world: above n 444. The MEF survey studied 5000 mobile media users in eight markets (UK, USA, Brazil, France, Germany, China, India and South Africa) to discover consumer perceptions as to the future of a connected world.

consequent loss of data control, and finally, data sovereignty<sup>456</sup> and inadequate redress mechanisms.<sup>457</sup> These are all also CIOT concerns; it may just be that consumers do not know it, yet.

Most Australians (60%) will cease doing business with companies they do not trust.<sup>458</sup> Studies suggest that almost half of consumers do not trust the IOT,<sup>459</sup> and 85% want to understand data collection practices before using CIOT devices.<sup>460</sup> Consumers privilege trust over user issues such as device ease of use (94%).<sup>461</sup> While Australian research is limited, Fortinet's smart home study reports that 65% of Australians are concerned about data breach, 60% see privacy as important and don't trust IOT data use, 60% agreed they would feel "completely violated..., extremely angry" if smart devices secretly collect and share their information (even anonymously), and 66% want to control their data access and use.<sup>462</sup> KPMG's international study agrees that "indiscriminate personal data collection risks alienating consumers", and that most people are 'concerned' about use of their data (56%).<sup>463</sup> Nielsen concurs; finding that unknowing or non-consensual use is the greatest CIOT concern (53%),<sup>464</sup> and Altimeter reports that 60% are uncomfortable with companies 'selling' their data.<sup>465</sup> Consumers are "distinctively wary" about smart home information, which may slow uptake, and potentially constrain industry 'value-add' capabilities. For example, most consumers do not want to disclose their online search history, location, address and medical records (80%), or use apps collecting their personal data (66%) or have their online-shopping data sold (75%) and surprisingly, only half would trade privacy for incentives such

---

<sup>456</sup> 'Data sovereignty' refers to data ownership and access, including where data is stored overseas.

<sup>457</sup> ACMA, 'The cloud: services, computing and digital data—Emerging issues in media and communications', *Occasional Paper 3* (June 2013); 'Cloud computing- emerging issues' (2015) <<http://acma.gov.au/theACMA/emerging-issues-cloud-computing>>

<sup>458</sup> OAIC, 'Community Attitudes to Privacy' *Research Report & Survey* (2014 accessed 8 Apr 2016) <<https://www.oaic.gov.au/resources/engage-with-us/community-attitudes/oaic-community-attitudes-to-privacy-survey-research-report-2013/2013-community-attitudes-to-privacy-survey-report.pdf>>

<sup>459</sup> Accenture, above n 427.

<sup>460</sup> TrustE, '2014 TRUSTe Privacy Index: Internet of Things Edition' (February 2014 accessed Mar 2016)

<<https://www.truste.com/resources/privacyresearch/>

us-internet-of-things-index-2014/.

<sup>461</sup> Deloitte, 'Deloitte Australian Privacy Index 2016: Trust without Borders' (2016 accessed Jun 2016): 19- 21

<<http://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index-2016.html>>

<sup>462</sup> For Australian statistics see Electrical Connection, 'Fortinet reveals Internet of Things: Connected Home survey results' connected. (27 May 2014 accessed 4 Apr 2016) <<http://www.connectedhome.com.au/fortinet-reveals-internet-things-connected-home-survey-results/>> For the global and US statistics, see Fortinet, 'Fortinet Reveals Internet of Things: Connected Home' *Survey Results* (23 Jun 2014 accessed 2 Jun 2016) <

<http://investor.fortinet.com/releasedetail.cfm?releaseid=855992>> Australian: US figures (in brackets) for these metrics were: 65% (68%) are concerned about data breach, 60% (57%) see privacy as important and do not trust how their IOT data would be used, 60% (67%) agreed they would feel "completely violated..., extremely angry" and take action if smart device were anonymously or secretly collecting and sharing their information, and 66% (70%) of people want to control both access to and use of their data.

<sup>463</sup> Brody, above n 447.

<sup>464</sup> Nielsen, 'The Internet of Things: Can It Find a Foothold with American Audiences Today?' (Nov 2014 accessed 3 Mar 2016) <<http://www.affinnova.com/resource-story/internet-of-things/>>

<sup>465</sup> Groopman, above n 451: 10. 45% are "very or extremely" uncomfortable with companies 'using' their data.

as free or cheaper products.<sup>466</sup> Turow identifies this as a “fallacy”, but this does not necessarily override consumer perception.<sup>467</sup> Indeed, consumers see many CIOT capabilities as “creepy”, not “cool”. “Creepy” includes: a free fitness tracker sharing data with the wearer’s employer (55%); smart car telematics reducing insurance premiums but informing police of dangerous driving (55%); smart meter home occupant analytics<sup>468</sup> or a cheap TV which monitors viewing habits (53%); smart device apps accessing contacts, photos and browsing history (84%); smart car geo-location data being used to offer nearby services, and device advertising using a consumer’s name [78%].<sup>469</sup> Studies confirm that consumers are uncomfortable with data use absent personal consent and very uncomfortable with their data being sold. While discomfort levels do increase with age and decrease with technology exposure,<sup>470</sup> incentives<sup>471</sup> or other variables;<sup>472</sup> the conclusions still hold firm - even with millennials.<sup>473</sup>

Analysts assert that trust solutions lie in industry hands. (Mis)trust is a business reputational risk with a financial cost: customers avoid non-privacy protective companies,<sup>474</sup> data as ‘currency’<sup>475</sup> needs rethinking, as does communicating CIOT benefits and its business models.<sup>476</sup> Clearly, CIOT providers must better “articulate and notify” consumers of data use: for example, most Australians (67%) do not

---

<sup>466</sup> See Joseph Turow, Michael Hennessy & Nora Draper, ‘The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation’, *University of Pennsylvania Annenberg School of Communications* (5 June 2015 accessed 3 Mar 2016) <<https://www.asc.upenn.edu/sites/default/files/Turow>> Turow points to the ‘trade-off fallacy’ whereby consumers express clear concerns as to data collection, use and sale, yet want the features which are usually used to incentivize data sharing or collection practices.

<sup>467</sup> An Accenture online survey found 60% want ‘real-time promotions’ (which often involve tracking) but do not want retailers to know their location (80%) and only 14% were prepared to share browsing history. Only 20% percent want retailers to know their location and just 14% are comfortable sharing their browsing history.

<sup>468</sup> Evans, above n 452; Brody, above n 447: 9

<sup>469</sup> Ibid.

<sup>470</sup> Other factors such as environmental and age differences vary. The rural and older segments report higher discomfort with data use and sales than the general population. In contrast, Lux Research suggest a generational change in privacy attitude to “embrace and accept”, c/f Altimeter, Deloitte, above n 461.

<sup>471</sup> Turow, above n 466.

<sup>472</sup> Analysts and academics are grappling with conflicting consumer evidence depending upon variables such as to the data or use involved, consumer attitude and age, and international / regional differences - which KPMG suggest, presents an unwelcome prospect for data collectors and advertisers alike.

<sup>473</sup> Altimeter’s study shows that while older generations express a more extreme concern as to privacy, “even for the youngest segment, well over 40% indicated concern or extreme concern for each type of data use”: Above n 451: 14. c/f Lux Research above n 26 which speculates (e.g. the go-pro / selfie generation) that younger generations embrace and live a ‘lifelog’ experience and are therefore far less caring of ‘privacy per se’: Lux, above n 26. Deloitte found that people complain more about privacy with age: Deloitte, above n 461: 11.

<sup>474</sup> Altimeter, above n 451; TRUSTe, ‘US Consumer Data Privacy Study: Consumer Privacy Edition’ (2014 accessed 4 Apr 2016) <<http://www.slideshare.net/trusteprivacyseals/2014-usconsumer-data-privacy-study-consumer-privacy-edition-fromtruste>>

<sup>475</sup> Timothy Morey, Theodore Forbath and Allison Schoop, “Customer Data: Designing for Transparency & Trust,” *Harvard Business Review* \*May 2014 accessed 3 Mar 2016) <<https://hbr.org/2015/05/customer-datadesigning-for-transparency-and-trust>>

<sup>476</sup> Accenture believe this will require an ethical framework: “...a framework for ethical communications businesses can adopt to better engage, build trust, and educate consumers around the use of their connected device data.”

want their data sent overseas, but 81% of apps in one study did so,<sup>477</sup> including technology<sup>478</sup> and smart self apps. IBM warn that current CIOT ecosystem trust may be a “fantasy”, arguing that trust is “very hard to engineer and expensive, if not impossible, to guarantee”.<sup>479</sup> They recast responsibility upon providers, and CIOT consumers may agree: a recent Canadian study found that only 27% of consumers thought smart car benefits outweighed privacy risks and most (74%) believed that car manufacturers should be required to “...design technology that would mean consumers wouldn’t have to choose between the benefits of technology and protecting privacy..”<sup>480</sup> These consumers do not believe industry assurances that CIOT data collection, storage and analysis, and anonymised data sold is privacy-safe, or that data sold will be de-identified - and with good reason.<sup>481</sup> Also in the privacy context, Deloitte identify five trends: firstly, more discerning consumer expectations, secondly, consumers want best practice personal information management as an “ethical obligation”, thirdly, that contractually-controlled third party data practices entail risks, fourthly, that privacy is a globalised expectation, and finally, a growing need to improve the data-commercialisation versus consumer choice (im)balance.<sup>482</sup> It is a salient warning for industry trust, one where long-term industry trust collides with short term financial benefits of data collection and exploitation.

CIOT consumer mistrust is on the industry radar, and with much-publicised security and privacy flaws, negative consumer awareness is rising. Remarkably, despite the many powerful players involved, the industry has yet, failed to disprove its consumer costs, market its benefits or to enhance the image of a smart world with consumers.

---

<sup>477</sup> These were government, banking and finance, social media, energy, health and fitness, insurance, retail, telecommunications, higher education, travel and transportation, real estate, technology and media.

<sup>478</sup> All data collected by this sector was sent overseas: Deloitte, ‘Global Mobile Consumer Survey: Southeast Asia Survey’ (Dec 2015 accessed 8 Mar 2016): 9 <<https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-2015-global-mobile-consumer-survey-southeast-asia-edition.pdf>>:

<sup>479</sup> Brody, above n 447.

<sup>480</sup> Canadian Automobile Association, ‘Survey’ cited here: <https://fipa.bc.ca/connected-car/>> 50% of respondents thought that smart car technologies put their privacy at risk while offering little benefit to consumers. Only 37% of respondents would agree to monitoring in exchange for an insurance discount, while 53% would not.

<sup>481</sup> Accenture’s 2014 online study suggests that 80% of consumers aged 20-40 in the US and the UK believe total privacy in the digital world is over: Accenture, ‘Eighty Percent of Consumers Believe Total Data Privacy No Longer Exists, Accenture Survey Finds’ (28 May 2014 accessed 2 Jun 2016) <<https://newsroom.accenture.com/news/eighty-percent-of-consumers-believe-total-data-privacy-no-longer-exists-accenture-survey-finds.htm>> This is not the Zuckerberg line that privacy is ‘dead’ as some controversially assert; as Svantesson comments, “To say that we do not need a right of privacy because our modern information society does not cater for privacy is akin to saying that we do not need a right to water in a desert – the removal of a fundamental right is justified by reference to the environment being hostile to, or making difficult the exercise of, such a right...”: Dan Svantesson, *Extraterritoriality in Data Privacy Law* (Denmark Narayana Press, 2013) :30.

<sup>482</sup> Deloitte, above n 461: 19- 21.

## 1.5 Conclusion – chapter one

Futurist Daniel Burris says that people do not think “big enough” when thinking about the internet of things.<sup>483</sup> As this chapter suggests, CIOT is set to change the world as we know it. But the predictions and their exponential-ities attract serious criticisms worth factoring into the debate: initial predictions failed to meet expectation by 2016; tech adoption rates often spike during initial production periods and then growth rates slow;<sup>484</sup> new technology may emerge and carve into or reshape a market rather than adding to it;<sup>485</sup> needed enablers may become disablers (for example, Australian road infrastructure)<sup>486</sup> and finally, a ubiquitous CIOT vision without commercial justification, is “...stretching the concept”. Arguably, every consumer device embedded with an IP address is, without a commercial justification, not inevitable – consumer disinterest in the ‘smart fridge’ or smart device contracting<sup>487</sup> are off-cited.<sup>488</sup> Finally, global internet access remains an issue – while increasing,<sup>489</sup> it is still only 50%<sup>490</sup> - so no matter how sensed-up, unconnected consumer ‘things’ are dead. But even if 2020 projections are half true, it is difficult to comprehend the social impacts of its pervasive nature, the complex technology-mix involved and business – consumer impacts. Overlaid by the myriad privacy, trust, data sovereignty and security implications of the “panopticon economy”<sup>491</sup> – these factors all collide to create “one of the biggest challenges of the next century”.<sup>492</sup>

---

<sup>483</sup> Daniel Burris, ‘The Internet of Things is far bigger than anyone realises’ *Wired* (Nov 2014 accessed 1 April 2016) <http://www.wired.com/insights/2014/11/the-internet-of-things-bigger/> and Burris, above n 15 (Part 2).

<sup>484</sup> For example, smartphone sales were 1B units worldwide in 2014, but Q5 2015, showed slowest sales growth since 2008 at 9.7%: Hosain, above n 267. There is evidence of slowing demand and reduced market share across all vendors (excluding Apple) and even Apple’s growth has declined after three quarters of declining sales

<sup>485</sup> Chinese fit band products retail at \$25 c/f Fitbit price points start at \$60- 250 USD ranging to hundreds of dollars: Pressman, above n 57.

<sup>486</sup> NTC, above n 397 and 408.

<sup>487</sup> Deloitte, above n 461: 10.

<sup>488</sup> Jamie Carter, ‘Forget smart fridges: The Industrial Internet of things is the real revolution’ *techradar.pro* (10 Mar 2015 accessed 8 Apr 2016) <<http://www.techradar.com/au/news/world-of-tech/forget-smart-fridges-the-industrial-internet-of-things-is-the-real-revolution-1287276>> “Many people out there have overestimated the market size for wearables and most importantly have overestimated the need for them”: Creative Strategies cited in Pressman, above n 57.

<sup>489</sup> 192 countries have active 3G mobile networks. By 2019 forecasts predict mobile internet penetration will reach 71% and use per device will more than triple: Internet Society, above n 79.

<sup>490</sup> World internet penetration rates as at 30 June 2016 are: Nth America (89%), Europe (73.9%), Australia/ Oceania (73.3%), Latin America/ Caribbean (61.5%), Middle East (57.4%), Asia (45.6%) and Africa (28.7%). World average is 50.1%: Miniwatts Marketing Group, ‘Internet World Penetration Rates by Geographic Regions- June 2016’ (accessed 2 Nov 2016) <<http://www.internetworldstats.com/stats.htm>> See also Ibid. Well over 1 million apps are available globally, which have been downloaded more than 100 billion times.

<sup>491</sup> Steve Ranger, ‘Inside the panopticon economy: The next internet revolution, privacy and you’ *ZDNet* (2 Mar 2015 accessed 7 Apr 2016) < <http://www.zdnet.com/article/inside-the-panopticon-economy-privacy-the-iot-and-you/>>

<sup>492</sup> Ibid.

## **PART II      A NORMATIVE FRAMEWORK TO IDENTIFY KEY ISSUES**

---

### **Chapter 2. Adopting a policy framework**

**Part I** of this paper has contextualised the Australian CIOT “market” including its scale, scope, stakes and predicted trajectory. This **Part II** sets up a policy-based approach to evaluating that market and to informing potential responses, by enabling a review of its detrimental impacts upon consumers collectively as well as specifically. It commences with the research question, justifies the smart category approach, adapts an analytic Australian policy framework, and then identifies smart home, car and self experience locally and internationally, to illustrate potential consumer ‘detriment’. In summary, **Parts II** and **III** locate the problems which justify the conclusions and recommendations set out in **Part IV**.

#### **2.1      Research Question**

This thesis considers the following research question:

**How can Australian regulators and policy makers best fulfil the objectives of the Australian Consumer Policy Framework to improve consumer wellbeing through empowerment and protection, cognisant of Australian consumer laws and privacy principles, while fostering the twenty-first century consumer internet of things, as exemplified by smart cars, home and self?**

#### **2.2      Scope & smart category justification**

This thesis has a limited consumer IOT and consumer protection law scope delineated in **Annex. A.1**: briefly, it excludes the industrial IOT, and consumer IOT contexts beyond the smart home, car and self. This decision does not reflect perceived consumer risk or that ‘smart’ issues do not overlap.<sup>493</sup> Rather, the selected smart categories represent the dominant CIOT purchase sectors internationally, and illustrate three 2016 Australian snapshots: one already market-established by consumer demand (smart self), one poised for implementation largely through provider decision-making (smart home) and one which is gradually but inevitably filtering into the market through supplier and government impetus (smart cars). The smart self evidences consumer demand shaped by fashion and utility, with evolving uses in health, insurance and other sectors, the smart home lacks discernible consumer demand but is driven

---

<sup>493</sup> As the discussion later suggests, the Part IV draft principles may apply in differing CIOT contexts.

by whitegoods and software manufacturers baking-in smart capacities<sup>494</sup> while entities such as insurers and utilities embrace the technology for economic and efficiency reasons, and finally, smart cars represent an industry-led public policy preference: smart(est) cars will save lives and benefit non-drivers, the environment and traffic management, which is in the public interest, and therefore embraced internationally, regardless of current consumer demand or preference. As this demonstrates, these three categories comprise three significant consumer markets which will affect most Australians, and thus, offer ample scope to examine CIOT in Australia.

The thesis focusses solely upon the main consumer protection laws in Australia: the federal Australian Consumer Law and the Australian Privacy Principles. As one of the first Australian studies of its kind in terms of close legal analysis of the consumer IOT, it is both useful and relevant to examine the principal legislative instruments and to identify any deficiencies in the frontlines of consumer and privacy protection in Australia.<sup>495</sup> To that end, the thesis adopts the recently reaffirmed<sup>496</sup> Australian Consumer Policy Framework (**ACPF** or **Framework**) objective as the underlying normative theme and to adapt selected regulatory policy assessment processes which are international best practice consumer policy-making methodologies.<sup>497</sup> This section briefly explains the Framework, commences an analysis and plots the course for the consideration of potential CIOT detriments throughout **Part III** and the recommendations in **Part IV**.

### 2.3 ACPF objectives

Consumer policy is "...a suite of government policies that deal with purchase of and use of consumer goods and services".<sup>498</sup> It focuses upon consumer market interaction, and is often informed by economic

---

<sup>494</sup> Samsung announced that by 2017, "90% of all Samsung products will be IoT devices — and that includes all our televisions and mobile devices... And five years from now, every single piece of Samsung hardware will be an IoT device, whether it is an air purifier or an oven."- Samantha Murphy, 'Samsung: By 2020, all of our products will be connected to the web' *Mashable Australia* (6 Jan 2015 accessed 20 Feb 2016) <<http://mashable.com/2015/01/05/samsung-internet-of-things/#4PJcq4DVGgqR>>

<sup>495</sup> Of course, this excludes many potentially relevant legal areas: see Annex. A1.3.

<sup>496</sup> Consumer Affairs Forum (CAF) consists of all Cth, State and NZ ministers in the areas of fair trading and consumer affairs, with the task to consider matters of national significance and develop a consistent approach where practicable: CAF (Legislative and Governance Forum on Consumer Affairs with Consumer Affairs New Zealand), 'Strategic Agenda 2015-2017' (2015 accessed 2 Jan 2016): 4 <[http://consumerlaw.gov.au/files/2015/09/CAF\\_strategic\\_agenda\\_2015.pdf](http://consumerlaw.gov.au/files/2015/09/CAF_strategic_agenda_2015.pdf)> One aspect of the 2016 ACL review process was to consider the policy framework, which appears to be well regarded: ACCC, 'Australian Consumer Law Review Interim Report' (Oct 2016 accessed 8 Oct 2016) <http://consumerlaw.gov.au/review-of-the-australian-consumer-law/have-your-say/>

<sup>497</sup> These derive from five main sources: OECD Recommendation on Consumer Policy Decision Making, Europe Economics (EE) reports to the European Commission, the OECD Consumer Policy Toolkit (Toolkit), the Australian Government Toolkit Companion 'Consumer Policy in Australia' (Companion) and the Australian Consumer Law Review Interim Report.

<sup>498</sup> Productivity Commission, 'Review of Australia's Consumer Policy Framework' (30 Apr 2008): II.2 <<http://www.pc.gov.au/inquiries/completed/consumer-policy/report/consumer2.pdf>>

analysis and consumer problem identification.<sup>499</sup> Consumer policy is also increasingly concerned with non-economic factors; such as political, social and moral aspects relevant to policy issues.<sup>500</sup> In 2009, the Intergovernmental Agreement for the Australian Consumer Law<sup>501</sup> adopted a national policy framework to enhance consumer protection and policy development, implementation and enforcement in Australia. Recently strategically reaffirmed,<sup>502</sup> the National Consumer Policy objective<sup>503</sup> states the normative policy aspiration underlying this thesis:

**...to improve consumer wellbeing through consumer empowerment and protection, to foster effective competition and to enable the confident participation of consumers in markets in which both consumers and suppliers trade fairly..."**

The Framework has six operational objectives<sup>504</sup> which are recast here under three main goals:

**Goal (1): to empower and protect consumers**

- to ensure that consumers are sufficiently well-informed to benefit from and stimulate effective competition;
- to meet the needs of those consumers who are most vulnerable or are at the greatest disadvantage

**Goal (2): to improve consumer confidence and wellbeing**

- to promote goods and services as safe and fit for their purposes
- to provide accessible and timely redress where consumer detriment has occurred

**Goal (3): to foster a fair and competitive consumer marketplace**

- to prevent practices which are unfair
- to promote proportionate, risk-based enforcement

These objectives also presuppose four concepts accepted by this thesis:

---

<sup>499</sup> Australian Government, 'Consumer Policy in Australia. A companion to the OECD Consumer Policy Toolkit' (2011 accessed 2 Mar 2016): 9

<[http://www.consumerlaw.gov.au/content/consumer\\_policy/downloads/Companion\\_to\\_OECD\\_Toolkit.pdf](http://www.consumerlaw.gov.au/content/consumer_policy/downloads/Companion_to_OECD_Toolkit.pdf)>

<sup>500</sup> Ibid: 11.

<sup>501</sup> In 2009, the Intergovernmental Agreement for the Australian Consumer Law adopted a national policy framework: Intergovernmental Agreement for the Australian Consumer Law, (2 Jul 2009)

[www.coag.gov.au/sites/default/files/IGA\\_australian\\_consumer\\_law.pdf](http://www.coag.gov.au/sites/default/files/IGA_australian_consumer_law.pdf) This provides in para. C that the ACL is jointly administered by federal and state/territory consumer law regulators.

<sup>502</sup> CAF is tasked to consider matters of national significance and to develop a consistent approach where practicable: CAF above n 496: 4.

<sup>503</sup> Ibid, paragraph D.

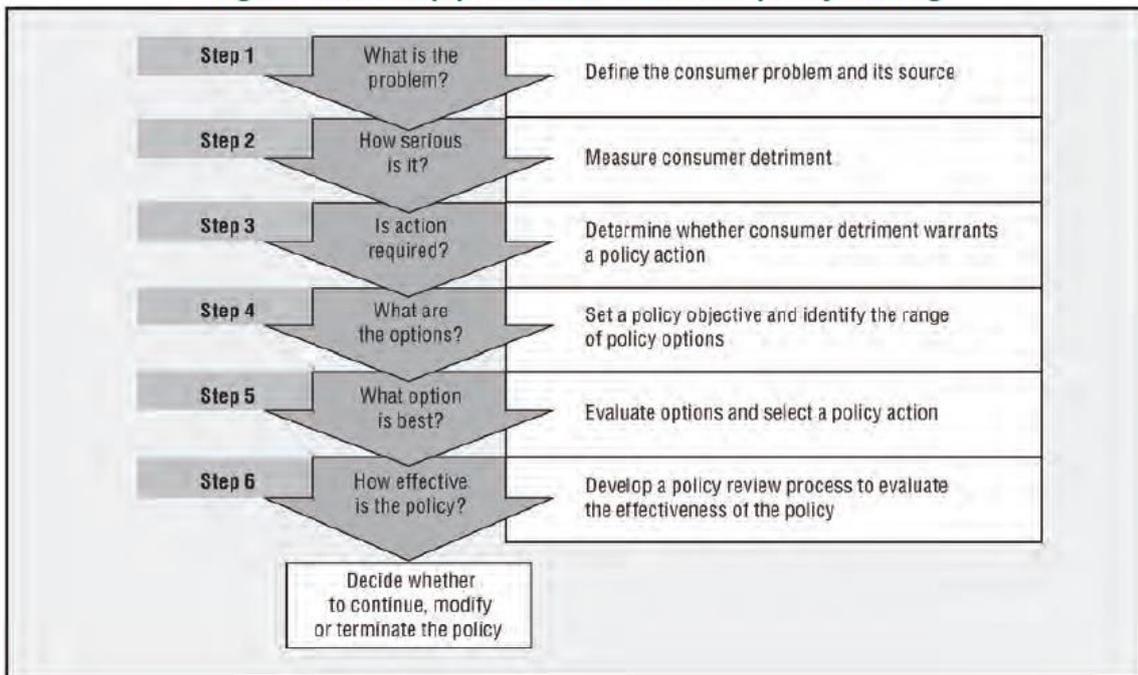
<sup>504</sup> Intergovernmental Agreement, above n 500: Recital C.

- that consumer wellbeing<sup>505</sup> (as opposed to economic exploitation) is a laudable social, political and economic policy objective, and is enhanced by empowered<sup>506</sup> and educated control and choice, as well as regulatory protection (hard or soft law and/ or other protective mechanisms);
- that effective competition is good for markets and produces desirable consumer outcomes;<sup>507</sup>
- that consumers have the right to be confident within the marketplace; and
- finally, that fairness is a desirable marketplace objective.

## 2.4 Adapting a consumer policy framework approach

Australia uses the OECD Consumer Policy Toolkit to guide its consumer policy development, which is detailed by flowcharts in **Annex. C** and summarized below:<sup>508</sup>

**Figure 1: Six-Step process for consumer policy making**



Source: OECD Consumer Policy Toolkit.

Graphic 2.1 Six-Step process for Consumer policy-making

Source: OECD<sup>509</sup>

<sup>505</sup> The EC assert that “consumer protection is at the heart of well-functioning markets”: OECD, ‘Consumer policy toolkit’ (OECD Publishing, 9 Jul. 2010): 112 <<http://www.oecd.org/sti/consumer/consumer-policy-toolkit-9789264079663-en.htm>>

<sup>506</sup> This is found in the European Consumer Agenda and funded by its Consumer Programme: European Commission, ‘A European Consumer Agenda-Boosting confidence and growth’ (2012): 225

<[http://ec.europa.eu/consumers/archive/strategy/docs/consumer\\_agenda\\_2012\\_en.pdf](http://ec.europa.eu/consumers/archive/strategy/docs/consumer_agenda_2012_en.pdf)>

<sup>507</sup> The 2008 Australian Productivity Commission Review found that educated and informed consumers are a best defence against predatorial firms, as well as create effective demand for competitive and innovative markets: above n 498.

<sup>508</sup> Australian Government, above n 499.

<sup>509</sup> OECD, above n 505: 11. OECD (2010), Consumer Policy Toolkit, OECD Publishing, Paris.

These steps are a guide and not prescriptive.<sup>510</sup> It is therefore proposed to *adapt* this approach – to identify problems, measure detriment (as practicable) and discern its (potential) significance, and to propose policy options – as the guiding methodology of this thesis.<sup>511</sup> The process requires and justifies the lengthy exploration of CIOT detriment and legal ‘gaps’ throughout Part III (**Ch. 3 – 6**), the process of formulating policy proposals (**Ch. 7**) and the ultimate recommendations and draft principles in **chapter 8**.

## 2.5 Applying the adapted Framework

### 2.5.1 Step 1: Problem definition & source

The first step involves determining the consumer problem from the consumer’s perspective, and its source, using three questions:

- (1) What is the problem from a consumer’s perspective?
- (2) What is its source – for example, business conduct, informational, behavioural, market or regulatory failure?
- (3) Which agencies are best equipped to address the problems, if any?<sup>512</sup>

Consumer ‘problems’ which may require regulatory intervention, include price, quality or safety, lack of timely consumer redress or evidence of consumer decisions “...inconsistent with their personal preferences and self-interests”.<sup>513</sup> This thesis identifies six main potential problems: complexity, security, performance and safety, privacy, consent and big data discrimination. Problem identification may occur through a range of resources: in this thesis, recourse is made to international cases and research by public,<sup>514</sup> private, consumer or international bodies; public hearings; academic commentary and the media.<sup>515</sup> Consumer cases are yet few and complaints data not readily available. While these may be the source most suggestive of consumer problems, it seems probable that in a nascent, complex and high tech environment, consumers are less able to identify or be alerted to problematic issues relating to CIOT

---

<<http://dx.doi.org/10.1787/9789264079663-en>> Graphic licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 IGO (CC BY-NC-SA 3.0 IGO)

<sup>510</sup> Above n 499: 7.

<sup>511</sup> As Annex C. suggests, these steps ordinarily require substantiating economic analysis (where practicable) at various steps, as well as a post-implementation policy evaluative process for step 6; obviously, there is little of the former as to the Australian market, so neither step is fully completed.

<sup>512</sup> This questions addresses capacity and resources which are not relevant here: OECD, above n 505: 114.

<sup>513</sup> OECD, above n 505: 116.

<sup>514</sup> See for example, McKinsey, above n 22 and 28; Verizon, above n 312 and Cisco, above n 98: 13, all of which are pro-CIOT but recommend that regulatory change is required.

<sup>515</sup> Ibid.

product information, performance and quality, and potentially questionable market practices affecting their wellbeing. As such secondary resources assume greater significance, as identified in Annex. B. and discussed in Part III.

Problem	Possible source(s)	Agency & chapter
<b>Complexity: Consumers confused by product and industry complexity</b>	Business conduct (design issues) Informational failure (complexity and cognitive overload) Consumer behaviour (heuristics, overconfidence, framing) Regulatory failure (low consumer education or proactive enforcement)	ACCC (limited) <b>Ch. 1</b>
<b>Security: Consumers confused by complex product security – is it secure or how to make it secure?</b>	Business conduct (design issues) Business conduct (framing) Informational failure (complexity and volume) Consumer behaviour (heuristics, overconfidence, framing, defaults) Regulatory failure (low consumer education; legal gaps; low enforcement)	ACCC (limited) <b>Ch. 3</b>
<b>Performance &amp; safety: Suppliers or products do not fulfil their promises or meet consumer expectation</b>	Business conduct (fraudulent sale deceptive sales; unfair contract terms, unconscionability; competitive issues) Consumer behaviour (overconfidence, framing) Regulatory failure (low enforcement, international supply chains) Consumer behaviour (heuristics, overconfidence, framing)	ACCC <b>Ch. 4</b>
<b>Privacy: Consumers confused by complex product data flows and privacy – who has it, is data private or how to make it so?</b>	Business conduct (informational issues) Informational failure (complexity and volume) Consumer behaviour (heuristics, overconfidence, framing)	OAIC <b>Ch. 5</b>
<b>Consent: Consumers do not understand product ‘legals’ (terms and conditions, instructions, privacy and software terms)</b>	Business conduct (misleading/unfair terms; exploitation of ‘consent’) Business conduct Informational failure (complexity and overload) Regulatory failure (complexity, length & access may make terms unfair or beyond consumer competence to understand; inadequate enforcement)	OAIC ACCC <b>Ch. 6</b>
<b>Data analytics &amp; discrimination:</b>	Business conduct (informational and disclosure issues)	ACCC, OAIC, &

Consumers unaware that data is stored and may be used by others or how it is used	Business conduct (security and anonymisation failures) Regulatory failure (low consumer education or proactive enforcement) Consumer behaviour (heuristics, overconfidence, framing)	Anti-discrimination Commissioner (all limited) <b>Ch.3</b> (briefly)

Table 2.1 Consumer ‘problem’ identification  
Source: author

The final question is which regulator is appropriate to address these problems. Consumer policy responsibility lies with Treasury,<sup>516</sup> with the ACCC and related state bodies as regulators. Given the privacy implications of CIOT policy and regulation, the OAIC is also significant, ACMA is relevant as to consumer telecommunications issues, as may be ASIC, police and others in (respectively) corporate regulation and criminal law contexts.<sup>517</sup> Given the consumer focus, and reflecting the Productivity Commission’s recommendations for (open) data consumer regulation,<sup>518</sup> this paper concentrates upon the ACCC and OAIC as principal regulators hereafter.

### **2.5.2 Step 2: Measure consumer detriment**

*“...the growing collection, processing and use of consumer transaction data for commercial ends ...is proving an increasingly important source of competitive advantage [which could be] an increasing source of consumer detriment...”<sup>519</sup> - UK CMA*

<sup>516</sup> ACL and consumer policy issues are generally referred to the Policy and Research Advisory Committee of the Standing Committee of Officials of Consumer Affairs. See [www.treasury.gov.au](http://www.treasury.gov.au). where Infrastructure, Competition and Consumer Division has general consumer policy responsibility. The ACCC is the relevant regulator. For telecommunications, the relevant regulator is the ACMA, and for therapeutic goods, see the Therapeutic Goods Administration.

<sup>517</sup> In a privacy context, complaints resolution crosses over sectoral external resolution schemes. For example, both ACMA and Telecommunications Industry Ombudsman operate in telecommunications issues.

<sup>518</sup> The PC recommends a *Data Sharing and Release Act* which proposes to increase individual control over data held about them via a new Comprehensive Consumer Right, with the ACCC as key regulator, which it justifies by asserting that “competition and consumer policy lies at the heart of the proposed changes”: PC, above n 190: Ch. 9.

<sup>519</sup> David Currie, ‘The new Competition and Markets Authority: how will it promote competition?’ *Beesley Lecture* (7 Nov 2013 accessed 10 Dec 2016) < <https://www.gov.uk/government/speeches/the-new-competition-and-markets-authority-how-will-it-promote-competition>>

'Consumer detriment' is an outcome of a consumer problem which is often difficult to measure. The EU defines it as consumer "... harm or damage",<sup>520</sup> while the OECD refers to a reduction in economic welfare.<sup>521</sup> The *Companion* cites market outcomes falling short of their potential, resulting in consumer "welfare losses".<sup>522</sup> Examples include where consumers are misled into purchases, pay more than they would have "had they been better informed"; experience unfair contract terms; or where goods or services are dangerous or defective, fail to meet reasonable expectations as to quality, performance or delivery, or fail to meet operational expectation, information provided or where delivery is not timely.<sup>523</sup> It has many forms, and its effects may be uniform, individual or variable.<sup>524</sup>

*Consumer detriment ... can be structural<sup>525</sup> in nature (i.e. affecting all consumers) or personal;<sup>526</sup> apparent to consumers or hidden; and financial or non-financial. Consumer detriment may be apparent to consumers immediately,<sup>527</sup> may take time to emerge<sup>528</sup> or remain hidden.<sup>529</sup>*

Personal and structural detriments may interact and overlap. As this paper is not an economic analysis, it does not distinguish between the two, as both prima facie affect consumers detrimentally.<sup>530</sup> While non-financial detriments are not readily measurable, their cost is as high as 25% of all economic costs.<sup>531</sup> Examples include:

---

<sup>520</sup> European Commission, 'Handbook to Assess Consumer Detriment' (n.d.)

<[http://ec.europa.eu/consumers/consumer\\_evidence/market\\_studies/docs/handbook\\_consumer-detriment.pdf](http://ec.europa.eu/consumers/consumer_evidence/market_studies/docs/handbook_consumer-detriment.pdf)>

<sup>521</sup> OECD, above n 505: 52

<sup>522</sup> Australian Government, above n 499: 19.

<sup>523</sup> OECD, 'OECD Recommendation on Consumer Policy Decision Making' (Mar 2014 accessed 5 Jun 2016)

<<http://www.oecd.org/sti/consumer/Toolkit-recommendation-booklet.pdf>>

<sup>524</sup> It may affect one group but not others, or exhibit a 'waterbed effect', so that some consumers benefit while others lose: OECD: above n 505: 56.

<sup>525</sup> Structural detriment involves the "ex ante reduction of consumer surplus" rather than on ex post outcomes of consumers in aggregate: Ibid 4.

<sup>526</sup> Personal detriment involves "ex post outcomes for those consumers who have a negative experience" (based upon reasonable expectations) and comprises both financial and non-financial detriment (which includes time lost and psychological detriment. EE comment: "We suggest that personal detriment should be assessed against a counterfactual of "reasonable expectations" rather than "expectations", partly because the latter might lead to under-estimation of the detriment suffered by vulnerable groups who may have low expectations.": Ibid: 4.

<sup>527</sup> The OECD use an (obviously) defective good as an example of this.

<sup>528</sup> Experience goods.

<sup>529</sup> Credence goods. An example might be a good that is leaching a chemical, of which a consumer is unaware.

<sup>530</sup> Structural detriments can flow on from personal detriment; OECD suggest that personal detriments may decrease consumer confidence in a market which may decrease transactions occurring in that market and so a decline; and decrease consumer confidence in a particular sales channel – thereby decreasing the range of product choice and / or weaken competition within that channel" OECD, above n 505: 76.

<sup>531</sup> This was applied by the Productivity Commission, 'Consumer policy framework' *Inquiry Report* (8 May 2008 accessed 20 Jan 2016) <<http://www.pc.gov.au/inquiries/completed/consumer-policy/report>>

Financial detriment (tangible – inconvenience time and money)	Non-financial detriment (intangible - limit choice & opportunity)
<b>Lost income due to injury/ time</b> <b>Cost to repair or replace</b> <b>Inflated prices</b> <b>Flawed product cost (e.g. where products fail to meet reasonable expectations based upon misleading information)</b> <b>Reduction in asset value (e.g. defective smart car is worth less)</b> <b>Other consequential costs: fire damage to property etc.</b> <b>Cost of expert advice</b> <b>Administrative, postage and travel costs to seek redress</b>	Psychological or emotional (anger, stress, embarrassment, disappointment etc.) Injury or adverse health effect Reduced choice Privacy breach or compromise of personal information Time to seek redress Inconvenience

Table 2.2 Financial & non-financial detriments  
 Source: Adapted from *Europe Economics & the OECD*<sup>532</sup>

Consumer detriment measurement tools include:

- Commissioned research providing qualitative appraisals and quantitative data;
- Statistics as to consumer behaviours, complaints data, enforcement data, other market comparison and information from international bodies;
- Information from specific interest groups (noting their bias and focus);
- Court judgements and enforcement actions may illustrate legal problems, market failures or “persistent market problems”.<sup>533</sup>

The OECD cites other common signs and (market) situations likely to evidence detriment,<sup>534</sup> as follows:

- Consumer complaints data;
- Evidence of unfair contract terms, or misleading advertising or unfair marketing practices like fraud;
- Complex products: complexity makes comparison difficult and may result in sub-optimal purchase decisions;

<sup>532</sup> Europe Economics, ‘Assessing the Impact of Policy on Consumer Detriment’ (2007 accessed 4 Jan 2016) <[http://ec.europa.eu/consumers/consumer\\_evidence/market\\_studies/docs/handbook\\_consumer-detriment.pdf](http://ec.europa.eu/consumers/consumer_evidence/market_studies/docs/handbook_consumer-detriment.pdf)>and OECD, above n 505: 55.

<sup>533</sup> Australian Government, above n 505: 19- 20.

<sup>534</sup> OECD, above n 505: 57.

- Products with high switching costs or where search/ switching rates are low: detriment may arise where switching products costs consumers (e.g. through contractual costs or interoperability issues); and may inhibit changing to better/ cheaper options;
- Defective or unsafe product sales: safety may be measured through accidents, injuries and 'dangerous' products;
- Price dispersion for apparently alike products (across geographic areas)
- Inadequate consumer redress response upon complaints;
- Commission payments upstream: these may not operate in consumer's best interests as advice may be tainted;
- Goods or services with 'experience' or 'credence' characteristics, or are purchased infrequently; and
- Customer dissatisfaction: re choice, quality, after-sales service etc.<sup>535</sup>

Other ways used to detect detriment include consumer and consumer organisation/ stakeholder complaints or consultations; feedback or research from such groups; business firm reports and research; and the media.<sup>536</sup> **Chapters 3 to 6** are an analysis of potential consumer problems and detriment within the CIOT, and cite a range of resources drawn from those detailed above. **Chapter 7** then uses those findings to complete the Framework analysis and to form the basis for the recommendations in **Part IV**.

### **2.5.3 Further steps overview: Steps 3- 6**

The remaining steps are explained briefly here, to complete the CPF discussion, justify why certain steps are excised and to foreground the practical Step 4 and 5 discussion once consumer detriment is established.

#### **Step 3 Determine if detriment warrants policy action**

This involves five sub-questions, which examine the scale of the detriment, who is experiencing it, assesses its expected duration; considers the likely consequences of taking no policy action and considers "other substantial costs to the economy".<sup>537</sup> As **Part I** reveals, the scope, scale and stakes of the CIOT are substantial, which suggests that detriment arising from it is also likely to be widespread and

---

<sup>535</sup> The OECD note that these may reveal problems otherwise difficult to quantify: above n 505: 57.

<sup>536</sup> OECD, above n 505: 58.

<sup>537</sup> Australian Government, above n 499: 23.

substantial. This would be balanced against significant factors such as stifling innovation, adverse international impacts or impeding CIOT implementation in Australia.

The determination requires a decision as to whether to proceed to **Step 4**, or whether more evidence as to steps 1 and/ or 2 are required, or whether no action is required at all. While contrary to the recommendations in this thesis, it is likely an Australian Government entity would require evidence as to real detriment within the Australian market, before committing to substantive policy action (other than perhaps encouraging industry-driven self-regulation). This thesis however, promotes a more pre-emptive approach having regard to the global nature of CIOT markets, providers and technology, international experience and research, and its significant adverse potential and long-lasting consumer impacts.

As such, this question is not addressed again and the dissertation assumes that the detriments identified in **Chapters 3- 6** justify policy action.

#### **Step 4 Set policy objectives and identify the range of policy actions**

A clear policy objective is specified to identify what is intended to be achieved for consumers and the market. The range of practically-possible policy options are also identified, using both supply and demand side tools, and include new actions together with refocusing extant approaches. The options also identify responsible entities for policy implementation and communication.<sup>538</sup> This is undertaken in **chapter 7**.

#### **Step 5 Evaluate Options and select policy action**

Policy option evaluation seeks to ascertain the most appropriate and cost effective method to achieve the objectives outlined in step 4. Often policy-makers will conduct a cost: benefit analysis, or trials, research and stakeholder consultation is undertaken. These useful approaches are again beyond scope, so the evaluation in **chapter 7** is made using available information and evidence, including the scope-scale-stakes in **chapter one** and the gaps and conclusions identified in **Part III**.

#### **Step 6 Develop a policy review process**

After a reasonable time, the policy actions and tools recommended in **Part IV** should be reviewed to determine if the objectives are being achieved in a cost-effective manner. This is included within the recommendations to ensure responsiveness.<sup>539</sup>

---

<sup>538</sup> It is common practice for government departments to undertake a Regulatory Impact Assessment using the Best practice Regulation handbook. This is an analogous process to the ACPF, repeats much of its process and is therefore, beyond scope: Australian Government, above n 499: 27- 28.

<sup>539</sup> New laws are reviewed within five years of commencement, while periodic ACL reviews, surveys and related data are collected to allow new issues to be identified, consumer detriment evaluated and effectiveness assessed: Department of

## 2.6 Conclusion

In summary, the search to establish consumer detriment across CIOT security issues, consumer law, privacy law and online contracting follows in Chapters 3- 6. The Framework is followed hereafter as tabulated below:

<b>TRACKING CONSUMER POLICY THROUGHOUT THIS PAPER</b>	
<i>Consumer detriment may be personal and/ or structural, and can be defined as harm or damage to consumers that occurs in connection with a transaction between the consumer and particular sellers or suppliers. (London Economics, 2009)</i>	
<b>Step 1: Problem definition</b>	<b>Parts 1 and II</b>
<b>Step 2: Measure consumer detriment</b>	<b>Part III</b>
<b>Step 3: Does the detriment warrant policy action?</b>	<b>Parts III and IV</b>
<b>Step 4: Define a policy objective and identify a range of policy options</b>	<b>Part IV (Table 7.2)</b>
<b>Step 5: Evaluate options and select policy action</b>	<b>Part IV</b>
<b>Step 6: Implement and then evaluate after time</b>	<b>Part IV</b>

Table 2.3 ACPF steps

Source: Author.

**Part III** commences the legal evaluation of extant Australian consumer regulation pertinent to the CIOT, how it responds to known and unknown examples of CIOT consumer detriment, and identifies certain ‘gaps’ within Australia’s current consumer protection framework, which **Part IV** offers strategies to redress.

---

Finance, Office of Best Practice Regulation, ‘Best practice regulation handbook’  
<<http://finance.gov.au/obpr/ptproposal/handbook/appendix-A-five-yearly-reviews.html>>

## PART III CONSUMER LAW GAP ANALYSIS

---

*“...a major challenge facing the uptake of the IOT in the EU are the gaps in the legal framework governing consumer protection and data. The regulation covering the IOT has not kept up with the speed at which the technology is developing...”<sup>540</sup>*

**Part III** is a selective assessment of Australian consumer laws and their capacity to respond to consumer IOT issues and consumer problems. **Chapter 4** reviews the Australian Consumer Law from a CIOT consumer perspective, **chapter 5** evaluates privacy law gaps and **chapter 6**, contractual issues from a behavioural economics perspective. It is impossible to conduct a risk or detriment assessment without scoping these systemic risks, which innately permeate the consumer law, privacy and contract analyses to follow; this is the task in this chapter.

### Chapter 3 CIOT ‘complexity’: an overview of (in)security, big(ger) data analytics, & (artificial) intelligence

*“...a significant opportunity and a very real threat...”<sup>541</sup>*

The consumer internet of things is complex, which of itself presents challenges for consumer protection and regulation. Recent enablers are accelerating CIOT risk:<sup>542</sup> ‘big data’ cloud storage;<sup>543</sup> increasingly powerful data analytics via machine-learning and algorithms, and rapidly-growing artificial intelligence, and biometric (voice, facial and fingerprint recognition) technologies.<sup>544</sup> These technologies all liberate CIOT value, but suffer innate flaws which become CIOT flaws; and so, create new forms of consumer

---

<sup>540</sup> Rebecca Schindler, above n 1. The EU has made significant strides since 2015 in this regard.

<sup>541</sup> Communications Alliance, above n 119.

<sup>542</sup> Technically, these include smaller cheaper complex-data-collecting semiconductors and increased IPv6 network capabilities. The former are sensors, transmitters, and controllers: *Ibid*: 15. This development was driven largely by the rapidly-growing mobile phone and tablet markets. Morgan Stanley indicate sensors cost around \$1 and Bluetooth chips even less: Morgan Stanley, ‘The Internet of Things is Now’ (2014 accessed 10 Feb 2016) <<http://www.technologyinvestor.com/wp-content/uploads/2014/09/internet-of-things-2.pdf>> The latter will grow from 3 billion users (2015) to a projected 340 trillion, trillion, trillion by 2050: Internet Society, above n 79. See also Blackett Report, above n 19: 15; Accenture, above n 24; Rose, above n 10.

<sup>543</sup> The Blackett Report cites the cloud, open-source software and “commoditised hardware”: above n 19: 15.

<sup>544</sup> These are known of as ‘dynamic human bandwidth interfaces’. Other factors relevant in an IOT development context (but not enablers per se) include 3D printing: Turck, above n 438. Also, crowd funding through sites like Kickstarter or Indiegogo lessen early-phase hardware development costs by creating demand and financing: Matt Turck, ‘The Internet of Things Is Reaching Escape Velocity’ *TechCrunch* (2 Dec 2014 accessed 8 Feb 2016) <<http://techcrunch.com/2014/12/02/the-internet-of-things-is-reaching-escape-velocity/>>

risk and new challenges for consumer protection and regulation. Structural<sup>545</sup> (systemic) detriments may generate potential misuses of market power, imperfect consumer information or information asymmetries, consumer information and choice overload, and even, regulatory failure.<sup>546</sup> This chapter places this complex ecosystem in its risk context to illustrate largely piecemeal and gap-ridden Australian legal responses, current pressing consumer threats and detriments, and a policy vacuum as to those which are rapidly, on their way.

### 3.1 (In)Security is complex... and pressing

*“The time to address IOT security is right now...”<sup>547</sup>*

*Our nation cannot afford a generation of IOT devices deployed with little consideration for security. The consequences are too high given the potential for harm to our critical infrastructure, our personal privacy, and our economy.<sup>548</sup>*

*“In the ever-growing Internet of Things, attackers already outpace the defenders. If developing solutions for software liability does not become more of a priority for everyone—including tech developers, manufacturers and consumers—there may be no winning this technological war...”<sup>549</sup>*

The CIOT exacerbates an internet ecosystem security ‘crisis’: cyberspace is a “national emergency”,<sup>550</sup> the IOT is systemically “indefensible”,<sup>551</sup> and “innovation is outpacing security”.<sup>552</sup> McAfee find a “trillion points of vulnerability...”,<sup>553</sup> which exponentially increase the “attack surface” – to physical (device) access, local Wi-Fi/ Ethernet or cloud infrastructure attacks, software viruses and malware. Any internet-

---

<sup>545</sup> Structural consumer detriment involves the “ex ante reduction of consumer surplus” which affects consumers in aggregate; this is, the loss in consumer welfare due to market or regulatory failures (rather than on ex post outcomes of consumers). ‘Consumer surplus’ means the difference between what a consumer is willing to pay for a product and what they actually do pay: OECD, Toolkit, above n 505: 75. “We argue that if consumers are fully informed and rational, then structural detriment fully captures the risk of ex post psychological detriment, because this risk will be taken into account in consumers’ willingness to pay (and will thus be captured in consumer surplus). In our view, there is no perfect candidate to use as the counterfactual for structural detriment, although possibilities include perfect competition or “well-functioning markets” (which is more realistic but less easy to define)”: OECD, above n 523: 4.

<sup>546</sup> OECD, above n 505: 75.

<sup>547</sup> US Department of Homeland Security, ‘Strategic principles for Securing the Internet of Things’ (Nov 2016 accessed 15 Nov 2016): 3

<[https://www.dhs.gov/sites/default/files/publications/Strategic\\_Principles\\_for\\_Securing\\_the\\_Internet\\_of\\_Things-2016-1115-FINAL....pdf](https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf)>

<sup>548</sup> Ibid: 13.

<sup>549</sup> Lillian Ablon, ‘Keeping Hackers Away from Your Car, Fridge and Front Door’ *The National Interest* (7 Dec 2015 Accessed 10 Jun 2016) <<http://nationalinterest.org/feature/keeping-hackers-away-your-car-fridge-front-door-14525?page=show>>

<sup>550</sup> The US Federal Bureau of Investigation (FBI) warned in September 2015 of IOT cybercrime risks, including personal data vulnerability as well as the potential for “compromising the IoT device to cause physical harm.”

<sup>551</sup> NSTAC, above n 66.

<sup>552</sup> Greg Austin, Australian Centre for Cyber Security, quoted in ComputerWorld ANZ, ‘CyberThreat looms large: is Australia doing enough as to cybersecurity?’ (July 2016 accessed 11 Jul 2016)

<[http://docs.media.bitpipe.com/io\\_13x/io\\_132733/item\\_1376580/ANZ\\_ISM\\_0716\\_ezine\\_FINAL.pdf](http://docs.media.bitpipe.com/io_13x/io_132733/item_1376580/ANZ_ISM_0716_ezine_FINAL.pdf)>

<sup>553</sup> Raj Samani, ‘3 Key Security Challenges for the Internet of Things’ *McAfee Intel Security Blog* (29 Oct 2014)

<<https://blogs.mcafee.com/business/3-key-security-challenges-internet-things/>>

connected CIOT device is a potential 'attack surface' and may become a compromised attack 'backdoor'. Cyber criminals will use them to cross the network "laterally" – to hard drives, laptops, phones and tablets - to steal personal information, credit card numbers, bank account log-ins, digital (data) eavesdropping or to send malicious or spam emails.<sup>554</sup>

The Australian Government has no mandated cybersecurity standards.<sup>555</sup>

### 3.1.1 Ecosystem flaws & data breach

Consumer IOT flaws are systemic: *devices* lack security-by-design, evidencing basic security flaws in design and operation; *software apps* suffer security vulnerabilities and innumerable cases of data breach and 'hacking';<sup>556</sup> and features such as social media integration imports user behavioural and settings-related risk. Finally, consumer data stored in the *cloud* carries its many risks:<sup>557</sup> interface insecurity;<sup>558</sup> outage potentials; offshore data processing and storage, and cross- jurisdictional data transfer;<sup>559</sup> potential data breach and devolved data security governance.<sup>560</sup> Consumer data breaches are

---

<sup>554</sup> FBI, 'Cyber Tip: Be Vigilant with your Internet of things (IoT) devices' (13 Oct 2015 accessed 2 Mar 2016) <<https://www.fbi.gov/news/stories/cyber-tip-be-vigilant-with-your-internet-of-things-iot-devices>>

<sup>555</sup> There are relevant (non-mandatory) ISO standards and the US President has signed an Executive Order mandating compliance with the NIST CSF for Federal agency compliance with the NIST Cybersecurity Framework: Sean Field, 'NIST Cybersecurity Framework Workshop - Day 1' *Maddocks* (17 May 2017 accessed 18 May 2017) <<https://www.maddocks.com.au/blog/nist-workshop/>>

<sup>556</sup> Art 29 WP, 'Opinion 02/2013 on apps on smart devices' (adopted 27 Feb 2013 accessed 2 Feb 2016) <[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf)>

<sup>557</sup> Mathews-Hunt, above n 151. ACMA and recent ABS research supports this view; suggesting that actual cloud usage far exceeds awareness levels: while 55% of those surveyed had 'heard' of cloud computing, only 26% realised they were using the cloud. It is a statistic which is likely to increase in the CIOT context, obscured by a device-focus, and questionable app privacy consents or terms and conditions.

<sup>558</sup> OWASP describes its aims to help consumers, manufacturers and developers to better understand IoT security issues and to enable better security decisions in "building, deploying or assessing IoT technologies": OWASP 'Internet of Things Project' and OWASP, 'Internet of Things Top Ten Project' (n.d. accessed 7 Apr 2016) <[https://www.owasp.org/index.php/OWASP\\_Internet\\_of\\_Things\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project)> ACMA and ABS research suggests that actual cloud usage far exceeds consumer awareness levels: while 55% of those surveyed had 'heard' of cloud computing, only 26% realised they were using the cloud, a statistic likely to increase in the CIOT context, where cloud use is obscured by a device-focus, and questionable app privacy consents or terms and conditions.

<sup>559</sup> Australian Cyber Security Centre (ACSC), '2015 Threat Report' (2015 accessed 9 Mar 2016): 22 <[https://acsc.gov.au/publications/ACSC\\_Threat\\_Report\\_2015.pdf](https://acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf)> ACSC identifies these as "significant risks".

<sup>560</sup> *Ibid.* Data in foreign jurisdictions may lawfully be accessed by foreign governments such as the US, which may occur without 'owner' notification.

commonplace - affecting the most 'secure' global operators<sup>561</sup> - like Google<sup>562</sup> and Apple.<sup>563</sup> Cloud attacks are increasing<sup>564</sup> and the recent *Heartbleed* virus, for example, affected one third of cloud services.<sup>565</sup> Most CIOT data is cloud-stored and much not encrypted, though experts warn that "...storing sensitive, unencrypted information in the cloud is foolish, no matter how you slice it."<sup>566</sup> Finally, CIOT apps on *smartphones* import device vulnerabilities: the 2016 Quadrooter<sup>567</sup> bug<sup>568</sup> gave hackers potential access to 900 million smartphones - and their connected CIOT apps and data - while the industry increased consumer risk through fix delays.<sup>569</sup> Industry explanations for security and data breach events are rarely comforting: detection and voluntary public disclosure is rare<sup>570</sup> and explanations often symptomatic of lax security risk assessments and practices generally: from poor designed-in device insecurity to a stolen laptop, to an employee with weak password security<sup>571</sup> or international contractor staff data theft. Inadequate industry corporate compliance, information provision, staff training, chain-of-

---

<sup>561</sup> These have affected most major online platforms - Gmail, twitter, dropbox, Facebook, Apple iCloud, Google Apps, Amazon, Microsoft Office 365, Outlook.com, Bing, Azure Cloud, Xbox, Cloudflare (including 750,000 other sites), Outlook.com mail, Amazon (Pinterest, Netflix, instagram) - affecting millions of users worldwide. Many are part of or supply services to, the CIOT data storage and processing ecosystem.

<sup>562</sup> Gmail users have experienced over a dozen outages since 2009. The most serious affected 'most' of 500 million users: Adrian Covert, 'Gmail at 10: How Google dominated e-mail' *CNNTech* (1 April 2014 accessed 28 June 2014) <<http://money.cnn.com/2014/04/01/technology/gmail>>

<sup>563</sup> Users were advised to change their passwords and not to pay a ransom demanded when malware locked Apple users out in Australia: Chris Griffith, 'Malware cripples Australian Apple iCloud accounts' *The Australian* (29 May 2014 accessed 29 July 2014) <<http://www.theaustralian.com.au/technology/malware-cripples-australian-apple-icloud-accounts/story-e6frgaxk-1226935680356>> *Wired* reporter Matt Honan's macbook air, ipad and iphone data was remotely wiped, when an Apple employee reset his iCloud password: Ted Samson, 'Dropbox fiasco serves as reminder of cloud-storage insecurity' *Infoworld* (2 Aug 2012 accessed 30 July 2014): 108 <<http://www.infoworld.com/t/cloud-security/dropbox-fiasco-serves-reminder-of-cloud-storage-insecurity-199197>>

<sup>564</sup> The volume and persistence of attacks is increasing and are "moving to the cloud". Alert Logic, Cloud Security Report (Spring 2014 accessed 10 July 2014) [12] <<http://www.findwhitepapers.com/force-download.php?id=37838>>

<sup>565</sup> James Bourne 'One in three cloud services was susceptible to Heartbleed, research shows' *Cloudtech* (12 May 2014 accessed 7 June 2014) <<http://www.cloudcomputing-news.net/news/2014/may/12/one-three-cloud-services-was-susceptible-heartbleed-research-shows/>>

<sup>566</sup> InfoWorld, 'Popular cloud sync app raises security fears' *Tech Watch* (8 Nov 2011 accessed 30 July 2014) <<http://www.infoworld.com/print/157776>>

<sup>567</sup> Phones affected include Samsung's Galaxy S7 and S7 Edge, HTC's One M9 and HTC 10, and Google's Nexus 5X, 6, and 6P.

<sup>568</sup> Security firm Check Point identify 'Quadrooter' as a series of four "interconnected flaws" whereby hackers can access the "root" android operating system and control the device - including tracking every action its operator takes and uploading that data anywhere - in up to 900 million smartphones worldwide: Alex Hern, 'Quadrooter Android bug could affect almost 1bn phones, researchers claim' *The Guardian* (8 Aug 2016 accessed 9 Aug 2016) <<https://www.theguardian.com/technology/2016/aug/08/quadrooter-android-bug-phones-hackers-smartphone>>

<sup>569</sup> Hern, *Ibid*: "Just because manufacturers know of the bug and how to fix it, doesn't mean consumers are safe: each individual manufacturer still has to create a specific fix for their model of phone, and in many cases individual mobile carriers then have to themselves agree to roll that fix out to their customers..." He cites CheckPoint: "Critical security updates must pass through the entire supply chain before they can be made available to end users. Once available, the end users must then be sure to install these updates to protect their devices and data." Google now pre-vets Store apps, but has no Chinese store and malicious apps can "slip between the cracks".

<sup>570</sup> Australia has recently passed mandatory data breach reporting; see Chapter 5.

<sup>571</sup> This occurred (in different ways) in both the Dropbox and Apple iCloud cases.

contractor liability and insurance is a data loss risk, just as much as hacking. And CIOT device and app providers are of course, best placed to assess and control each of these risks.

Of course, data breach<sup>572</sup> - and misuse - happens.<sup>573</sup> It is lucrative,<sup>574</sup> expensive,<sup>575</sup> technologically challenging,<sup>576</sup> damaging to consumer trust<sup>577</sup> and can occur at any link in a long CIOT supply chain.<sup>578</sup> Detrimental consumer outcomes include identity theft<sup>579</sup> and fraud,<sup>580</sup> stalking, embarrassment or discrimination, and financial loss.<sup>581</sup> It is a fundamental issue to CIOT security, data integrity and a trust barrier, but Australian regulatory action is lagging. Further, credible solutions such as those advanced by

---

<sup>572</sup> "Data breach" means "...when personal information ... is lost or subjected to unauthorised access, modification, disclosure, or other misuse of interference...": OAIC, 'Guide to Information Security' (April 2013 accessed 10 Apr 2015) [2] <<http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-securing-personal-information>>

<sup>573</sup> Corporate security and consumer data breach may arise the hostile attack or hacking, as well as inadvertently through accidental data disclosure, lost or stolen computers and human or programming error, as well as systemic corporate failure, such as latent system vulnerabilities, poor employee training, systems or undetected misconduct, inadequate corporate compliance, deficient anonymisation and poor product design, risk assessment and security practices. Anywhere that data is collected, collated, used or stored is a potential target or source of breach.

<sup>574</sup> An Australian driver's license is valued at \$417- 450 on Agora and passport is worth \$5110. While noting dark web data sale marketplaces, the Government did not quantify the likely example value: Commonwealth Parliament House of Representatives, *Privacy Amendment (Notifiable Data breaches) Bill 2016 Explanatory Memorandum* (2016 accessed 2 Oct 2016): 17 [60] < [http://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/Bills\\_Search\\_Results/Result?bld=r5747.>](http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r5747.>)

<sup>575</sup> In 2015 (c/f 2014), the average breach involved 20,000+ records at \$158 (154) each, tallying to a total cost of \$4 (2.82) million dollars per company: Ponemon Institute LLC, '2016 Cost of Data Breach Study: Australia' (Oct 2016 accessed 20 Oct 2016) < <http://www-03.ibm.com/security/data-breach/>> Data breach costs consumers in terms of lost privacy and potential economic exposure to identity theft and other criminal activity.

<sup>576</sup> OAIC, above n 572: 16.

<sup>577</sup> OAIC, 'Data Breach Notification Guide: A Guide to handling personal information security breaches' (Aug 2014 accessed 3 Apr 2015) [9] < <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>>. For example, in 2015, UK phone company TalkTalk lost 250,000 customers' data: Rene Millman, 'TalkTalk loses 250,000 customers post-breach – now supplier scam too' *SC Magazine* (30 Jan 2016 accessed 20 Oct 2016) <http://www.scmagazineuk.com/talktalk-loses-250000-customers-post-breach--now-supplier-scam-too/article/469535/>>

<sup>578</sup> Randall Rothenberg, 'IAB Head: 'The Digital Advertising Industry Must Stop Having Unprotected Sex' *Business Insider* (6 Feb 2014 accessed 9 Apr 2015) <<http://www.businessinsider.com.au/iab-randall-rothenberg-supply-chain-2014-2>>

<sup>579</sup> One definition is the 'knowing transfer, possession or use of any name or number that identifies another person with the intent of committing or aiding and abetting a crime': US Identity Theft and Assumption Deterrence Act 1998. In first half 2016, identity theft was the leading type of global data breach (64%), and malicious outsiders were the leading cause (69%): George Nott, 'Australia leads APAC for data breaches' (21 Sept 2016 accessed 29 Sept 2016) CIO <http://www.cio.com.au/article/607231/australia-leads-apac-data-breaches/> Healthcare industries had 27% of breaches but 5% of compromised records, versus government, which suffered 14% of breaches but 57% of record loss. For the costs which establish consumer detriment see: Alessandro Acquisti, Curtis R. Taylor and Liad Wagman, 'The Economics of Privacy', *Journal of Economic Literature*, 52:2, (8 Mar 2016) Sloan Foundation Economics Research Paper No. 2580411, <http://ssrn.com/abstract=2580411> at page 37.

<sup>580</sup> Identity theft means the acquisition or collection of an individual's PI for criminal purposes and for the first half of 2015, 53.2% of breaches were caused by identity theft which constitutes 74.9% of compromised records. The crime is "one of the most common and costly crimes in Australia": Commonwealth Parliament House of Representatives, *Privacy Amendment (Notifiable Data breaches) Bill 2016 Explanatory Memorandum* (2016 accessed 2 Oct 2016): 16 [60] < [http://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/Bills\\_Search\\_Results/Result?bld=r5747.>](http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r5747.>) The estimated economic impact exceeds \$2B annually and 4- 5 % of those affected experience financial loss: Attorney-General's Dept, 'Identity Crime and Misuse in Australia' (2013- 4 accessed 5 Aug 2016): 4 < <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Identity-Crime-and-Misuse-in-Australia-2013-14.pdf>>

<sup>581</sup> Above n 574: 13 [60]

OWASP (Annex. D),<sup>582</sup> GSMA,<sup>583</sup> the FTC,<sup>584</sup> OECD,<sup>585</sup> or non-governmental activist groups<sup>586</sup> remain largely ignored or ill-implemented voluntary recommendations or guidelines<sup>587</sup> – while some experts assert that no clear solutions exist.<sup>588</sup> In the past decade, costly<sup>589</sup> database breaches of consumer data have reached pandemic levels.<sup>590</sup> Governments,<sup>591</sup> the world's largest companies<sup>592</sup> and supposedly, the most secure entities in the world<sup>593</sup> have fallen victim – as have hundreds of millions of consumers.<sup>594</sup>

---

<sup>582</sup> OWASP above n 558.

<sup>583</sup> GSMA, above n 113; GSMA, 'Automotive IoT Security: Countering the Most Common Forms of Attack' (22 March 2016 accessed 2 Apr 2016) <<http://www.gsma.com/connectedliving/automotive-iot-security-countering-the-most-common-forms-of-attack/>>

<sup>584</sup> FTC, above n 118.

<sup>585</sup> OECD, 'Guidelines for the Security of Information Systems and Networks' (2002 accessed 2 Apr 2016)

<<https://www.oecd.org/sti/ieconomy/15582260.pdf>>; OECD, above n 197.

<sup>586</sup> I Am the Cavalry, 'Five Star Automotive Cyber Safety framework' (2015) <<https://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf>>; I Am The Cavalry, 'Hippocratic Oath for Connected Medical Devices', (19 Jan 2016 accessed 2 Sept 2016) <<https://www.iamthecavalry.org/wp-content/uploads/2016/01/I-Am-The-Cavalry-Hippocratic-Oath-for-Connected-Medical-Devices.pdf>> It describes itself as "a global grassroots organization that is focused on issues where computer security intersects public safety and human life. We strive to ensure that these technologies are worthy of the trust we place in them", and focus on cars, medical devices, home electronics and public infrastructure.

<sup>587</sup> GSMA, above n 108; NIST, 'Framework for Improving Critical Infrastructure Cybersecurity' (12 Feb 2014 accessed 2 Sept 2016) version 1.0 <<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>>;

<sup>588</sup> Bruce Schneier, 'Data is a toxic asset, so why not throw it out?' *CNN* (1 Mar 2016 accessed 26 Mar 2016)

<<http://edition.cnn.com/2016/03/01/opinions/data-is-a-toxic-asset-opinion-schneier/index.html>

<sup>589</sup> In 2015 (c/f 2014), the average breach involved 20,000+ records at \$158 (154) each, tallying to a total cost of \$4 (2.82) million dollars per company: Ponemon, above n 575. In addition to cost data, the global study puts the likelihood of a material data breach involving 10,000 lost or stolen records in the next 24 months at 26%.

<sup>590</sup> Information is Beautiful, above n 43.

<sup>591</sup> Australian Government breaches have been severe: in 2012, almost 10,000 asylum seekers' details leaked online, in 2014, G20 leader's details (e.g. including passport details, dob and visa details) but did not notify victims of the breach (e.g. caused by human error, not systemic, the received email and deleted mail box content was (it was claimed) deleted, and the recipients deemed it "unlikely" that the email would be "...accessible, recoverable or stored elsewhere on their system": Paul Farrell and Oliver Laughland, 'Asylum-seeker data breach to be investigated by privacy commissioner' *The Guardian* (19 Feb 2014 accessed 9 Apr 2015) <<http://www.theguardian.com/world/2014/feb/19/asylum-seeker-data-breach-to-be-investigated-by-privacy-commissioner>>

<sup>592</sup> LinkedIn suffered compromise to 167 million accounts (login and password), and 427 million MySpace passwords which have been decrypted and are on sale on the dark net as at mid 2016, and Tumblr lost some 65 million login (not password) credentials: Roger Hackett, 'LinkedIn Lost 167 Million Account Credentials In Data Breach' *Fortune* (18 May 2016 accessed 4 Jun 2016) <<http://fortune.com/2016/05/18/linkedin-data-breach-email-password/>> While the breach occurred in 2012, it was originally believed that 6.5 million encrypted passwords had been stolen, but the data has recently been offered for sale on a dark market website in 2016. Most passwords were cracked within days of the theft as they were not 'salted': <https://haveibeenpwned.com/>. LinkedIn's Chief Information Security officer indicates their response is to invalidate the passwords and to contact users to reset them. He claimed stated that LinkedIn now salts passwords (adds random data to passwords prior to encryption to make them less able to be 'cracked'). Older examples include: in 2013, SnapChat lost 4.7 million user details; eBay lost 145,000 member details; Adobe lost 38 million customer IDs; Apple lost 12 million user details, America's second largest insurer lost 80 million health records. In 2014, retailer Target lost 40 million credit card numbers (which led to US prosecutions settled in May 2017 for \$18.5 million settlement with 47 states and Washington, D.C.) and Sony lost 100 terabytes of data. top US data brokers, Lexis Nexis, D & B and Alteryx each lost millions of social security records - despite "...iron-clad means of protecting their data:" Enigma Software, 'Cyber Attacks Aimed at Data Brokers D&B, Alteryx and LexisNexis Claim Theft of Important Data' (2013 accessed 9 Apr 2015) <<http://www.enigmasoftware.com/cyber-attacks-data-brokers-db-alteryx-lexisnexis-theft-important-data/>> These included social security number, name, and other personal data.

<sup>593</sup> For example, the Snowden revelations as to the US NSA.

<sup>594</sup> Recent examples include Friend Finder Network (412 million), Anthem (80 million) which is the second largest US health insurer, MySpace (164 million)

Australian cases are multiplying.<sup>595</sup> While systems flaws or failures are commonly the cause, the public face of breach is hacking; that is, any of criminal access to steal data for black market sale, hacktivism,<sup>596</sup> state-based political or terrorist purposes,<sup>597</sup> or simply, to prove that it can be done.<sup>598</sup>

*"There are two types of companies. Those that have been hacked and know it and those that have been hacked and don't know it..."<sup>599</sup>*

While most CIOT hacks to date have been white hat in origin, the CIOT has been implicated not only for its patent security vulnerability as a source of consumer data disclosure, but also, as a means to effect attacks on other systems. From a risk management alert perspective, it should be enough to cite authoritative government<sup>600</sup> and security experts<sup>601</sup> who warn of serious CIOT vulnerabilities across every link in the CIOT chain – from device to software to cloud platform. So, while court cases as to CIOT security issues are only starting to emerge internationally, there is ample evidence already that its chain-of-operation entails significant vulnerability and potential for consumer detriment. CIOT attacks compromise network privacy and security, and increase the likelihood of data and property theft, burglary and other criminal activity (e.g. ongoing malicious control<sup>602</sup> or 'smart' robberies<sup>603</sup>), increases consumer surveillance, tracking and stalking risk, reduces consumers' ability to control personal or (business-related) proprietary information dissemination,<sup>604</sup> and impairs the peaceful enjoyment of (for example) a

---

<sup>595</sup> In 2016, the Gemalto Breach Level index reveals that Australia led the APAC region for data breach with 22 incidents (followed by India (13) Japan & NZ (7)).

<sup>596</sup> For example, Anonymous members attacked PayPal, Mastercard and Visa in 2011 to protest their refusal to process Wikileaks donations: Kim Zetter, 'Hacker Lexicon: What are the Dos and DDOS attacks?' WIRED (16 Jan 2016 accessed 22 Oct 2016) <<https://www.wired.com/2016/01/hacker-lexicon-wha-are-dos-and-ddos-attacks/>>

<sup>597</sup> US authorities confirm that Russia hacked Podesta's emails, which were then leaked via Wikileaks to damage Clinton's unsuccessful bid for president in 2016. In 2007, Estonian sites were attacked allegedly by Russian 'nationalists', and in 2008, Georgia claimed Russia has initiated DDoS attacks, just a few weeks before Russia invaded: Zetter, above n 596.

<sup>598</sup> In 2016, Krebs security was attacked using DDoS, in the then biggest such attack known. Google assisted them to recover as their own provider could not due to cost: KrebsOnSecurity, 'Who makes the IoT Things under Attack?' <https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/>; Eduard Kovacs, 'Over 500,000 IoT devices vulnerable to Mirai botnet' SecurityWeek (7 Oct 2016 accessed 7 Oct 2016) <<http://www.securityweek.com/over-500000-iot-devices-vulnerable-mirai-botnet>>

<sup>599</sup> Andreas Baumhof, *ThreatMetrix* chief technology officer quoted in Acohidio, above n 140.

<sup>600</sup> For example, the EU Art 29 WG, the ACCS, and the US NHTSA.

<sup>601</sup> For example, Cisco, HP, IEEE, McAfee (and many others) as well as popular sources such as Securityweek, Krebs on Security, Schneider, etc.

<sup>602</sup> Colin Neagle, 'Scary stories of hacking Internet of Things devices are emerging, but how realistic is the threat?' *NetworkWorld* (2 Apr 2015 accessed 2 Sept 2016) <<http://www.networkworld.com/article/2905053/security0/smart-home-hacking-is-easier-than-you-think.html>> In 2015, one Honeywell wi-fi thermostat user reviewed the product favourably, reporting that he was maliciously controlling it to adjust temperature settings to inflict discomfort and cost on his wife and her new boyfriend. Another is an attack based upon scanning local IP space, finding IP cameras and then being able to observe inhabitants to learn their behaviours – and rob their house "intelligently".

<sup>603</sup> *Ibid.*

<sup>604</sup> In the 2014 TrendNet case (discussed Ch 4) the FTC pleaded that the camera video, audio streams or images may be used in business contexts which exposed commercial information as well as private information.

smart home. Further in many cases, consumers have no way to detect breach, so its impacts may be long term and extend to third parties, who may unwittingly be affected too.

Consumer CIOT cases are few, but emerging. As there are no explicit CIOT consumer or privacy law cases in Australia,<sup>605</sup> the next section uses research and cases from various jurisdictions. These cases are of course, not a coherent body of law, nor would they necessarily be decided the same way in Australia. But they are illustrative and possibly, predictive of potential future Australian CIOT cases or regulatory activity.

### 3.1.2 'Smart' (in)secure examples

#### (a) Smart Home

*"...media hype over theoretical demonstrations at DefCon and Black Hat...are soon spun into too many fantastical, sky-is-falling scare stories..."*<sup>606</sup>

Smart home systems have shown significant security vulnerabilities.<sup>607</sup> The Canadian Privacy Commission report that 80% of devices use factory defaults and do not require strong passwords, 70% did not encrypt devices and 60% lacked software update encryption or had insecure web interfaces.<sup>608</sup> Symantec's<sup>609</sup> 2015 report found no integrated security software in devices tested, leaving consumers unprotected, uninformed and unable to detect malware. Of CIOT mobile apps, 20% did not use industry-standard Secure Sockets layer (SSL) encryption in cloud communications,<sup>610</sup> "many" CIOT cloud platforms exhibited "common web application vulnerabilities" and two thirds of apps had "security issues", of which six were "serious".<sup>611</sup> The study concluded that known mitigation techniques are "often neglected", leaving "...millions of people at risk of cyberattacks..."<sup>612</sup> A 2015 HP study found that smart

---

<sup>605</sup> See *Google Inc. v Australian Competition and Consumer Commission* [2013] HCA 1.

<sup>606</sup> Tom Paterson, Chief Trust officer of UNISYS, quoted in Jeff John Roberts, 'Volkswagens, Voting Machines and Hype over Hacking' *Fortune* (14 Aug 2016 accessed 15 Aug 2016) < <http://fortune.com/2016/08/14/volkswagens-voting-machines-and-hype-over-hacking/>>

<sup>607</sup> HPE, 'How safe are home security systems? An HPE study on IoT security' (Nov 2015 accessed 6 Apr 2016) <<http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-7342ENW.pdf>>

<sup>608</sup> Office of the Privacy Commissioner of Canada, above n 215.

<sup>609</sup> In July 2016 the world's largest antivirus firm had its entire product line-up of 17 enterprise products and eight Norton antivirus products, exposed as containing "critical vulnerabilities" with "potentially devastating consequences". In combination, a hacker could hijack a consumer's machine or compromise "an entire enterprise fleet" – and use its self-replicable 'wormable' remote code execution nature to hijack other devices purely by sending an email or a link (which did not even need to be clicked). Vulnerabilities have been also identified in security software of Intel, FireEye, Kaspersky, McAfee to Trend Micro: Travis Ormandy, 'How to compromise the Enterprise Endpoint' *Google's Project Zero* (28 Jun 2016 accessed 3 Jul 2016) < <http://googleprojectzero.blogspot.com.au/2016/06/how-to-compromise-enterprise-endpoint.html>>

<sup>610</sup> *Ibid*: 3.

<sup>611</sup> 'Serious' means they enabled unauthorised access to backend systems: *Ibid*: 5.

<sup>612</sup> *Ibid*.

TVs, webcams, thermostats, remote power outlets, door locks, home alarms, scales, garage door openers and home hubs show an “alarmingly high average number of vulnerabilities per device”,<sup>613</sup> and confirmed mobile and cloud concerns”,<sup>614</sup> concluding ominously, that smart home consumers may not be alone in monitoring their home.<sup>615</sup> Security researchers have since shown that light bulbs,<sup>616</sup> baby monitors,<sup>617</sup> refrigerators, smart TVs and wi-fi enabled toys like ‘Hello Barbie’<sup>618</sup> and Smart Bear<sup>619</sup> are all hackable, exposing consumers to data breach. In 2015, toy manufacturer VTech lost 4.6 million adult and 6.4 million children’s details through hacking.<sup>620</sup> One study found all leading baby monitor devices “trivial” to exploit, exhibiting “critical, highly exploitable vulnerabilities”,<sup>621</sup> allowing hackers to monitor live feeds, change camera settings, and authorise a third party to remotely control and view the monitor.<sup>622</sup> The authors cautioned that security did not increase with price (in fact risk increased with features) and that devices were insecure by default, difficult to patch and security status impossible to monitor, creating both an in-home security risk but also increasing business vulnerability with merging home and office work environments. Researchers have also triggered home alarms, unlocked doors and taken control of Samsung’s *SmartThings* platform.<sup>623</sup> Other proven hacks include Belkin WeMo, Samsung fridges, Hue

---

<sup>613</sup> HPE, ‘Internet of things research study 2015 report’ (2015 accessed 6 Apr 2016)

<<http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf>> these included weak passwords (80%) and a lack of encryption (70%).

<sup>614</sup> HPE, above n 607: 3.

<sup>615</sup> HPE, above n 607.

<sup>616</sup> Security researchers demonstrated how LIFX smart bulbs could be exploited enabling theft of Wi-Fi usernames and passwords.

<sup>617</sup> Mark Stanislav and Tod Beardsley, ‘Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities’ Rapid7 (Sept 2015 accessed 4 Feb 2016) <<https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf>>

<sup>618</sup> Mattel’s doll is wi-fi enabled to collect and store speech to her, to which she responds. Collection is via a mobile app to a cloud server where the voice recording is analysed and stored: Samuel Gibbs, ‘Privacy fears over ‘smart’ Barbie that can listen to your kids’ *The Guardian* (13 Mar 2015 accessed 10 May 2016) <

<https://www.theguardian.com/technology/2015/mar/13/smart-barbie-that-can-listen-to-your-kids-privacy-fears-mattel>>; James Patto, ‘These toys have eyes (and ears too): VTech security breach raises ‘Internet of Things’ privacy fears’ *Minter Ellison Blog TMT and IP blog* (21 Apr 2016 accessed 25 Apr 2016) <

<http://www.lexology.com/library/detail.aspx?g=e9fc4a57-4bbb-43d7-a414-24c72b383ac4>>

<sup>619</sup> The hacked Bear allowed access to children’s profiles, including name, dob, gender, language and toys played with. Zack Whittaker, ‘Two newly-discovered flaws light fire under IoT security’ *ZDNet* (2 Feb 2016 accessed 7 Apr 2016) <<http://www.zdnet.com/article/two-newly-discovered-security-flaws-light-fire-under-internet-of-things-again/>>

<sup>620</sup> Patto, above n 618.

<sup>621</sup> Stanislav, above n 617.

<sup>622</sup> Chris Matyszczyk, ‘Hacker Shouts at Baby Through Baby Monitor’ *CNET* (Apr 2014 accessed 2 Jan 2016) <[www.cnet.com/news/hacker-shouts-at-baby-through-baby-monitor/](http://www.cnet.com/news/hacker-shouts-at-baby-through-baby-monitor/)>; Kashmir Hill, ‘Baby Monitor Hack’ Could Happen to 40,000 Other Foscam Users’ *Forbes* (27 Aug 2013 accessed 2 Jan 2016)

<[www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/](http://www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/)>

<sup>623</sup> Earlence Fernandes, Jaeyon Jung, and Atul Prakash, ‘Security Analysis of Emerging Smart Home Applications’ in Proceedings of 37th IEEE Symposium on Security and Privacy, 2016’ (May 2016 accessed 5 May 2016) <<https://iotsecurity.eecs.umich.edu/>>. See also Greenberg, above n 350.

lights, Trane<sup>624</sup> and Nest thermostats, Kevo locks, MyQ garage, Ubi, Wink Hub, smart cameras<sup>625</sup> and many others.<sup>626</sup> While responsible manufacturers will act to rectify security issues or even withdraw and refund unfixable devices, it begs the question why researchers can detect these flaws, instead of designers/ manufacturers pre or even, post release.<sup>627</sup>

Research has translated into real- life cases recently. The US Federal Trade Commission (FTC) has been an active security advocate: mostly using its wide section 5(a) power prohibiting “unfair or deceptive acts or practices in or affecting commerce.”<sup>628</sup> Factually, those practices are generally either deceptive and/ or unfair security representations or more recently, actionably lax corporate security practices. In *FTC v Trendnet*,<sup>629</sup> ‘SecurView’ home security or baby monitoring cameras were hacked due to (ironically) poor security, enabling over 700 live internet feeds from people’s homes and unauthorised third party surveillance.<sup>630</sup> *Trendnet* had falsely represented its devices as ‘secure’, had not taken reasonable steps to secure devices given their use, or to ensure security settings would be observed and not provided (overall) reasonable security to prevent unauthorized access to personal information.<sup>631</sup> Specifically, the devices transmitted unencrypted user login credentials in readable text over the Internet, stored logins on the mobile app without encryption, failed to employ reasonable and appropriate software design and testing and failed to actively monitor security vulnerabilities to enable early detection.<sup>632</sup> The settlement required customer update notification<sup>633</sup> and a two-decade long security compliance program, monitored by bi-annual independent risk assessments to “...address security risks that could result in unauthorized access to or use of the company’s devices, and to protect the security, confidentiality, and

---

<sup>624</sup> Cisco researchers found that Trane ComfortLink devices allow attackers remote access to thermostat controls, but also photos and stored on the devices and access to the user’s home (including computer) network: Krebs, ‘IoT Reality: Smart Devices, Dumb Defaults’ (8 Feb 2016 accessed 3 Mar 2016) < <http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/>>

<sup>625</sup> Irena Bojanova, ‘Hacking IoT’ *IEEE Computer Society* (12 Feb 2015 accessed 21 Mar 2016) < <https://www.computer.org/portal/web/sensing-iot/content?g=53926943&type=article&urlTitle=hacking-iot>>

<sup>626</sup> See Phil Laplante, ‘Repository of IOT Failures’ <<http://iotfdb.laplante.io/>> and [www.nvd.nist.gov](http://www.nvd.nist.gov).

<sup>627</sup> The FTC suggests several reasons: manufacturers may not be traditional ‘security’ conscious companies, devices may be very small which may inhibit security capacity and for example. In one case. researchers have even purchased devices, uploaded malware, returned them to store and exerted control immediately upon installation.

<sup>628</sup> Federal Trade Commission Act (FTC Act) (15 USC §45).

<sup>629</sup> *Complaint of FTC, TRENDnet Inc.*, No. C-4426 (7 Feb 2014 accessed 3 Feb 2016) <<http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf>>

<sup>630</sup> *Ibid*: 5. Other devices could be eavesdropped upon by anyone with their internet address. The device marketing claims that consumers may use the cameras to monitor “babies at home, patients in the hospital, offices and banks, and more.”: FTC, Federal Register, Vol 78, No 176 (11 Sept 2013 accessed 2 Mar 2016): 55718 < <https://www.ftc.gov/sites/default/files/documents/cases/2013/09/130911trendnetfrn.pdf>>

<sup>631</sup> *Ibid*.

<sup>632</sup> *Ibid*. This included a failure to monitor security research.

<sup>633</sup> This entailed information as to the device problem, how to update it and two years’ free technical support with respect to effecting the update or disabling the device: FTC, ‘FTC Approves Final Order Settling Charges Against TRENDnet, Inc.’ (7 Feb 2014 accessed 16 Mar 2016) <<https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc>>

integrity of information that is stored, captured, accessed, or transmitted by its devices”.<sup>634</sup> A similar outcome<sup>635</sup> arose in *FTC v AsusTEK*,<sup>636</sup> which reinforced that CIOT security is not just protecting consumer *data*, but also about consumer information, and protecting a user’s network<sup>637</sup> and equipment.<sup>638</sup> The FTC alleged that Asus routers and cloud service used weak default passwords, failed to encrypt data, used poor default settings and that Asus failed to inform consumers or rectify known flaws in a timely manner.<sup>639</sup> Hackers posted IP addresses of almost thirteen thousand routers online and accessed over three thousand AiCloud accounts, enabling identity theft and other demonstrable consumer detriments.<sup>640</sup> The FTC alleged unfair or deceptive acts or practices as to security failures and security misrepresentations, and agreed a detailed long-term settlement. Perhaps in the shadow of Asus and spawned by an article,<sup>641</sup> several class actions<sup>642</sup> were filed, alleging that ADT home security devices are marketed falsely, are unencrypted, easily hacked and are not secure or safe.<sup>643</sup> These cases were settled for \$16M in 2017.<sup>644</sup> In contrast, the FTC has filed complaint against Taiwanese CIOT manufacturer D-Link alleging unfair or deceptive acts or practices ‘in connection with Defendants’ failure to take reasonable steps to secure the routers and Internet-protocol cameras they designed for, marketed, and sold’ in the United States. The case alleges false and deceptive security marketing/

---

<sup>634</sup> *Ibid.*

<sup>635</sup> *In the Matter of ASUSTek*, File No. 142 3456, Agreement containing Consent Order, (26 Feb 2016)

<<https://www.ftc.gov/system/files/documents/cases/160222asusagree.pdf>>

<sup>636</sup> *ASUSTek*, File No. 142 3456, Complaint (26 Feb 2016); Agreement containing Consent Order, (26 Feb 2016)

<https://www.ftc.gov/system/files/documents/cases/160222asusagree.pdf>

<sup>637</sup> FTC, ‘ASUS Settles FTC Charges That Insecure Home Routers and “Cloud” Services Put Consumers’ Privacy At Risk’ (23 Feb 2016 accessed 23 Feb 2016) <[https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put?utm\\_source=govdelivery](https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put?utm_source=govdelivery)>

<sup>638</sup> European Union, Article 29 Data Protection Working Party, ‘Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)’ (19 Jul 2016 accessed 20 Aug 2016): 18 <[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf)>

<sup>639</sup> 12,900 devices were hacked, due to router and cloud insecurity, including weak default passwords, failure to encrypt data, poor default settings and Asus’ failure to address known flaws in a timely manner or to inform consumers of their existence: FTC above n 637. See also Lesley Fair, ‘ASUS case suggests 6 things to watch for in the Internet of Things’ (23 Feb 2016 accessed 23 Feb 2016) <<https://www.ftc.gov/news-events/blogs/business-blog/2016/02/asus-case-suggests-6-things-watch-internet-things>>

<sup>640</sup> Specifically, 12,937 routers and 3131 AiCloud accounts were compromised.

<sup>641</sup> Kashmir Hill, How Your Security System Could Be Used to Spy on You, *Forbes* (Jul. 23, 2014) <[www.forbes.com/sites/kashmirhill/2014/07/23/how-your-security-system-could-be-used-to-spy-on-you](http://www.forbes.com/sites/kashmirhill/2014/07/23/how-your-security-system-could-be-used-to-spy-on-you)> (accessed Jan. 18, 2016).

<sup>642</sup> *Baker v ADT Corporation* No 14 cv 8988 Case No. 1:14-cv-08988 Filed 9.11.2014 <

<https://www.truthinadvertising.org/wp-content/uploads/2015/02/Baker-v-ADT-amd-cmpt.pdf>> See also *Cheatham v. ADT CORP.*, No. CV-15-02137-PHX-DGC, 161 F.Supp.3d 815 (2016); and

*Michael Edenborough & Ors., v. ADT, LLC d/b/a ADT Security Services, INC.*, United States District Court, N.D. California (Filed Feb 27, 2017)

<sup>643</sup> *Baker v ADT Corporation* No 14 cv 8988 Case No. 1:14-cv-08988 Filed 9.11.2014. See also *Cheatham v. ADT CORP.*, No. CV-15-02137-PHX-DGC, 161 F.Supp.3d 815 (2016)

<sup>644</sup> Edenborough, above n 642. The judge granted a stay, as a Settlement Agreement had been signed to (pending court approval) settle all claims as part of a national class settlement in *Dale Baker v. The ADT Corporation* and ADT, LLC d/b/a ADT Security Services, Case No. 15-cv-02038-CSB-DGB (U.S.D.C. C.D. Illinois).

informational claims, and the failure to address well-known and easily preventable security flaws.<sup>645</sup> While the claim would likely succeed in Australia based upon (allegedly) misleading and deceptive security representations,<sup>646</sup> it is contentious in the US.<sup>647</sup> There is no “actual” harm pleaded, rather the FTC allege a failure which placed consumers at “significant risk of harm”<sup>648</sup> and is “likely” to cause “substantial injury”.<sup>649</sup> However, recent US authority suggests that harm is not “unfair” under section 45(n) if “speculative”, less than intangible or a low likelihood occurrence, regardless of its magnitude.<sup>650</sup> D-Link is defending itself aggressively,<sup>651</sup> claiming the case is false, “speculative” and any settlement would render it “hostage” to “unrelentingly litigious [FTC] oversight”.<sup>652</sup> The Acting FTC Chair agrees thematically at least: her FTC reforms will end both ‘speculative’ injury cases as regulatory overreach,<sup>653</sup>

---

<sup>645</sup> *FTC v D-Link Corporation and D-Link Systems, Inc.*, Case No: 3:17-cv-00039 filed 5 Jan 2017; Complaint for permanent injunction and other equitable relief, United States District Court of California, San Francisco Division <[https://www.ftc.gov/system/files/documents/cases/170105\\_d-link\\_complaint\\_and\\_exhibits.pdf](https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf)> unfair or deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), in connection with Defendants’ failure to take reasonable steps to secure the routers and Internet-protocol cameras they designed for, marketed, and sold to United States consumers.

<sup>646</sup> While there is no “law” in Australia that defines CIOT device security, as Ch. 5 suggests, ACL section 18 catches conduct ‘likely’ to mislead or deceive, which the courts have found, renders it unnecessary to prove that anyone was misled or deceived at all: *Parkdale Custom Built Furniture Pty Ltd v Puxu Pty Ltd* [1982] HCA 44. The word “likely” means a real or not remote chance or possibility of conduct being misleading or deceptive “regardless of whether it is less or more than 50%”: *Global Sportsman Pty Ltd v Mirror Newspapers Limited* (1984) 2 FCR 82.

<sup>647</sup> Jeremy Goldman, Partner, Frankfurt Kurnit Klein & Selz who specializes in digital law cited in Michael Kan, ‘The FTC IoT security case against D-Link is a test of power’ *ComputerWorld* (6 Jan 2017 accessed 20 Jan 2017) <<http://www.computerworld.com/article/3155464/security/the-ftc-iot-security-case-against-d-link-is-a-test-of-power.html>>

<sup>648</sup> Above n 645: 7.

<sup>649</sup> Above n 645: 27. Acts or practices are unfair under s 5 if they ‘cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition: 15 U.S.C. § 45(n)’.

<sup>650</sup> *LabMD, Inc. v. The Federal Trade Commission*, Petition for Review of a Decision of the FTC’ Case No 16-16270-D, US Court of Appeals for the Eleventh Circuit, (10 Nov 2016) <<http://www.thompsoncoburn.com/docs/default-source/default-document-library/labmddecision8d702626dda26f05acb8ff0000ba5cc9.pdf?sfvrsn=0>> Under the FTC Act, section 45(n), an action or practice is unfair if it “causes or is likely to cause substantial injury to consumers”. The FTC had reversed an administrative law finding harm due to an unauthorised file disclosure, a ‘privacy harm’ that may have affected reputations or emotions (which is a substantial injury) or alternatively, the unauthorised disclosure was likely to cause substantial injury. It interpreted “likely” to mean “a significant risk”, stating that “a practice may be unfair if the magnitude of the potential injury is large, even if likelihood of the injury occurring is low.” LabMD appealed, arguing that “likely” means a “high probability of occurring” and the 11<sup>th</sup> Circuit held that the FTC interpretation was not reasonable. It held that speculative, “not even intangible” harm was insufficient to be “likely” and therefore not “unfair” as required under section 45(n). It considered extrinsic materials (e.g. FTC, Policy Statement on Unfairness (Dec. 17, 1980)

<<https://www.ftc.gov/publicstatements/1980/12/ftc-policy-statement-unfairness>>) which indicate that the term “likely” was meant to exclude “emotional impact and more subjective types of harm”: Fredric Roth & Melissa Ventrone, ‘11th Circuit better defines FTC’s ‘Unfair’ standard – The details are in the damage’ *Thompson & Coburn LLP* (29 Nov 2016 accessed 5 Dec 2016) <<http://www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes/post/2016-11-29/11th-circuit-better-defines-ftc-s-unfair-standard---the-details-are-in-the-damage>>

<sup>651</sup> D-Link has described the FTC case as false, unwarranted and baseless. D-Link has enlisted anti-regulation group, ‘Cause of Action’, which has stated that allowing the FTC to target companies based on the potential for a data breach potential, without actual or likely consumer harm, will result in limitless corporate liability and chill IOT innovation.

<sup>652</sup> D-Link, ‘D-Link Systems Inc. Enlists Cause of Action Institute to Defend Corporate & Consumer Rights’ *Media Release* (10 Jan 2017 accessed 2 Feb 2017) < <http://us.dlink.com/press-centre/press-releases/d-link-systems-inc-enlists-cause-of-action-institute-to-defend-corporate-consumer-rights/>>

<sup>653</sup> She argues FTC enforcement should focus on actual or likely consumer injury, where companies breach promises to consumer’s detriment: Maureen K. Ohlhausen, Acting FTC Chairman ‘Opening Keynote at ABA 2017 Consumer Protection Conference’ (2 Feb 2017 accessed 20 Feb 2017):3 and 6 <<https://www.ftc.gov/public-statements/2017/02/opening-keynote->

and disproportionate FTC settlements “untethered from consumer harm”.<sup>654</sup> Ironically, given the oft-put industry position that law stifles innovation whereas flexibility enhances innovation, one security firm CEO defended D-Link, implying legal uncertainty as to security:

*“You can’t really hold people accountable, when no one knows what the law is doing...”*<sup>655</sup>

Of course, the FTC has clear court-affirmed cybersecurity authority, so there is little doubt that US law requires companies to use commercially reasonable data protection methods against hacking,<sup>656</sup> nor is there reason to suppose that their consumer devices and apps ought not afford such protection too. But clearly, smart home security has been problematic from inception: WikiLeaks has shown that the CIA remotely hacks smart TVs, cars and phones, to activate microphones and cameras for location, audio and text communications surveillance<sup>657</sup> - even when ‘off’. That such “zero-day vulnerabilities” were not advised to device manufacturers left consumers, government and critical infrastructure vulnerable to weaponized device attack.<sup>658</sup> Indeed in 2016, the smart home as an attack vector emerged.<sup>659</sup> An

---

aba-2017-consumer-protection-conference> It is difficult to separate “likely” from “speculative” though it seems that the latter is further along the spectrum.

<sup>654</sup> Ohlhausen argues that the FTC must answer two questions: How were consumers harmed? And how does this action address harm?” She states that consumer harm is necessary to meet their statutory mandate and “good consumer policy”. Later however she contradictorily asserts: “The FTC should focus enforcement on matters where consumers are actually injured or likely to be injured, or where companies don’t keep their promises, to the consumer’s detriment. The agency should focus on cases with objective, concrete harms such as monetary injury and unwarranted health and safety risks. The agency should not focus on speculative injury, or on subjective types of harm”: Ibid: 4.

<sup>655</sup> Robert Graham, Errata Security CEO cited In Kan, above n 647.

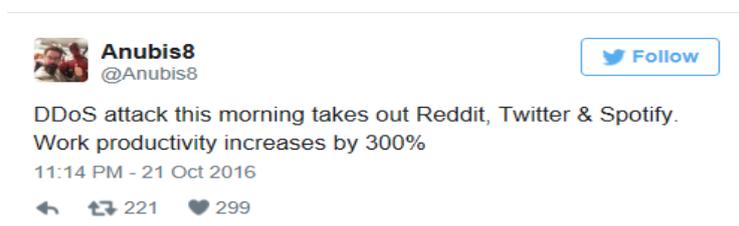
<sup>656</sup> *FTC V Wyndham Worldwide Corporation, Wyndham Hotel Group LLC, Wyndham Hotels and Resorts LLC And Wyndham Hotel Management Incorporated*, United States Court of Appeals for the 3rd Circuit, Case No. 14-3514 (Filed 24 Aug 2015) <https://epic.org/amicus/ftc/wyndham/Mem-Op-14-3514.pdf> at page 10.

<sup>657</sup> Wikileaks, ‘Vault 7: CIA Hacking Tools Revealed’ (7 Mar 2017 accessed 12 Mar 2017) <<https://wikileaks.org/ciav7p1/>> ‘Vault 7’ as Wikileaks call it, contains 8,7761 pages described as a part of the “the majority of [the CIA’s] hacking arsenal including malware, viruses, trojans, weaponized “zero day” exploits, malware remote control systems and associated documentation”. The CIA does not confirm or deny such leaks; but contends “...”legally prohibited from conducting electronic surveillance targeting individuals here at home... and CIA does not do so.”: Central Intelligence Agency, ‘CIA Statement on Claims by Wikileaks’ (8 Mar 2017 accessed 12 Mar 2017) <<https://www.cia.gov/news-information/press-releases-statements/2017-press-releases-statements/cia-statement-on-claims-by-wikileaks.html>> Wikileaks claim the source wishes to “... initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons.”: It is also asserted that the dump describes agency tools, but are not the full programmes and that the latter will be handed to the affected tech companies to enable rectification of their products.

<sup>658</sup> Wikileaks claim that by 2016 end, the CIA had created over a thousand “hacking systems, trojans, viruses, and other “weaponized” malware”: Ibid. Note that spying on American citizens in this manner is illegal (without a FISA warrant) and the CIA denies it has done so.

<sup>659</sup> Danny Palmer, ‘The first big Internet of Things security breach is just around the corner’ *ZDNet* (1 Jul 2016 accessed 2 Aug 2016) < <http://www.zdnet.com/article/the-first-big-internet-of-things-security-breach-is-just-around-the-corner/>> Note that the first alleged criminal smart home device hack occurred in late 2013, involving 300,000 malicious emails, many sent via home routers, multi-media systems, smart TVs and “at least one refrigerator”: MarketWatch, ‘Proofpoint Uncovers Internet of Things (IoT) Cyberattack’ *Proofpoint Press Release* (16 Jan 2014 accessed 2 Feb 2016) < <http://www.marketwatch.com/story/proofpoint-uncovers-internet-of-things-iot-cyberattack-2014-01-16>> The attack was simple- relying largely upon misconfigured devices or those set up using default passwords only. c/f Paul Thomas, ‘Despite the News, Your Refrigerator is Not Yet Sending Spam’, Symantec (Jan. 23, 2014), <<http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam>>

'apocalyptic'<sup>660</sup> DDoS<sup>661</sup> attack involving tens of millions of hacked smart home devices<sup>662</sup> disrupted US East Coast internet traffic; crashing sites from Spotify to PayPal, to the New York Times.<sup>663</sup> As one wag (later) tweeted:



Graphic 3.1: Some Americans retained a sense of humour  
Source: USA TODAY<sup>664</sup>

The attack caused widespread consumer detriment and significant business cost. Security researchers advise the best defence is to patch each vulnerable device, in a slow (sometimes impossible) process depending upon device age, access and capability. While it was perhaps the first mass consumer experience with smart home insecurity, more will follow:

“It will keep going... Even if there’s a power outage, [the malware] will just be back and re-infect the devices. It’s never going to stop...”<sup>665</sup>

### (b) Smart self

*What kind of loser hacks into Fitbit accounts?*<sup>666</sup>

<sup>660</sup> Shaun Waterman, 'FTC, reigning in data actions, is urged to drop D-Link case' cyberscoop (2 Feb 2017 accessed 20 Feb 2017) < <https://www.cyberscoop.com/ftc-data-actions-ohlhausen-trump-d-link-case/>>

<sup>661</sup> The acronym stands for distributed denial of service, which means an attack which overwhelms the system with data, usually an overload of a web server through requests to view its pages. While there are other methods, the aim is to shut down a site: Zetter, above n 596.

<sup>662</sup> Such as routers, video recorders and security cameras: Jedidiah Bracy, 'The IoT Zombies are already at your front door' *Privacy Tech* (29 Sept 20-16 accessed 2 Oct 2016) <https://iapp.org/news/a/how-poorly-secured-iot-devices-can-take-down-your-website/>

<sup>663</sup> The attack blocked traffic to the US internet directory servers of Dyn, flooding it with malicious requests which disrupted the entire system. It began at 7:10 a.m. ET Friday morning and was resolved by 6.17 pm. It affected Twitter, Spotify, Netflix, Amazon, Tumblr, Reddit, PayPal and other sites. It used Mirai software which uses malware in phishing emails to first infect a home network or computer, then spreads across the network, taking over set-top boxes, dvr's, routers and security cameras used by businesses and retailers: these devices in turn create a robot network, or botnet, to send the millions of messages that knocks the out victims' computer systems. Mirai was released on the so-called dark web.

<sup>664</sup> Eli Blumenthal and Elizabeth Weise, 'Hacked home devices caused massive Internet outage', *USA TODAY* (21 Oct. 2016 accessed 22 Oct. 2016) <<https://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/>>

<sup>665</sup> Allison Nixon of Flashpoint, cited in DDoS Attacks, 'IoT malware clashes in a botnet territory battle' (18 Apr 2017 accessed 19 Apr 2017) < <http://ddosattacks.net/iot-malware-clashes-in-a-botnet-territory-battle/>> The latest software is Hajime, which is "Mirai on steroids" infecting around 100,000 devices internationally in six months.

<sup>666</sup> Ibid, citing a post on the Fitbit community forum.

Wearables are highly hackable. Researchers have hacked health-critical smart devices: insulin pumps,<sup>667</sup> pacemakers,<sup>668</sup> implantable defibrillators,<sup>669</sup> drug infusion drips and even MRI scanners.<sup>670</sup> One recent study showed that patient lives, privacy and hospital networks are at risk due to device vulnerabilities.<sup>671</sup> In response, the Australian Therapeutic Goods Administration (TGA), ‘reminds’ manufacturers to “perform risk assessments”,<sup>672</sup> while smart fitness devices<sup>673</sup> for “general wellness”<sup>674</sup> are non-TGA and largely unregulated. As Fitbit’s CEO explains, “It’s not a medical-grade device; it’s a consumer device. In that setting, it works incredibly well.”<sup>675</sup>

Smart self devices have “severe security vulnerabilities”.<sup>676</sup> HPE research found that all smartwatches tested had security flaws which exposed user data, and 30% allow user account penetration.<sup>677</sup> IEEE

---

<sup>667</sup> Jonathan D. Rockoff, ‘J&J Warns Insulin Pump Vulnerable to Cyber Hacking’ *The Wall Street Journal* (4 Oct 2016 accessed 6 Oct 2016) <<http://www.wsj.com/articles/j-j-warns-insulin-pump-vulnerable-to-cyber-hacking-1475610989>>

<sup>668</sup> Darlene Storm, ‘Pacemaker hack says worm could possibly ‘commit mass murder’ *ComputerWorld* (17 Oct 2012 accessed 18 Apr 2016) <<http://www.computerworld.com/article/2473402/cybercrime-hacking/pacemaker-hacker-says-worm-could-possibly--commit-mass-murder-.html>>

<sup>669</sup> In December 2016, researchers found security flaws in ten currently-used ICDs: Eduard Marin, Dave Singelée, Flavio D. Garcia, Tom Chothia, Rik Willems and Bart Preneel, ‘On the (in)security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them’ (2016 accessed 2 Dec 2016): 1

<<https://www.esat.kuleuven.be/cosic/publications/article-2678.pdf>> Hackers may command devices to administer a (fatal) shock, disable therapy or steal patient data, and track user location: Jeremy Kirk, ‘Pacemaker hack can deliver a deadly 830volt jolt’ *ComputerWorld* (17 Oct 2012 accessed 18 Apr 2016) <<http://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html>>

<sup>670</sup> Lauren Zanolli, ‘Welcome to Privacy Hell, Also Known As The Internet Of Things’ *FastCompany* (23 Mar 2015 accessed 6 Apr 2016) <<http://www.fastcompany.com/3044046/tech-forecast/welcome-to-privacy-hell-otherwise-known-as-the-internet-of-things>>; James Niccolai, ‘Thousands of medical devices are vulnerable to hacking security researchers say’ *PCWorld* (29 Sept 2015 accessed 4 Apr 2016) <<http://www.pcworld.com/article/2987813/thousands-of-medical-devices-are-vulnerable-to-hacking-security-researchers-say.html>>

<sup>671</sup> Eduard Marin, Dave Singelée, Flavio D. Garcia, Tom Chothia, Rik Willems and Bart Preneel, ‘On the (in)security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them’ (2016 accessed 2 Dec 2016): 1 <<https://www.esat.kuleuven.be/cosic/publications/article-2678.pdf>> they proved that remote hacks using off-the-shelf equipment is possible, due to sensor and monitor inter-connectivity, remote monitoring and near-field communications technology.

<sup>672</sup> Australian Govt, Department of Health, ‘Device cybersecurity a key issue’ *Medical Devices Safety Update* 4:2 (Mar 2016 accessed 16 Jan 2017) <<https://www.tga.gov.au/sites/default/files/medical-devices-safety-update-volume-4-number-2-march-2016.pdf>>

<sup>673</sup> The Australian TGA can impose security-related standards but industry product development timelines mean they may lag the latest security standards.

<sup>674</sup> See U.S. FDA, above n 203. This non-binding guidance stipulates that : “general wellness products” are both: (1) “...intended for only general wellness use...” and (2) “present a low risk to the safety of users” and others.

<sup>675</sup> Selina Wang, ‘Fitbit’s Move into Medical Gadgets Risks Attracting FDA Scrutiny’ *Bloomberg Technology* (15 Apr 2016 accessed 20 Aug 2016) <<https://www.bloomberg.com/news/articles/2016-04-15/fitbit-s-move-into-medical-gadgets-risks-attracting-fda-scrutiny>>

<sup>676</sup> Hiltz, above n 204. They looked at (inter alia) Fitbit Charge HR, Apple Watch, Jawbone Up 2, Garmin’s Vivosmart, Withings Pulse O2, Basis Peak, Mio Fuse, and Xiaomi Mi Band.

<sup>677</sup> 70% of firmware was unencrypted, data flows went through multiple (unknown) backend destinations via its app, cloud interfaces used weak passwords; communications are “trivially intercepted” in 90% of cases: Hewlett Packard (HPE), ‘Internet of Things Security Study: Smartwatches’ Submission to FTC PrivacyCon 2016 (2016 accessed 6 Apr 2016) [https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00050-98093.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00050-98093.pdf)

claim that 9 of 9 reviewed fitness trackers expose user location data.<sup>678</sup> While data theft seems less common, the ecosystem is of itself a business risk – as each employee logging onto a work network by device opens up another system attack point.<sup>679</sup> Cases are few, but there is a market for consumer fitness device information. Fitbit,<sup>680</sup> recently suffered a spate of fraudulent warranty claims, arising from leaked and stolen accounts;<sup>681</sup> with hackers<sup>682</sup> boasting they accessed leaked account logins and passwords (from third party sites) traded online on forums and websites for between 50 cents and \$5 per record.<sup>683</sup> Accessible data included name, weight, GPS data, regular running routes, and (possibly) sleeping patterns from hundreds of accounts (at least), but there is no public evidence of mass data theft. As such, the fraud – obtaining a new Fitbit falsely under warranty - is low level. While Fitbit (belatedly) posted additional security advice<sup>684</sup> they view this as third party theft - though acknowledge that double encryption would have been ‘smarter’ security. These deficiencies may not be significant for an average user, unless device data accuracy becomes an issue. Researchers show that apps reveal logins and failed to stop data tampering during transmission, which allows hackers to enter false data. Accuracy becomes important if device data is admitted in evidence in a court case or for a prosecution,<sup>685</sup> or employers adopt a corporate wellness program or life or health insurers use data to assess premiums or other incentives.<sup>686</sup> False data may yield prejudicial inferences or expose users to personal risk, such as for example, placing a person at a crime scene or removing information indicative of a medical condition. Consumers may thus face financial and personal injury, discrimination or adverse assumptions based upon inaccurate or false data. Consumer guarantee issues as to (in)accuracy are discussed further in chapter 5.

---

<sup>678</sup> Researchers have also hacked into children’s HereO smart watches allowing access to family location and location history: Whittaker, above 619.

<sup>679</sup> “Companies that offer service via mobile devices will be vulnerable, as well as organizations where BYOD includes new IoT devices.” Richard Kam, ‘The security of IoT: Is your Fitbit a key for criminals?’ *IAPP* (22 Jan 2016)

<<https://iapp.org/news/a/the-security-of-iot-is-your-fitbit-a-key-for-criminals/>>

<sup>680</sup> PC, ‘Digital Disruption: What do governments need to do?’ *Research Paper* (June 2016 accessed 10 June 2016) <<http://www.pc.gov.au/research/completed/digital-disruption/digital-disruption-research-paper.pdf>>

<sup>681</sup> One hacker claimed the motivation to be “warranty fraud” and “social engineering”, until the manufacturer improves security and/ or changes its policy: Sara Spary, ‘These Fraudsters Say They Broke Into Fitbit Accounts Using Passwords Bought For 50 Cents’ *BuzzFeedNews* (7 Jan 2016 accessed 12 Nov 2016) <[https://www.buzzfeed.com/sarasparry/revealed-the-self-styled-hackers-who-defrauded-fitbit?utm\\_term=.ney9vY8Pq#.ceaXrLZjW](https://www.buzzfeed.com/sarasparry/revealed-the-self-styled-hackers-who-defrauded-fitbit?utm_term=.ney9vY8Pq#.ceaXrLZjW)>

<sup>682</sup> Fitbit security spokesperson said it was not a hack, but rather fraud – as the data had been purchased from third party sites and not stolen from Fitbit.

<sup>683</sup> *Ibid.*

<sup>684</sup> Fitbit now recommends customers use multi-factor authentication by signing in via Google and avoid reusing passwords across different sites: Fitbit, ‘Can someone take over my account?’ *Fitbit Help* (n.d. accessed 10 Nov 2016) <[https://help.fitbit.com/articles/en\\_US/Help\\_article/1969](https://help.fitbit.com/articles/en_US/Help_article/1969)>

<sup>685</sup> A recent Australian case rejected use of Fitbit sleep data, although it was a family court matter, decided on its facts: *Oster & Houli* [2015] FCCA 398 (25 February 2015) The judge refused to accept Fitbit evidence as to child’s sleep patterns.

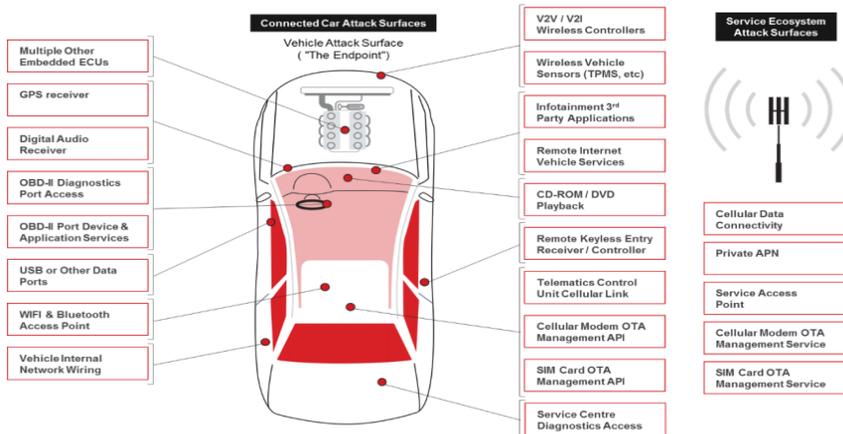
<sup>686</sup> Hilts, above n 197.

(c) Smart cars

...the FBI and NHTSA are warning the general public and manufacturers – of vehicles, vehicle components, and aftermarket devices – to maintain awareness of potential issues and cybersecurity threats related to connected vehicle technologies in modern vehicles...<sup>687</sup>

It's scary to know you could be driving down the highway and a hacker could seize control of your car. Toyota never mentions this risk when extolling its technology to sell you the car...<sup>688</sup>

There are no Australian smart car security cases or known complaints,<sup>689</sup> but US cases are emerging.<sup>690</sup> Bond-like scenarios of cars careening out of driver control, criminal ransomware attacks or assassin/terrorists remotely hijacking vehicles to kill or kidnap occupants, or bomb targets, are suddenly possible and alarming. Car hacking<sup>691</sup> is simply, the infiltration of vehicle software systems and becomes easier as system complexity and software multiplies.<sup>692</sup>



Graphic 3.2 Connected Car Attack Surface

Source: GSMA<sup>693</sup>

<sup>687</sup> FBI, 'Motor vehicles increasingly vulnerable to remote exploits' (17 Mar 2016 accessed 11 May 2016) <

<https://www.ic3.gov/media/2016/160317.aspx>>

<sup>688</sup> Goldman Scarlato & Penny, P.C., 'Cahen v. Toyota' (2 Feb 2016 accessed 11 May 2016)

<<http://iotclassaction.com/cahen-v-toyota/>>

<sup>689</sup> Note that most car manufacturers are adept at managing complaints through their dealer network or in-house through manufacturer customer-assistance centres. These records, unless sufficient in number or severity to warrant public recall action, never become public.

<sup>690</sup> It is standard practice in the automotive industry to rely upon overseas data, as the Australian market is so much smaller and potentially, slower to reveal potential problems. There seems little reason why this principle ought not also apply with respect to substantiating consumer detriment. See for example, the recent Toyota Takata airbag recall which began in the US and flowed into the Australian market even though there were no Australian incidents:

<http://www.toyota.com.au/news/toyota-australia-recalls-vehicles>. In the year to June 2016 end, 2.5 million cars were recalled in Australia, with 15 brands announcing 92 recalls: ACCC, 'Product Safety Australia', (17 Aug 2016) <[www.recalls.gov.au](http://www.recalls.gov.au)>

<sup>691</sup> A definition is: is the "manipulation of the code in a car's electronic control unit (ECU) to exploit a vulnerability and gain control of other ECU units in the vehicle": Margaret Rousem 'Car Hacking' TechTarget

<<http://internetofthingsagenda.techtarget.com/definition/car-hacking>>

<sup>692</sup> The average car sold today has 60 microprocessors in it.

<sup>693</sup> GSMA, above n 113.

Since 2015, researchers have hacked vehicles such as Jeep Cherokee,<sup>694</sup> various VW, BMW, Audi and Toyota,<sup>695</sup> Ford and GM,<sup>696</sup> Tesla (and other marques)<sup>697</sup> the Nissan app,<sup>698</sup> and insurance dongles<sup>699</sup> - enabling remote control<sup>700</sup> of steering, braking and/ or disabling of driving features.<sup>701</sup> Given the catastrophic potential detriment of car hacks, there is no public evidence that it has occurred, but the CIA clearly has expertise.<sup>702</sup> After the Jeep hacks and despite zero customer reports, Fiat recalled 1.4 million cars for software updates, supposedly setting an “important precedent” in security vulnerability response,<sup>703</sup> although one which is mandatory in Australia with respect to safety-related defects. Recent research suggests that VW (allegedly) has ignition<sup>704</sup> and keyless entry vulnerabilities affecting almost 100 million cars,<sup>705</sup> ran a Tesla off-road from 22 kilometres away<sup>706</sup> and hacked a Jeep in Missouri wirelessly - from Pittsburgh.<sup>707</sup>

---

<sup>694</sup> The infamous Jeep case involved remote control of windscreen wipers, dashboard functions, transmission, speed and brakes; the researchers disabled the brakes and crashed the car (gently) into a ditch. The initial hack involved laptops wired into the Jeep. By 2015, the hacks could be performed remotely: Greenberg, above n 400.

<sup>695</sup> Cara McGoogan, ‘BMW, Audi and Toyota cars can be unlocked and started with hacked radios’ *The Telegraph* (25 Apr 2016 accessed 25 Apr 2016) <<http://www.telegraph.co.uk/technology/2016/03/23/hackers-can-unlock-and-start-dozens-of-high-end-cars-through-the/>>

<sup>696</sup> Joe Acker, ‘Toyota, Ford, GM Topple Car Hacking Claims’ *Law360* (25 Nov 2015 accessed 16 Aug 2016) <<https://www.law360.com/articles/731922/print?section-automotive>>

<sup>697</sup> Ibid. The following were susceptible: Audi: A3, A4, A6; BMW: 730d; Citroen: DS4 CrossBack; Ford: Galaxy, Eco-Sport; Honda: HR-V; Hyundai: Santa Fe CRDi; Kia: Optima; Lexus: RX 450h; Mazda: CX-5; Mini: Clubman; Mitsubishi: Outlander; Nissan: Qashqai, Leaf; Opel: Ampera; Range Rover: Evoque; Renault: Traffic; Ssangyong: Tivoli XDi; Subaru: Levorg; Toyota: Rav4; Volkswagen: Golf GTD, Touran 5T.

<sup>698</sup> Pete Bigelow, ‘Nissan disables Leaf app due to hacking concerns’ *autoblog* (25 Feb 2016 accessed 3 Apr 2016) <<http://www.autoblog.com/2016/02/25/nissanconnect-ev-leaf-app-hacking-followup/>> Researchers found that using the VIN and basic web-development knowledge, climate controls and trip logs for any Leaf that used the NissanConnect EV app were accessible, anywhere in the world. Aside from privacy breach, theoretically, using heat or air conditioning could drain the battery.

<sup>699</sup> Metromile and Progressive dongle hacks have enabled control of the car.

<sup>700</sup> John Markoff, ‘Researchers Show How a Car’s Electronics Can Be Taken Over Remotely’ *The New York Times* (9 Mar 2011 accessed 16 Mar 2016) <<http://www.nytimes.com/2011/03/10/business/10hack.html>>

<sup>701</sup> Bojanova, above n 625.

<sup>702</sup> Wikileaks, above n 657.

<sup>703</sup> NHTSA Recall Campaign Number 15V461000. There is now a class action pleading that this has reduced vehicle value.

<sup>704</sup> The attack uses cheap radio hardware to intercept key fob signals and use them to clone the key. However, the real-world potential for the attack has been questioned: the thief must be located within 300 metres of the car and the shared key code also required may be found within different components in different model year VWs. A second issue was found with the use of HiTag2 cryptography, which is an old “legacy security algorithm, introduced 18 years ago. Its manufacturer no longer recommends be used in cars: Andy Greenberg, ‘A New Wireless Hack can Unlock 100 Million Volkswagens’ *WIRED* (10 Aug 2016 accessed 12 Aug 2016) <https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/>

<sup>705</sup> Flavia D. Garcia, David Oswald, Timo Kasper and Pierre Pavlides, ‘Lock It and Still Lose It – On the (In)Security of Automotive Remote Keyless Entry Systems’ *Proceedings of the 25th USENIX Security Symposium* (10-12 August 2016, Austin, TX) <<https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia>>

<sup>706</sup> Olivia Solon, ‘Team of hackers take remote control of Tesla Model S from 12 miles away’ *The Guardian* (21 Sept 2016 accessed 3 Oct 2016) <<https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes>>

<sup>707</sup> Pete Bigelow, ‘Jeep in St. Louis hacked from’ *autoblog* (21 Jul 2016 accessed 3 Sept 2016) <<http://www.autoblog.com/2015/07/21/jeep-choke-hacked/>> The researchers remotely controlled braking, transmission and steering via a security hole in Chrysler’s UConnect infotainment system

In the real world, smart car consumers have suffered car theft, data theft, and other forms of cyberattack. US police recently arrested hackers who stole over 100 Jeeps in Texas,<sup>708</sup> and ransomware attacks have occurred whereby malicious code installed in smart cars disables them, until criminals are paid.<sup>709</sup> Computer-based door hacks and decryption or amplification attacks upon car key fobs are now recognised methods of car theft.<sup>710</sup> Further misuse or theft of manufacturers' credentials led to over 100 cars being remotely immobilised in Texas,<sup>711</sup> and GPS "spoofing"<sup>712</sup> may allow hackers to hijack navigation systems.<sup>713</sup> Aside from these media-reported examples, EPIC assert that records are "woefully inadequate" and that as at 2015, only 6 of 14 manufacturers claimed they could detect wireless intrusions.<sup>714</sup> Perhaps in response to growing media, security industry<sup>715</sup> and regulator concern, US DOT released (criticised) Proactive Safety Principles,<sup>716</sup> and the Global Manufacturers released unenforceable, (low-level) privacy principles<sup>717</sup> and "aspirational" (best practice) security principles.<sup>718</sup> The new NHTSA Federal Policy weakly proposes "voluntary" compliance reports, unsanctioned

---

<sup>708</sup> Reese Counts, 'Hackers arrested after stealing more than 30 Jeeps in Texas' *autoblog* (4 Aug 2016 accessed 3 Sept 2016) < <http://www.autoblog.com/2016/08/04/hackers-steal-30-jeeps-houston-texas/>> The thieves accessed Fiat Chrysler's DealerCONNECT software, then entered the vehicle identification number, and reprogrammed vehicle security systems to accept a generic key.

<sup>709</sup> Such code has been installed via mechanics' diagnostic USBs and remotely: Nora Young, 'Your Car Can be Held for Ransom', *CBCradio* (May 22, 2016 accessed 4 Jun 2017) <<http://www.cbc.ca/radio/spark/321-life-saving-fonts-ransomware-cars-and-more1.3584113/your-car-can-be-held-for-ransom-1.3584114>>

<sup>710</sup> Nick Bilton, Keeping Your Car Safe From Electronic Thieves, *N.Y. Times* (Apr. 15, 2015 accessed 4 Jun 2016) < <http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html>.>; Andy Greenberg, 'Radio Attack Lets Hackers Steal 24 Different Car Models', *WIRED* (Mar. 21, 2016) <<https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/>.>; Cadie Thompson, 'A Hacker Made a \$30 Gadget That Can Unlock Many Cars That Have Keyless Entry', *Tech Insider* (Aug. 6, 2015 accessed 25 Aug 2016) < <http://www.techinsider.io/samy-kamkar-keyless-entry-car-hack-2015-8>>; and

<sup>711</sup> Kevin Poulsen, Hacker Disables More than 100 Cars Remotely, *WIRED* (Mar. 17, 2010) <<https://www.wired.com/2010/03/hacker-bricks-cars/>> The system allows the dealer to disable the ignition system, or trigger the horn to remind owners when a payment is due.

<sup>712</sup> Spoofing is "the act of broadcasting a fake GPS signal to fool a device into thinking it's somewhere else, and/or at a different point in time."

<sup>713</sup> Guy Buesnel, 'GPS Spoofing Is Now A Real Threat – Here's What Manufacturers of GPS Devices Need to Know' Spirent (Sept. 14, 2015 accessed 4 Jun 2016) < [http://www.spirent.com/Blogs/Positioning/2015/September/GPS\\_Spoofing\\_Is\\_a\\_Real\\_Threat](http://www.spirent.com/Blogs/Positioning/2015/September/GPS_Spoofing_Is_a_Real_Threat)>

<sup>714</sup> EPIC, Cahen, 'Brief of Amicus Curiae Electronic Privacy Information Center in Support of Plaintiffs-Appellants and in Support of Reversal' (5 Aug 2016 accessed 20 Sept 2016) < <https://epic.org/amicus/cahen/EPIC-Amicus-Cahen-Toyota.pdf>>

<sup>715</sup> See for example, I Am the Cavalry, above n 586.

<sup>716</sup> Department of Transport (US), 'Proactive Safety Principles' (2016 accessed 7 Jun 2016) <<https://www.transportation.gov/briefing-room/proactive-safety-principles-2016>>; Jay W Belle Isle, 'Claybrook: DOT's "Proactive" Safety Principles Worthless' Legal Reader (18 Jan 2016 accessed 2 Jun 2016) <<http://www.legalreader.com/claybrook-dots-proactive-safety-principles-worthless/>>

<sup>717</sup> Auto Alliance, above n 399. These "... in many respects fell short of what was required under Canadian privacy laws": K. Thompson and Arie van Wijngaarden, 'Cybersecurity Best Practices for Connected cars Released' (16 Aug 2016 accessed 2 Sept 2016) <<http://www.canadiancybersecuritylaw.com/2016/08/cybersecurity-best-practices-for-connected-cars-released/>>; Lawson, above n 36 (Privacy Analysis). The author is of the view they also fall short of the Australian Privacy Principle requirements (see Ch. 5).

<sup>718</sup> C-ISAC is an industry-funded body designed to facilitate security information-sharing and will oversee the principles: C-ISAC, 'Automotive Cybersecurity Best Practices' (2016) <https://www.automotiveisac.com/best-practices/>>

vulnerability disclosures<sup>719</sup> and describes evolving cybersecurity as requiring more research before “regulatory standard(s)”.<sup>720</sup> Australia has not tackled these issues in recent reports either: the NTC avoid smart car security issues,<sup>721</sup> to focus upon local road rule questions while no doubt, awaiting international solutions for the bigger concerns.

As to cases, there is no Australian smart car litigation, though there is a record of safety-related software defects necessitating safety-based recall – which are latent product defects of significant concern to consumers.<sup>722</sup> These represent 60 to 70% of all EU/ US recalls.<sup>723</sup> Australia has had over thirty vehicle-related software defect recalls since 2014 (**Sched. 3**) - but no identifiably smart car litigation to date. While US consumer laws differ from Australian approaches, in fundamental effect there is sufficient thematic similarity to warrant consideration – especially in a litigation-weak CIOT context. The first US class action *Cahen et al v Toyota et al*,<sup>724</sup> alleges a failure to ensure “basic electronic security”,<sup>725</sup> such that basic functions are susceptible to hostile take-over, endangering occupant safety. The case identifies information asymmetry and market failure, pleading unfair, deceptive and/ or fraudulent business practices by manufacturers<sup>726</sup> which cost owners money (through diminution of vehicle value) and for failure to inform owners that their cars are hackable, marketing them as ‘safe’ when they knew otherwise, and risking “theft, damage, serious physical injury, or death”, while enabling covert insecure data collection and transmission.<sup>727</sup>

---

<sup>719</sup> To the industry Auto-ISAC body. This is voluntary and so may depend upon each type and severity of case.

<sup>720</sup> NHTSA, above n 327: 21.

<sup>721</sup> In its C-ITS report, they with some reservation, assert the Privacy Act to be sufficient protection and their recent enquiry as to regulatory responses to trials (etc) does not address smart car security regulation at all: .NTC, ‘Executive Summary, Regulatory Options for Automated Vehicles’ *Issues Paper* (Feb 2016 accessed 30 May 2016) <[http://www.ntc.gov.au/Media/Reports/\(66E42530-B078-4B69-A5E3-53C22759F26E\).pdf](http://www.ntc.gov.au/Media/Reports/(66E42530-B078-4B69-A5E3-53C22759F26E).pdf)> as to privacy, see NTC, above n 406.

<sup>722</sup> A recent recall by GM involved 4.3 million cars for an air bag software defect, which has been “linked” to one death and three injuries in the United States.

<sup>723</sup> Bill Fleming, IEEE Vehicular technology magazine cited by Philip Ross, ‘A Cloud connected car is a hackable car, worries Microsoft’ IEEE Spectrum, (11 Apr 2014 accessed 5 Sept 2016) < <http://spectrum.ieee.org/tech-talk/transportation/advanced-cars/a-connected-car-is-a-hackable-car>>

<sup>724</sup> *Cahen, Tompulis, Nisam, Gibbs and Langdon C. v. Toyota Motor Corporation, Toyota Motor Sales, USA Inc., Ford Motor Company, General Motors LLC, and Does 1 through 50*, Case No 15-CV-01104-WHO (Filed 1 July 2015) < <https://epic.org/amicus/cahen/Cahen-First-Amended-Complaint.pdf>>

<sup>725</sup> Ibid.

<sup>726</sup> The case was pleaded in common law fraud and contract (breach of warranty) plus Californian statutory violations including: Unfair Competition Law (“UCL”), Cal. Bus. Prof. Code § 17200, et seq.; Consumers Legal Remedies Act (“CLRA”), Cal. Civ. Cod § 1250, et seq. False Advertising Law (“FAL”), Cal. Bus. Prof. Code § 17500, et seq.; Implied Warranty of Merchantability, Cal. Com. Code § 2314; Song-Beverly Consumer Warranty Act, Cal. Civ. Code §§ 1791.1 & 1792; and breach of privacy under the Constitution, Cal. Const. art. I, § 1. FAC ¶¶ 62-138.

<sup>727</sup> Ibid: 3 [6 and 7]

“...even though drivers have reasonable expectation of privacy as to such data, defendants share it with or sell it to third parties, often without adequate security (making it an attractive target for hackers).”<sup>728</sup>

The complaint cites the *Markey Report* (2015) which found a “clear lack of appropriate security measures to protect drivers against hackers... or against those who may wish to collect and use personal driver information”.<sup>729</sup> While initially dismissed for lack of standing and failure to state a claim (‘speculative’ injury),<sup>730</sup> the plaintiff has appealed.<sup>731</sup> In Australia, it is possible such a claim could proceed under ACL sections 18 and 29, especially if vehicle security standards conflicted with representations or failed to comply with an Australian Standard (Ch 5). A second US case is *Flynn*<sup>732</sup> which (again) alleged manufacturer fraud (as to undisclosed, as-yet unmaterialized future risks) which inflated vehicle prices:

“A vehicle purchased, leased, or retained under the reasonable assumption that it is safe is worth more than a vehicle known to be subject to the unreasonable risk of catastrophic accident because of defects... Plaintiffs... are subjected to a continuing increased risk of severe injury or death but for the Defendants’ failure to disclose or remedy the defect.”<sup>733</sup>

It is alleged that the vehicle Uconnect system is defective, unmerchantable and not reasonably safe for its intended use within the vehicle. That claim might be argued in Australia relying upon consumer guarantees as to acceptable quality and (less likely) fitness for purpose, and strict products liability, which are further discussed in **chapter 4**.

---

<sup>728</sup> Ibid: 3 [6]

<sup>729</sup> Ibid: 1.

<sup>730</sup> Dismissal grounds included a lack of standing, failure to substantiate (future) economic loss and ‘speculative’ injury. Federal courts have judicial power over “cases” and “controversies”: US Constitution Art III. Standing requires plaintiffs establish (inter alia) Injury-in-fact, which means the plaintiff suffered an invasion of a concrete, particularized, and actual or imminent (and not conjectural or hypothetical) “legally protected interest”: EPIC, ‘Cahen v. Toyota Motor Corporation’ Epic.org (n.d. accessed 8 Aug 2016) < <https://epic.org/amicus/cahen/#EPIC>>

<sup>731</sup> Cahen, above n 723, Appellants’ Opening Brief <https://epic.org/amicus/cahen/Appellant-Cahen-Opening-Brief.pdf>; EPIC, ‘Cahen v. Toyota Motor Corporation’ Epic.org Amicus Curiae (n.d. accessed 8 Aug 2016) <<https://epic.org/amicus/cahen/#EPIC>>

<sup>732</sup> *Flynn, Brown et al v. FCA US Llc F/K/A Chrysler Group LLC and Harmon International Industries, Inc*, US Dist Court Sthern Dist Illinois, Case No. 3:15-cv-855, Class Action Complaint: [https://www.law360.com/dockets/download/55c103f7a36d4660ce000028?doc\\_url=https%3A%2F%2Fecf.ilsd.uscourts.gov%2Fdoc1%2F06913233689&label=Case+Filing](https://www.law360.com/dockets/download/55c103f7a36d4660ce000028?doc_url=https%3A%2F%2Fecf.ilsd.uscourts.gov%2Fdoc1%2F06913233689&label=Case+Filing); Memorandum Of Law In Support Of Its Motion To Dismiss The Amended Class Action Complaint: <<http://Www.Liabilitydesk.Com/Wp-Content/Uploads/2016/02/15-Cv-00855-Mjr-Dgw-Document-71-1.Pdf>> See also Steven Trader, ‘Drivers in Fiat Car Hacking Suit Say their injuries are real’ *Law360* (22 Mar 2016 accessed 16 Aug 2016) <[http://www.law3560.com/articles/774475/drivers-in-fiat-car-hacking-suit-say-ther-injuries-are-real?article\\_related\\_content=1](http://www.law3560.com/articles/774475/drivers-in-fiat-car-hacking-suit-say-ther-injuries-are-real?article_related_content=1)>

<sup>733</sup> Cahen above n 723. See also Acker, above n 696.

## 3.2 Big CIOT data uses and (ab)uses

*It's kind of amazing that we all settled on the term "big data" before the "Internet of things" really arrived... {it} will generate information on a scale we can't really comprehend yet..."<sup>734</sup>*

*"People give out their data often without thinking about it... they have no idea that it will be sold to third parties."<sup>735</sup>*

Big data is significant and absent regulatory control, promises consumers discrimination and algorithmic defect. Given their infinite potential for significant future consumer detriment and potential overlaps into Chs. 5 and 6, these two significant consumer issues are very briefly considered here.

### 3.2.1 Big(ger) data can be "discriminating"

*"Internet of things" sensor data is high in quantity, quality and sensitivity. This means the inferences that can be drawn are much bigger and more sensitive...."<sup>736</sup>*

*Profiling technologies are by their very nature discriminatory tools. They allow unparalleled kinds of social sorting and segmentation which could have unfair effects..."<sup>737</sup>*

*"Algorithms, when they are not transparent, can lead to a distortion of our perception, they can shrink our expanse of information."<sup>738</sup>*

Deliberate or unethical corporate data use and discrimination are another contentious aspect of CIOT data collection. Consumers already complain of offensive or 'creepy' data collection and targeted advertising in online retail<sup>739</sup> and social media,<sup>740</sup> but with CIOT, that creepiness will increase, because

---

<sup>734</sup> Krazit, above n 186.

<sup>735</sup> EC Vice-President Viviane Reding cited in Aleks Krotowski, 'Big Data age puts privacy in question as information becomes currency' *The Guardian* (22 April 2012 accessed 28 Mar 2015) <<http://www.theguardian.com/technology/2012/apr/22/big-data-privacy-information-currency>>

<sup>736</sup> Mauritius Declaration, 'Resolution on Big Data' 36th International Conference of Data Protection and Privacy Commissioners (15 Oct 2015 accessed 7 Feb 2016) <<http://www.privacyconference2014.org/media/16427/Resolution-Big-Data.pdf>>

<sup>737</sup> David Wright, 'A Framework for the ethical impact assessment of information technology' *Ethics and Information Technology* (2011) 13:199–226 accessed 3 Mar 2016 <http://dl.acm.org/citation.cfm?id=2035938>

<sup>738</sup> Chancellor Angela Merkel cited in Kate Connolly below. They may create "filter bubbles and echo chambers": Eli Pariser, 'Beware online filter bubbles' *TED 2011* (mar 2011 accessed 2 Nov 2016) <[https://www.ted.com/talks/eli\\_pariser\\_beware\\_online\\_filter\\_bubbles/transcript?language=en](https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles/transcript?language=en)> reducing the diversity of information or channelling it to fit previous behaviours rather than providing a balanced selection of information.

<sup>739</sup> The infamous *Target* pregnancy advertising case reveals the dilemma: where *Target* faced an irate parent, who learned of his teenage daughter's pregnancy – via her purchase history- profiled catalogue advertising in his mailbox. The predictive model was based upon consumer spending patterns, applied to its customer database and used to target catalogue coupon offers: Charles Duhig, 'Campaigns mine personal lives to get out vote' *The New York Times* (14 Oct 2012 accessed 15 Mar 2014):1 <[http://www.nytimes.com/2012/10/14/us/politics/campaigns-mine-personal-lives-to-get-out-vote.html?\\_r=0](http://www.nytimes.com/2012/10/14/us/politics/campaigns-mine-personal-lives-to-get-out-vote.html?_r=0)>

<sup>740</sup> Social media – and especially Facebook - is implicated: it has tracked user web purchases, posted purchase information on that user's friend's newsfeeds, and conducted mass 'emotional contagion' experiments: Benjamin R. Mulcahy and Dante M. DiPasquale 'Efficiency v. Privacy: is online behavioral advertising capable of self-regulation?' (14 April 2010 accessed 15 Mar 2015) <http://documents.lexology.com/f7f5451b-f755-4c1e-b855-521f924ee99b.pdf> Re experiments, see Adam D. I. Kramer, Julie E. Guillory and Jeffery T. Hancock, 'Experimental Evidence of Massive-Scale Emotional contagion through Social Networks' 111 *Proc. Nat'l Acad. Sci. USA* 8788 (2014) Note Facebook could not exclude minors from its sample,

seemingly unimportant data can “in aggregate reveal a lot about what a person gets up to...”<sup>741</sup> Alphabet and Facebook make millions annually from user data in a highly successful business plan - which CIOT providers are rapidly positioning themselves to emulate.<sup>742</sup>

Data mining enables data analytics: the application of mathematical and statistical modelling of data to locate meanings, patterns and draw conclusions, inferences, and even, predictions. IBM has already illustrated that home electricity and sensor data can allow accurate extrapolations as to human behaviour, preferences and habits within a smart home.<sup>743</sup> Trivial data snippets can reveal when dinner is cooked, which rooms occupied, by how many people, and whether someone smokes.<sup>744</sup> This can be socially beneficial if ‘safely’(?) anonymised<sup>745</sup> or by explicit consent,<sup>746</sup> but not if home occupants (and visitors) are unknowingly profiled in daily life, or where individual behaviours are modified to avoid “detection” of perceived anomaly.<sup>747</sup> Smart carmakers can use telematics to track vehicle problems by user behaviour and/ or location, and smart self devices monitor user ‘fitness’ patterns - to gain “actionable insights” for product improvement but also, personalised (behavioural) services and marketing, profiling and categorization. Add this data trove to publicly available sources, and purchased broker data, and CIOT

---

which added to allegations that the study was unethical: Kashmir Hill, ‘Facebook Added ‘Research’ To User Agreement 4 Months After Emotion Manipulation Study’ *Forbes* (30 June 2014 accessed 30 July 2014) <<http://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/>> Facebook has also done research to determine if users are lonely and whether ads perform better with algorithmically-generated (i.e. fake) friend ‘endorsements’: James Grimmelmann, ‘The Law and Ethics of Experimenting on Social Media Users’ unpublished working paper provided to the author by email, Mar 2015: manuscript page 4. Professor Grimmelmann formally complained to the FTC but there has been no public outcome.

<sup>741</sup> Nick Heath, ‘I know what you ate last supper: What home sensors will reveal about your life’ *Techrepublic* (5 Feb 2-014 accessed 4 Mar 2-16) <<http://www.techrepublic.com/blog/european-technology/i-know-what-you-ate-last-supper-what-home-sensors-will-reveal-about-your-life/>>

<sup>742</sup> In Facebook’s case, manipulating users for research purposes was not conducted with user consent beyond their usual terms and conditions, which were retrospectively changed: Hill, above n 740.

<sup>743</sup> IBM Human Centric Solutions, ‘Innovation for the People of a Smarter Planet’ (2015 accessed 4 Apr 2016) <[http://www03.ibm.com/able/news/bolzano\\_video.html](http://www03.ibm.com/able/news/bolzano_video.html)> The researchers ‘taught’ the system to recognise which specific devices were in use and graphical data enabled them to guesstimate (accurately) when people ate pasta for dinner. Sensors read carbon monoxide/ dioxide, temperature and humidity.

<sup>744</sup> Heath, above n 771.

<sup>745</sup> For example, in a smart grid context enabling better deployment of electricity resources.

<sup>746</sup> For example, an Italian seniors ‘Living Safe’ project where sensor data generated home maintenance alerts and even, profiled daily routines so that helpers could be sent if a resident inexplicably deviated. The outcome was positive: participants reported an improved lifestyle (66%) and the City Council saved 31% in elder care costs: IBM Human Centric Solutions, ‘Innovation for the People of a Smarter Planet’ (2015 accessed 4 Apr 2016) <[http://www03.ibm.com/able/news/bolzano\\_video.html](http://www03.ibm.com/able/news/bolzano_video.html)>

<sup>747</sup> Art 29 WG, above n 49: 8. In a smart car context, those modifications are usually perceived as positive: drivers will drive more carefully knowing their driving is surveilled. In smart fitness, the view is similar: people will do more inspired by their tracker, or via its social competition apps. In reality, people opt out of the latter if they develop fitness fatigue or just get sick of the device: Stephanie Lee, ‘Why Activity Trackers could be Running out of Steps’ *BuzzFeed News* (28 Feb 2015 accessed 23 Mar 2016) <<http://www.buzzfeed.com/stephaniemlee/why-activity-trackers-could-be-running-out-of-steps#.cgReqWyJd>>

offers providers massively increased revenue potentials through data sales and insightful consumer knowledge.<sup>748</sup>

There are four main concerns whereby the “benign differentiation”<sup>749</sup> detected by the CIOT may through collection, dissemination and fusion<sup>750</sup> and analytics, adversely affect consumer interests: discrimination, market distortion through price discrimination,<sup>751</sup> data inaccuracy and criminal uses. Firstly, discrimination arises through algorithmic profiling which enables digital “redlining” via categorisation; which inevitably adversely affects the vulnerable. This may distort the market through differential pricing<sup>752</sup> or through automated profiling software which ‘scores’ consumers based upon real, inferred or predicted attributes as to suburbs, housing, job security, health, insurance, employment, creditworthiness, payment capacity and so on.<sup>753</sup> Consumers have no control over the facts or inferences<sup>754</sup> drawn or their categorisation – but may experience latent discriminatory consequences. The CIOT exacerbates this by volume and its oft-assumed accuracy. Potentially discriminatory government, employer and insurer already exist: the US government assesses individual’s “risk”<sup>755</sup> via algorithm, as well as “physiological and behavioural

---

<sup>748</sup> Lawson, above n 36: 29.

<sup>749</sup> Peppet, above n 283.

<sup>750</sup> Jeff Hagens, co-founder of SmartThings stated that 10,000 households alone can generate over 150 million data points a day – the information may be mundane (temperature etc) but collectively, can “produce extremely detailed profiles of your behaviour”:

<sup>751</sup> Price discrimination is ‘differential pricing’ is and is defined as the practice of charging consumers different prices for the same product; usually based upon the goal of pricing based upon what people are prepared to pay, rather than costs. It is accepted in some areas: for example, cinemas charge different prices to children, pensioners etc. There are three types: “personalized” or “first degree price discrimination” occurs where sellers charge different buyers different prices (e.g. individually- negotiated prices); quantity discounts (second degree price discrimination) is where the “per-unit price falls” with amounts purchased; and third degree price discrimination refers to different pricing for different groups (e.g. children’s discounts): Executive Office of the President, ‘Big Data and Differential Pricing’ Feb 2015 accessed 10 May 2016) [https://obamawhitehouse.archives.gov/sites/default/files/whitehouse\\_files/docs/Big\\_Data\\_Report\\_Nonembargo\\_v2.pdf](https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf). The Competition and Consumer Act 2010 (Cth) formerly prohibited price discrimination in relation to the supply/ acquisition of goods of “like grade or quality” but this was repealed in 1995. The rationale was that misuse of market power would address any cases of significance.

<sup>752</sup> People in higher-income areas received greater discounts in one study, though it was unclear if this reflected local competitive forces legitimately or not: Jennifer Valentino-Devries and Jeremy Singer-Vine, ‘Websites vary prices, deals based on User’s information’ *The Wall Street Journal* (24 Dec 2012 accessed 20 Apr 2015) <<http://www.wsj.com/articles/SB10001424127887323777204578189391813881534>>

<sup>753</sup> One example involved a US businessman whose credit limit was reduced after a holiday where he shopped in stores with patrons who exhibited a “poor repayment history”: N. Newman ‘How big data enables economic harm to consumers, especially to low-income and other vulnerable sectors of the population’ *Journal of Internet Law*, 18(6), 11-23 (2014 accessed 3 Apr 2015) <<http://search.proquest.com/docview/1639829818?accountid=26503>> Google was also found to have knowingly allowed illegal pharmacies to target ill people through its *Adwords* search engine function.

<sup>754</sup> *Ibid.* For example, one data broker classified those who responded to sweepstakes offers on a “sucker list” which it promoted as an ideal “subprime credit offer” grouping. Categories reveal the concern: “...’ethnic second-city strugglers’, ‘retiring on empty: singles’, ‘tough start: young single parents’, ‘credit crunched city families’, and ‘rural and barely making it’...”

<sup>755</sup> See for example, *EPIC v. Customs and Border Protection (Analytical Framework for Intelligence) Complaint* (Filed 18 Jul 2014) Civil Action No. 14-1217 US District Court for the Dist of Columbia <<https://epic.org/foia/dhs/cbp/afi/>> EPIC sought CBP disclosure as to a passenger screening program combining detailed personal information with “secret algorithms” to devise traveller “risk assessments”, including US citizens. EPIC filed an appeal to a refusal on 6 April 2017.

signals” indicative of the likelihood of committing a crime,<sup>756</sup> and in criminal sentencing.<sup>757</sup> Employers may analyse CIOT data in talent analytics and recruitment<sup>758</sup> and monitor employees’ behaviour, location, whether in the office, company car or via their smartphone use. Employee wellness programmes already incentivize data sharing through free fitness monitors and apps, but as Peppet suggests, these have unexpected, inferred negative correlations.<sup>759</sup> Frequent ‘exercise’ for example, may imply impulsivity and self-gratification – which (apparently) correlates to higher credit card debt, drug and alcohol abuse, eating disorders and smoking. Sleep problems correlate to poor psychological health, poor cognition and depression.<sup>760</sup> In smart cars, acceleration, braking patterns or geolocation may suggest certain personality traits, smart home data may reveal work hours and mobile phone app use has many personal correlations.<sup>761</sup> Such inferential, prejudicial conclusions in the hands of government, employer, insurer, marketer, financier or others may unfairly elevate consumer risk profiles, adversely limit or deny prospects or opportunities – and/ or cost consumers personally and economically.

Secondly, profiling overlaps with price discrimination which may create both “market power [with]in product markets” and market inefficiency<sup>762</sup> as consumers are not fairly informed of all prices.<sup>763</sup> User-based insurance (UBI) is a contentious case in point. Insurers welcome driver data,<sup>764</sup> as do low-risk

---

<sup>756</sup> Jason Tashea, ‘Courts are Using AI to sentence criminals. That must stop now’, *WIRED* (17 Apr 2017 accessed 18 Apr 2017) <[https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/?mbid=nl\\_41717\\_p1&CNDID=>](https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/?mbid=nl_41717_p1&CNDID=>); Mitch Smith, ‘Wisconsin, a Backlash Against Using Data to Foretell Defendants’ Futures’ *The New York Times* (22 Jun 2016 accessed 10 Feb 2017) <[https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html?\\_r=0>](https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html?_r=0>)

<sup>757</sup> See as to the COMPAC scale, Megan Garber, ‘When Algorithms Take the Stand’ *The Atlantic* (30 Jun 2016 accessed 10 Feb 2017) <<https://www.theatlantic.com/technology/archive/2016/06/when-algorithms-take-the-stand/489566/>> Angwin’s research suggests that COMPAS predictions had about a 60% accuracy. She concludes it is biased against blacks, and as to algorithms: “We trust them too much”: Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, “Machine Bias” (May 23, 2016) ProPublica <<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>> Algorithmic predictions are given to judges in Arizona, Colorado, Delaware, Kentucky, Louisiana, Oklahoma, Virginia, Washington and Wisconsin “...to inform decisions about who can be set free at every stage of the criminal justice system, from assigning bond amounts... to even more fundamental decisions about defendants’ freedom”. ProRepublica analysed risk scores for 700 People and found that 20% of those predicted to commit violent crimes did so within two years and that when all possible crimes (including misdemeanours) were included, the algorithm had a 61% accuracy as to those deemed likely to reoffend within two years. The algorithm creator disputes the findings.

<sup>758</sup> Burdon, above n 336.

<sup>759</sup> Peppet, above n 283.

<sup>760</sup> Ibid.

<sup>761</sup> Kaivan Karmi, ‘The Role of Sensor Fusion and remote emotive Computing (Rec) in the Internet of Things 6-7 (2013) <[http://cache.freescall.com/files/32bit/doc/white\\_paper/SENFEIOTLFWP.PDF](http://cache.freescall.com/files/32bit/doc/white_paper/SENFEIOTLFWP.PDF) cited Ibid. Mobile phone data such as accelerometer/ gyroscope, heart rate data and how a consumer holds their phone, types a message (and so on) may all, so analysts assert, reveal certain emotions or mental states.

<sup>762</sup> Newman, above n 753. Sellers increase profits but buyers lose: “Economic models generally show that overall prices in the economy will end up higher than any model where consumers know all prices...”

<sup>763</sup> Newman, above n 753 citing Joseph Stiglitz.

<sup>764</sup> Insurers business model seeks to mitigate insurance risk, lower fraud and optimise profit. While traditional car insurance premiums may reduce with accidents, it is likely that smart car contents insurance will increase, as will cyber insurance. Business opportunities will also boom via existing customer bases, insurance expertise, brand value, fraud department skills and price comparison website familiarity – these may add to consumer business models: Jain, above n 245.

consumers who welcome premiums reflecting that risk.<sup>765</sup> Smart home, car and self data offers insurers many benefits<sup>766</sup> - including marketable data - but UBI may present unfair price discrimination potentials, as well as risks where data may be shared, disclosed, used for investigations, claims surveillance and enforcement purposes.<sup>767</sup> For example, one Australian UBI insurer promises not to use collected driving data in claims or investigations – unless it does:

Your own data is not used against you in claims unless it supports other compelling evidence of fraud or information that leads us to believe that you may have misrepresented the truth.<sup>768</sup>

The CIOT may exacerbate insurance price discrimination, against vulnerable consumers - the elderly, the poor and the sick – resulting in insurance denial or unaffordability. Australian caryard financiers are already using GPS dongles to locate and immobilise vehicles if consumers fall behind in payments.<sup>769</sup> Privacy-intrusive tracking is often incentivized: car loans are contingent upon dongle consents, or Oscar credit an Amazon gift card \$1 every day customers meet an algorithm-driven fitness target.<sup>770</sup> In Australia, health insurers already partner with brands such as Fitbit to offer consumers points and incentives for healthy behaviours, though usually via separate loyalty programmes rather than premium reductions.<sup>771</sup> AAMI's Safe Driver app collects speed, braking, fatigue and smartphone use data – but consumer returns are questionable: consumers *may* get free roadside assist upon renewal,<sup>772</sup> and QBE 'suggest' premiums may reduce. Behavioural economists assert that incentivized safe driving or fitness is unlikely to change those who most need it: the young and fit are more likely to strive for Oscar's \$1 and millennials are also more likely to use UBI (44%).<sup>773</sup> How this plays out for those who are less advantaged seems obvious, absent specific regulatory protections which can address algorithmic discrimination.<sup>774</sup>

---

<sup>765</sup> These include 'pay-as-you-drive' or 'pay-how-you-drive' approaches.

<sup>766</sup> For example, improved fraud reduction, automated notice of loss, improved accident investigations and liability determination, stolen vehicle tracking and disabling, vehicle monitoring, geo-fencing, etc.

<sup>767</sup> David Lindsay cited in McNamara, above n 339.

<sup>768</sup> Insurance Box, 'Journey data privacy policy' (n.d. accessed 2 Apr 2017) <<http://insurancebox.com.au/documents/privacy-promise.pdf>>

<sup>769</sup> Car yards offering finance in most states have begun deploying the devices, which can track the movements of a car and even immobilise it if a payment is missed: Tom Cowie, 'Car yards offering finance in most states have begun deploying the devices, which can track the movements of a car and even immobilise it if a payment is missed seat' The Sydney Morning herald (5 Oct 2014 accessed 6 Feb 2016) <<http://www.smh.com.au/national/gps-trackers-put-repo-man-in-passenger-seat-20141001-10os1q.html>>

<sup>770</sup> Lapowski, above n 339.

<sup>771</sup> See for example, the QANTAS Assure program which has an insurance component offered by QBE.

<sup>772</sup> McNamara, above n 339.

<sup>773</sup> Nielsen, 'Usage-based Insurance and telematics' (2016 accessed 2 Aug 2016) <<http://www.nielsen.com/us/en/insights/reports/2016/usage-based-insurance-and-telematics.html>>

<sup>774</sup> There are potential evidential problems in establishing that an algorithm has a discriminatory effect and hence, specific legislation after an inquiry and regulatory gap analysis, would be the best approach.

Finally, the risk of data error or inaccuracy is serious: it defeats data 'relevance' and may impact consumers through inequity and inefficiency.<sup>775</sup> Those not feeding data may become socially marginalised or fall off the social policy spectrum altogether.<sup>776</sup> Further despite privacy rights, data correction (much less withdrawal of consent or deletion) is almost impossible when consumers may not know which CIOT entities hold or analyse their data. Almost certainly, legal gaps may arise as to extant discrimination-protected categories, such as age, disability, race and sex<sup>777</sup> but also, that novel or refined forms of discrimination will arise needing regulatory protection.<sup>778</sup> Though beyond scope here, Australian anti-discrimination laws are limited in effect and unlikely to protect against economic (or other) sorting based upon data-induced analysis of individual personality, habit and character traits.<sup>779</sup> For example, while employers are free not to hire those with covertly perceived traits they do not like, data 'analysis' may provide a scientific gloss to decision-making which overrides interviewer perception; insurers may calculate premiums or cover based upon inferences which are not individually accurate, lenders may infer creditworthiness likewise, and many other situations may arise where analysed traits provide inaccurate inferences or relevance. That these may be prejudicial, wrong or unfair, and taint a person's record (perhaps) indefinitely,<sup>780</sup> are all potential issues for consumer discrimination law. Criminal use is also ever-present: profiling also enables highly targeted, predatory marketing tactics which prey upon

---

<sup>775</sup> The US right-to-work 'e-verify' system is an example where inaccurate results have dire consequences. Errors have been found due to multiple surnames, surname changes and the like; but have reduced error rates for US citizens over 60% in the past five years – which suggests it may originally have caused some chaos: EOP, above n 41: 52.

<sup>776</sup> An example of this in Boston concerned a mobile app used to repair road potholes (using smartphone GPS and accelerometer data) to help the Public Works Dept allocate its resources for repairs. It disproportionately favoured younger, wealthier neighbourhoods and discriminated against poorer, more socially disadvantaged areas due to user distribution: Baker & McKenzie, 'Internet of Things: Some Legal and Regulatory Implications' (Feb 2016 accessed 16 Mar 2016): [15http://www.bakermckenzie.com/files/Uploads/Documents/Australia/ar\\_australia\\_internetofthings\\_feb16.pdf](http://www.bakermckenzie.com/files/Uploads/Documents/Australia/ar_australia_internetofthings_feb16.pdf)

<sup>777</sup> Federal legislation is as follows: *Australian Human Rights Commission Act 1986 (Cth)*, *Age Discrimination Act 2004 (Cth)*, *Disability Discrimination Act 1992 (Cth)*, *Racial Discrimination Act 1975 (Cth)* and *Sex Discrimination Act 1984 (Cth)*. State laws are: *Anti-Discrimination Act 1977 (NSW)* *Anti-Discrimination Act 1996 (NT)* *Anti-Discrimination Act 1991 (Qld)* *Anti-Discrimination Act 1998 (Tas)* *Discrimination Act 1991 (ACT)* *Equal Opportunity Act 1984 (SA)* *Equal Opportunity Act 2010 (Vic)* *Equal Opportunity Act 1984 (WA)*

<sup>778</sup> For example, in NSW, audio recording without consent is a criminal offence, but video recording is lawful. See the federal *Surveillance Devices Act 2004 (Cth)*. States legislation is *Surveillance Devices Act 1999 (Vic)*, *Surveillance Devices Act 2007 (NSW)*, *(NT)*, *Invasion of Privacy Act 1971 (Qld)*, *Surveillance Devices Act 1998 (WA)*, *Listening Devices Act 1991 (Tas)*, *Surveillance Devices Act 1998 (WA)* *Listening Devices Act 1991 (Tas)*; and the federal, *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth)*. Use of surveillance devices by the Australian Security Intelligence Organisation (ASIO), the Australian Security Intelligence Service (ASIS) or the Defence Signals Directorate (DSD) are covered by the *Australian Security Intelligence Organisation Act 1979 (Cth)* and the *Intelligence Services Act 2001 (Cth)*.

<sup>779</sup> Australian Human Rights Commission (AHRC), 'A Quick Guide to Australian Discrimination Laws' (2014 accessed 8 Aug 2016) <<https://www.humanrights.gov.au/employers/good-practice-good-business-factsheets/quick-guide-australian-discrimination-laws>>

<sup>780</sup> As discussed above, the Privacy Act enables access to data for correction purposes, but it may be that an individual does not know who holds their data to ask that question, or that the data per se appears unremarkable or unchallengeable but the algorithm which interprets it generates what an individual might perceive to be unfair or inaccurate inferences. Access to that "value-added" data is not necessarily guaranteed under the PA which again, may be a gap.

perceived individual vulnerabilities, and allows unscrupulous scammers to target the vulnerable.<sup>781</sup> As Peppet suggests, in the consumer IOT, privacy norms are fractured<sup>782</sup> and “...everything may reveal everything *enough* to justify real concern”.<sup>783</sup> and the intrusive nature of CIOT data and fusion,<sup>784</sup> analysed via big data/ algorithms, enables context-violating data use which “breaks privacy norms”.<sup>785</sup>

### 3.2.2 Artificial intelligence & a brave new consumer world

“...the development of full artificial intelligence could spell the end of the human race...”<sup>786</sup>-  
Stephen Hawking

“Artificial Intelligence implicates a wide range of economic, social, and political issues...”<sup>787</sup>

“I’m sorry Dave I can’t do that...” Hal, 2001

The CIOT’s future is artificial intelligence.<sup>788</sup> Of all aspects of qualitative difference and unlimited scope, the “...seemingly all-knowing algorithm”<sup>789</sup> and impacts of artificial/ machine intelligence within smart cars, homes and self remain exponential and exceptional. Suffice to say, the transformational nature of consumer devices which respond to consumer demand but may come to generate demand itself, and to control and regulate consumer lifestyle and wellbeing, portends revolutionary societal change with potentially unknown scope, scale and stakes.

---

<sup>781</sup> An example is where illegal pharmacies targetted ill people through Google’s *Adwords* search engine function. This cost Google a \$500 million civil forfeiture settlement, representing gross advertising revenue plus gross revenue made by Canadian online pharmacies from illegal drug sales in the US: US Department of Justice, ‘Google Forfeits \$500 Million Generated by Online Ads and Prescription Drug Sales by Canadian Online Pharmacies’ (24 Aug 2011 accessed 25 April 2015) <<http://www.justice.gov/opa/pr/google-forfeits-500-million-generated-online-ads-prescription-drug-sales-Canadian-online>>

<sup>782</sup> Nissebaum cited in footnote 239, Peppet above n 283: 124.

<sup>783</sup> Peppet, above n 283:121.

<sup>784</sup> Essentially this means combining data from two or more contemporaneous sources, to gain greater depth of insight – for example, combining smart home data with Fitbit data may reveal what a person does at home in greater detail.

<sup>785</sup> Nissebaum cited in footnote 239: Peppet above n 283: 124.

<sup>786</sup> Sonali Kohli, ‘Bill Gates joins Elon Musk and Stephen Hawking in saying artificial intelligence is scary’ *Quartz* (29 Jan 2015 accessed 25 May 2016) < <http://qz.com/335768/bill-gates-joins-elon-musk-and-stephen-hawking-in-saying-artificial-intelligence-is-scary/>>

<sup>787</sup> EPIC, ‘Testimony to ‘The Promises and Perils of Emerging Technologies for Cybersecurity, 115th Cong.’, U.S. Senate Committee on Commerce, Science, & Transportation (22 Mar 2017 accessed 28 Mar 2017): 1 <<https://epic.org/testimony/congress/EPIC-SCOM-IoTandAI-Mar2017.pdf>>

<sup>788</sup> Mark Jaffe, ‘IoT Won’t Work Without Artificial intelligence’ *WIRED* (n.d. accessed 3 Mar 2016)

<http://www.wired.com/insights/2014/11/iot-wont-work-without-artificial-intelligence/>; Cade Metz, ‘Artificial intelligence is setting up the internet of things for a huge clash with Europe’ *WIRED* (11 Jul 2016 accessed 12 Jul 2016) < <http://www.wired.com/2016/07/artificial-intelligence-setting-internet-huge-clash-europe/>>; Tom Simonite, ‘Microsoft and Google want to let artificial intelligence loose on our most sensitive data’ MIT Technology review (19 Apr 2016 accessed 21 Apr 2016) <<https://www.technologyreview.com/s/601294/microsoft-and-google-want-to-let-artificial-intelligence-loose-on-our-most-private-data/>>

<sup>789</sup> Ed Finn of Arizona State University coined this phrase as to John C. Havens, ‘Heartificial Intelligence: Embracing Our Humanity to Maximise Machines’ <<http://www.johnchavens.com/#!books/cdzt>>

Big data, like unsmart devices, is dumb. The entire CIOT design premise is that smart devices will seamlessly learn to anticipate and even shape human needs, rather than merely responding to preferences or detected patterns. In other words, through AI technology, the CIOT ecosystem may learn to shape, manipulate or overtake consumer decision-making.<sup>790</sup> But that learning is imperfect: with AI comes “copying human biases... embedded in data”<sup>791</sup> and the potential encoding of “discrimination in automated decisions...”<sup>792</sup> – for example, Microsoft’s failed AI chatbot Tay,<sup>793</sup> which within hours of online interaction, learnt hate-filled, antisocial mores. Indeed, bias potentials may be innate: the “inadvertent outcome” of the technologies,<sup>794</sup> such that corrective human intervention will be “required”.<sup>795</sup> In this way, algorithms may create device safety (or other) defects through anti-social decision-making. In February 2016, Google’s very safe<sup>796</sup> smart car<sup>797</sup> hit a bus - a trivial ‘bump’<sup>798</sup> – which revealed the non-trivial difficulty of designing algorithms to safely understand social norms.<sup>799</sup> The car’s software required refinement to “more deeply understand” the (playground) principle that big buses are less likely to yield to little cars (even when they should).<sup>800</sup> The root cause was an AI failure to cope with the vagaries of human behaviour. But on road, it seems safe to assume that driving variants are virtually infinite, and that

---

<sup>790</sup> Jaffe, above n 788. Microsoft say: “AI systems feed off both positive and negative interactions with people... In that sense, the challenges are just as much social as they are technical.”: Peter Lee, ‘Learning from Tay’s introduction’ *Official Microsoft Blog* (25 Mar 2016 accessed 4 Apr 2016) < <https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/>>

<sup>791</sup> Professor Alan Whitfield cited in the PC, above n 190. He gives the example that if past human decisions as to recruitment shortlists may build in bias against age, gender or race. Machine learning that emulates human decisions could replicate those biases – e.g. the Tay algorithm that interacted with ‘human’ users, and started spewing Nazi rhetoric.

<sup>792</sup> Saqib Shah and Julian Chokkattu, ‘Microsoft kills AI Chatbot Tay (twice) after it goes full Nazi’ *DigitalTrends* (30 Mar 2016 accessed 4 Apr 2016) <<http://www.digitaltrends.com/social-media/microsoft-tay-chatbot/>>

<sup>793</sup> Microsoft had to apologise and withdraw the bot: “...we’ll look to bring Tay back only when we are confident we can better anticipate malicious intent that conflicts with our principles and values.” Peter Lee, ‘Learning from Tay’s introduction’ *Microsoft Blog* (25 Mar 2016 accessed 15 Aug 2016) <https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/> Note the implied reference to malicious actors going after the bot; whether or not the case, similar concerns have been expressed as to smart car targeting on road as well.

<sup>794</sup> EOP, above n 41. (Algorithmic Systems)

<sup>795</sup> Whitfield, above n 791.

<sup>796</sup> In six years and 1.7 million miles, they tallied only eleven minor accidents and caused none. These were all light-damage, no injury events, fully reported on their website: Google, ‘Google Self-driving Car project Monthly Report July 2016’ (Aug 2016 accessed 14 Aug 2016)

<<https://static.googleusercontent.com/media/www.google.com/en//selfdrivingcar/files/reports/report-0716.pdf>>

<sup>797</sup> Unlike Tesla, Google’s self-driving cars remain in test phase since 2009. Their plan is a completely autonomous vehicle, rather than a phased-in variant. As at 31 July 2016, Google report 24 (modified) Lexus RX450h SUVs and 34 of its prototypes are driving an average of 20-22 thousand miles per week. These cars are contributing to Google’s AI learning and as such, also have a current commercial value to the company.

<sup>798</sup> A Google vehicle (at 2 mph) collided lightly with a transit bus (at 15 mph).

<sup>799</sup> The Google car was in a lane blocked by road works and waiting to merge into the adjacent lane to resume travel. The bus could have given way, but it did not.

<sup>800</sup> Google, ‘Google Self-Driving Car Project Monthly Report’ (Feb 2016 accessed 8 Apr 2016)

<http://static.googleusercontent.com/media/www.google.com/en//selfdrivingcar/files/reports/report-0216.pdf>> See also Chris Ziegler, ‘A Google self-driving car caused a crash for the first time’ *The VERGE* (29 Feb 2016 accessed 3 Mar 2016) <<http://www.theverge.com/2016/2/29/11134344/google-self-driving-car-crash-report>>

there will always been an unlikely, unexpected situation - the consumer safety question is how well systems will adapt – until all cars are connectively smart and thereby, presumably, predictable.



- 1 **Sensors**  
Lasers, radars and cameras detect objects in all directions
- 2 **Interior**  
Designed for riding, not for driving
- 3 **Electric batteries**  
To power the vehicle
- 4 **Rounded shape**  
Maximizes sensor field of view
- 5 **Computer**  
Designed specifically for self-driving
- 6 **Back-up systems**  
For steering, braking, computing and more

Graphic 3.3 Waymo functional prototype self-driving car circa 2016  
Source: Waymo (formerly Google)<sup>801</sup>

It seems likely that smart devices will soon know humans, better than they know themselves. But these looming signposts of success are also risk markers,<sup>802</sup> of which regulators should be acutely aware and which in a *precautionary principle* context, should already inform regulatory decision-making. The GDPR provides that individuals have the right not to be subject to automated process-based and profiled decision-making,<sup>803</sup> but no such 'right' or even a right to 'review' exists in Australian law.<sup>804</sup> As at 2016,

<sup>801</sup> Waymo website <<https://waymo.com/>>

<sup>802</sup> AI superintelligence is, potentially, an existential threat to humankind: Future of Life, 'AI Open Letter' citing Stuart Russell, Daniel Dewey and Max Tegmark, 'Research priorities for Robust and Beneficial Artificial Intelligence' Association for the Advancement of Artificial intelligence' (Winter 2015 accessed 25 May 3016) <<http://futureoflife.org/ai-open-letter>> The concern is that once machines can self-program, they have the independent capacity to retrain themselves faster than their human developers, in a potentially infinite feedback loop – ending in worst case, in human enslavement or extermination. Secondly, like nuclear fission, AI is a "dual use" technology, capable of both great evil and great good. As physicist Stephen Hawking warns, in the short term, the impact depends upon who controls AI, whereas in the long term, the question becomes, can it be controlled at all? If fears as to AI are premised upon computers controlling the world, then the IOT is, unless carefully regulated and controlled, a vital stepping-stone to that eventuality.

<sup>803</sup> GDPR Art. 22, subject to (a) where necessary to enter into a contract; (b) as authorised by the Union or State law which includes safeguards to address "rights freedoms and legitimate interests"; or (c) is based upon the individual's explicit consent. Note that the US Govt released two White House reports – 'Preparing for the Future of Artificial Intelligence' (supra 815) and the 'National Artificial Intelligence Research and Development Strategic Plan'. The Senate Commerce Committee conducted hearings on "The Dawn of Artificial Intelligence (Apr 2017).

<sup>804</sup> PC, above n 190: 308. The PC notes that additional rights to prevent processing relying upon grounds such as consumer distress or an appeal right as to automated decisions "might help engender... community confidence" but points to likely

early smart home digital voice assistants like *Google Now*<sup>805</sup>, *Microsoft's Cortana*<sup>806</sup>, *Amazon's Alexa*,<sup>807</sup> *Apple's Siri*<sup>808</sup> and "*Viv*",<sup>809</sup> are entering consumers' homes. As one technologist comments, it heralds a shift from obeying human commands to looking after humans like a "family pet".<sup>810</sup> It all poses social, ethical and regulatory concerns which loom large over the CIOT: Merkel warns against algorithmic secrecy,<sup>811</sup> the European Parliament is investigating<sup>812</sup> and EPIC has recommended amendments to Asimov's *Rules of Robotics* to specifically address smart devices,<sup>813</sup> while tech luminaries have established OpenAI as an ethical research non-profit.<sup>814</sup> Other leading thinkers have created a Future of Life Institute and Principles.<sup>815</sup> Long term, AI implications must be foremost in CIOT policy maker's minds.

AI is an inevitable part of the CIOT future, as it enables far *greater value* to be extracted from devices and data, through its contextual analysis and interpretation - which in turn creates far greater overall value. AI will monetize data beyond its collector's wildest dreams:<sup>816</sup> as IBM suggests: "...the value of data goes up every day AI advances."<sup>817</sup> Like AI-informed smart cars, smart health value confers massive public policy benefits<sup>818</sup> and is a consumer benefit argument already won.

---

business and enforcement costs. Subject to public interest and individual rights balancing, the EU and UK require consumer notification if an automated decision is being made and allows them to request it not be made or ask that it be reconsidered.

<sup>805</sup> Google speaks via Google Now and on android smartphones, and in smart cars via the Android Auto app.

<sup>806</sup> Cortana speaks across smartphones, on Windows 10 PCs and tablets, and in smart cars.

<sup>807</sup> Alexa is cloud-based and speaks via Echo wireless speakers and via a (non-Amazon) speaker called Tribby.

<sup>808</sup> Siri 'speaks' on iPhone, Apple TV, Apple Watch and in smart cars via a 'CarPlay' app.

<sup>809</sup> See the different 'personalities' of Siri, Alexa, Google and Cortana here: Edward C. Baig, 'Personal digital assistants are on the rise (and they want to talk)' USA TODAY (9 May 2016 accessed 22 May 2016)

<<http://www.usatoday.com/story/tech/columnist/baig/2016/05/08/personal-digital-assistants-rise-and-they-want-talk/83715794/>> Note however, that online is a difficult environment.

<sup>810</sup> Teena Maddox, 'Wozniak talks: Self-driving cars, Apple Watch, and how AI will benefit humanity' TechRepublic (24 June 2015 accessed 25 May 2016) < <http://www.techrepublic.com/article/wozniak-talks-self-driving-cars-apple-watch-and-how-ai-will-benefit-humanity/>>

<sup>811</sup> Kate Connolly, 'Angela Merkel: internet search engines are 'distorting perception'' *The Guardian* (28 Oct 2016 accessed 2 Nov 2016) < <https://www.theguardian.com/world/2016/oct/27/angela-merkel-internet-search-engines-are-distorting-our-perception>>

<sup>812</sup> A cross-party working group will formulate recommendations for submission to the EU Digital Commissioner in 2017, to become guidelines.

<sup>813</sup> 1. A robot may not injure a human; 2. A robot must obey the orders of a human except (1); 3. A robot should protect itself except (1) and (2); 4. A robot must always reveal the basis of its decision ("Algorithmic Transparency") [NEW]; 5. A robot must always reveal its actual identity [NEW]; Mark Rothenberg, Presentation (2016 accessed 2 Nov 2016)

<<https://epic.org/privacy/intl/EPIC-38ICDPPC-kyn-10-16.pdf>>

<sup>814</sup> Open AI, <<https://blog.openai.com/introducing-openai/>>

<sup>815</sup> Future of Life, above n 802 citing Stuart Russell, Daniel Dewey and Max Tegmark, 'Research priorities for Robust and Beneficial Artificial Intelligence' Association for the Advancement of Artificial Intelligence' (Winter 2015 accessed 25 May 2016) <http://futureoflife.org/ai-open-letter> >; Future of Life Institute, 'Asilomar AI Principles' (2017 accessed 20 Feb 2017) <<https://futureoflife.org/ai-principles/>>

<sup>816</sup> Experts at Fortune's 'Brainstorm Technology Conference' point out that the relationship is reciprocal: the development and improvement of AI is dependent upon big data, which is why Google, Amazon and Facebook are already in the AI field. While they provide free (open source) AI software for app developers, its utility is limited: Jonathan Vanian, 'Why Data Is The New Oil' Fortune (11 Jul 2016 accessed 11 Jul 2016) <<http://fortune.com/2016/07/11/data-oil-brainstorm-tech/>>

<sup>817</sup> Ibid.

<sup>818</sup> Smart health will revolutionise medical provision, diagnosis and care. Pressures on health budgets are extreme right across the world, third world health is parlous and CIOT offers a systemic potential to reduce costs, without diminution in care. CIOT benefits include, reduce hospitalisation and consultation time, enable remote patient care, fully inform acute care

### 3.3 Conclusion

This chapter broadly and briefly scopes sophisticated practices and technologies so intertwined with the consumer IOT that soon they will become inseparable from a consumer perspective.<sup>819</sup> But while hacking is a persistent and problematic criminal activity, improved security and big data practices, and socially-responsible AI controls,<sup>820</sup> seem floating somewhere intangible, beyond the law. This is a serious and short-sighted gap. Clearly, hacking can be reduced through better, mandated security practices, just as big data management<sup>821</sup> and AI development<sup>822</sup> can be influenced by clearer constraints and enforcement.<sup>823</sup> This thesis does not pretend to address these critically-serious questions other than to reveal a broader CIOT policy-making context, and to identify related and future consumer detriment. Big data and AI risk potentials are perhaps the starkest illustrations justifying a pre-emptive regulatory approach. Indeed, rather than allowing continued industry development in a gap-riven environment – *more of the same* but squared over volume and time - regulators are better placed to promote positive regulation or self-regulatory practice to address consumer protection issues identified and foreseen, and instil industry best practice by collaboratively setting appropriate incentivising laws in place – as *carrots* to create, promote and justify high industry standards. This approach to CIOT regulation is revisited in **Part IV**.

---

and remotely monitored post-acute care: *Ibid*. An example of the latter is post knee surgery: shoe insole sensors can measure walking foot pressure, and paired with accelerometers, can measure stride cadence – data which can enable a medical assessment of limping, imbalance, activity levels and recovery program progress and effectiveness.

<sup>819</sup> Jaffe, above n 788.

<sup>820</sup> Metz, above n 789.

<sup>821</sup> Susana Etlinger and Jessica Groopman, 'The Trust Imperative: A Framework for Ethical Data Use' *Altimeter* (25 Jun 2015 accessed 2 Aug 2016) <http://www.altimetergroup.com/pdf/reports/The-Trust-Imperative-Altimeter-Group.pdf>

<sup>822</sup> EOP, 'Preparing for the Future of Artificial Intelligence' (Oct 2016 accessed Oct 2016)

[https://www.whitehouse.gov/sites/default/files/whitehouse\\_files/microsites/ostp/NSTC/preparing\\_for\\_the\\_future\\_of\\_ai.pdf](https://www.whitehouse.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf);

Susan Etlinger, "AI" *Altimeter* (Jan 2017 accessed 3 Feb 2017) <http://www.altimetergroup.com/pdf/reports/The-Age-of-Artificial-Intelligence-Altimeter.pdf>

<sup>823</sup> Future of Life, above n 202.

## Chapter 4 ACL and CIOT: an overview<sup>^</sup>

*We are sceptical that consumer protection as currently conceived and implemented will be sufficient to uphold consumer rights in an environment where...devices in our homes, our vehicles and about our persons, become smarter and more connected...- Consumers International*<sup>824</sup>

*You are entitled to expect every business you deal with to honour its obligations under the Australian Consumer Law...*<sup>825</sup>

The Australian Competition and Consumer Commission (**ACCC**) has not publicly addressed the consumer IOT, but has its weather eye, if not resources, on an incoming storm.<sup>826</sup> It has cautioned the app industry,<sup>827</sup> vigorously pursued product defect action and recall actions applicable to ‘devices’,<sup>828</sup> but enforcement work as to consumer guarantees<sup>829</sup> and unfair contract terms<sup>830</sup> in either a device or software context<sup>831</sup> has lagged to the law’s detriment. The recent ACL Review reports that stakeholders mostly assume that the ACL is “flexible enough to adapt” to emerging technologies such as CIOT,<sup>832</sup> but in its final Report, CAANZ implies otherwise, warning that smart devices warrant continuous close monitoring.<sup>833</sup> Their final proposals recommend limited consumer guarantees-related research into “purely digital products” and “emerging technologies” in 2018- 19,<sup>834</sup> in a move unnecessarily narrow and

---

<sup>^</sup>Reader note: This section is a basic overview of ACL provisions potentially relevant in a CIOT context; it does not purport to summarize all relevant law but rather seeks to highlight any uncertainties or gaps. As a reminder from chapter 2, ACCC means Australian Competition and Consumer Commission (the regulator) and CAANZ means Consumer Affairs Australia and New Zealand (the policy-maker).

<sup>824</sup> CI, above n 44.

<sup>825</sup> Michael Schaper, ‘Speech to Council of Small Business of Australia National Small Business Summit, Sydney’ *Australian Competition and Consumer Commission* (27 July 2011 accessed 17 July 2014) [1] <<http://www.accc.gov.au/system/files/SPEECH%20-%20M%20Schaper%20-%20COSBOA%20-%2027%20July%202011%20FOR%20WEB.pdf>>

<sup>826</sup> Discussion between Delia Rickard, ACCC Deputy Chair and the author.

<sup>827</sup> See also ACMA, Mobile apps—Emerging issues in media and communications, *Occasional Paper 1* (May 2013) <<http://www.acma.gov.au/theACMA/Library/researchacma/Occasional-papers/emerging-issues-in-media-and-communications-occasional-papers-1>>

<sup>828</sup> ACCC, ‘Product Safety: A Guide to Testing’ (Oct 2013 accessed 2 Aug 2016) <<https://www.accc.gov.au/publications/a-guide-to-testing-product-safety>>

<sup>829</sup> ACCC, ‘2016 ACCC Compliance and Enforcement Policy’ (Feb 2016 accessed 3 Mar 2016) <[http://www.accc.gov.au/system/files/2016%20ACCC%20Compliance%20and%20Enforcement%20Policy\\_0.pdf](http://www.accc.gov.au/system/files/2016%20ACCC%20Compliance%20and%20Enforcement%20Policy_0.pdf)>; ACCC, ‘The ACCC’s accountability framework for investigations’ (2016 accessed 2 Jun 2016) <<https://foi.accc.gov.au/sites/foi.accc.gov.au/files/repository/ACCC%27s%20accountability%20framework%20for%20investigations.pdf>>

<sup>830</sup> ACCC, ‘Unfair contract terms under scrutiny’ *Media Release* (28 Mar 2017 accessed 28 Mar 2017) <<http://www.accc.gov.au/media-release/unfair-contract-terms-under-scrutiny>>

<sup>831</sup> The ACCC appears to recognise this in announcing its intent to focus upon these areas throughout its 2017 planning.

<sup>832</sup> See CAANZ, ‘Australian Consumer Law Review Final Report’ (Apr 2017 accessed 20 Apr 2017) <[https://cdn.tspace.gov.au/uploads/sites/86/2017/04/ACL\\_Review\\_Final\\_Report.pdf](https://cdn.tspace.gov.au/uploads/sites/86/2017/04/ACL_Review_Final_Report.pdf)> For example, ACL Review Findings 2.6.2: 67. “The review generally found that the ACL is sufficiently flexible to address emerging issues, including dynamic developments in the online environment”.

<sup>833</sup> CAANZ, above n 496 [Interim Report]: 200.

<sup>834</sup> CAANZ, above n 832.

disappointingly delayed.<sup>835</sup> Indeed, the policy approach suggests some contextual “regulatory disconnection”<sup>836</sup> perhaps reflecting all or any of low consumer CIOT complaints,<sup>837</sup> slim market penetration, information lag, planned priority lock-in, time constraints,<sup>838</sup> awaiting other enquiry outcomes, little government impetus<sup>839</sup> - and low stakeholder awareness or concern.<sup>840</sup> Quite legitimately, the ACCC places a resource-honed focus upon risk,<sup>841</sup> over costly pre-emptive research, consumer education or investigative activities.<sup>842</sup> However as this thesis proposes, the consumer IOT evidences such international regulatory concern, research-evidenced detriment, scope-scale-stakes and impending social impact, that consumer detriment pre-emption through compliance-based and properly-resourced<sup>843</sup> consumer and provider education, regulatory stocktake and enforcement action becomes a justified course.<sup>844</sup>

This chapter commences that regulatory stocktake approach. While not purporting to summarize all relevant ACL provisions or catch every potential deficiency, this thesis evidences that the recent ACL

---

<sup>835</sup> Such research, given smart market timings into Australia and overlaid by growing consumer detriments identified in other jurisdictions, is likely to justify expanding their enquiry to how the ACL and other consumer protection legislation responds overall.

<sup>836</sup> Brownsword, cited in Kayleen Manwaring, ‘A Legal Analysis of Socio-Technological Change Arising Out of eObjects’ Working Paper (2016 accessed Jun 2016: 3) <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2690024](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2690024)>

<sup>837</sup> Consumer complaints are a lead indication of detriment, so triggering resources without them raises legitimate risk: benefit questions. There is also evidence that the ACCC’s capacity to consider and escalate complaints is limited: “... only a very small proportion of fair trading complaints (approximately 1%) are ultimately escalated to the round table meeting and/or the under-assessment meeting, raising the possibility that some matters may be ‘missed’”: Australian Labor Party, ‘Submission to the Productivity Commission ACL Review’ (Oct 2016 accessed 12 Oct 2016)

[http://www.pc.gov.au/\\_data/assets/pdf\\_file/0010/206938/sub001-consumer-law.pdf](http://www.pc.gov.au/_data/assets/pdf_file/0010/206938/sub001-consumer-law.pdf) It seems likely to the author however, that the ACCC is discriminating enough to be alert to potentially unique CIOT complaints.

<sup>838</sup> The ACCC escalates some 60 cases of 10,000 complaints per quarter, which means many cases are being ignored. It yields \$1.50 back: ALP, *Ibid*. In contrast the FTC’s enforcement budget is \$50 million (overall for consumer protection, \$184 million) <[https://www.ftc.gov/system/files/documents/reports/fy-2016-2017-performance-plan-fy-2015-performance-report/pprfy16-17\\_0.pdf](https://www.ftc.gov/system/files/documents/reports/fy-2016-2017-performance-plan-fy-2015-performance-report/pprfy16-17_0.pdf)> The ALP also recommends funding for an independent market study function.

<sup>839</sup> Note the FTC has initiated several important conferences this year, including one which dealt specifically with a cross-disciplinary examination of notice and choice including from behavioural economics, psychology and other perspectives.

<sup>840</sup> Few submissions to the ACL Review mentioned CIOT, much less addressed its potential harms. This was especially the case as to submissions from large law firms, representative legal bodies and others whom the Review might legitimately expect would identify legal deficiency. It may be that some of these groups lack sufficient CIOT awareness. For a useful submission as to emerging technology, see ACCAN, ‘Australian Consumer Law Review Submission by ACCAN’ (May 2016 accessed 20 Aug 2016) <

[http://consumerlaw.gov.au/files/2016/07/Australian\\_Communications\\_Consumer\\_Action\\_Network.pdf](http://consumerlaw.gov.au/files/2016/07/Australian_Communications_Consumer_Action_Network.pdf)>; Consumer Action Law Centre, ‘Australian Consumer Law Review’ (30 May 2016 accessed 3 Sept 2016) <<http://consumeraction.org.au/wp-content/uploads/2016/05/Consumer-Action-ACL-Review-Submission-FINAL.pdf>>

<sup>841</sup> For example, the ACCC did not investigate fake online reviews until well after the FTC had exposed a problem: Kate Mathews-Hunt, ‘Gaming the system: fake online reviews v. consumer law’ *Computer Law & Security Review*, 31 (1) (2015): 3-25

<sup>842</sup> In 2015, ACCC Head Rod Simms foreshadowed a hope to increase sectoral research and market analysis: Rod Simms, ‘2015 Priorities’ (19 Feb 2015 accessed 2 Aug 2016) <<http://www.accc.gov.au/speech/priorities-2015>>

<sup>843</sup> Despite the ACCC’s workload ever-increasing, as are enforcement costs - its budget is not. The ACCC has long adopted a selective enforcement approach, its litigation budget is a humble \$24.5 million, which no doubt explains its highly selective (and perhaps conservative) approach to pursuing cases in court.

<sup>844</sup> There is Australian government precedent for this approach in terms of an emerging technology: Australian Government, ‘Cloud Computing Regulatory Stock Take Report’ (21 Jan 2014 accessed 2 Jan 2016) <<https://www.communications.gov.au/publications/cloud-computing-regulatory-stock-take-report%C2%A0>>

review does not go far enough to address emerging or digital technologies. In locating multiple ‘gaps’, uncertainties or deficiencies, suggestive of contextual “regulatory disconnection”<sup>845</sup> the paper evidences how new harms, legal or practical uncertainties, regulatory over/ under-inclusiveness and even, obsolescence<sup>846</sup> require response. Recommendations are underlined in Part III. The chapter frames its recommendations against selected CIOT cases, two illustrative hypotheticals and current ACL interpretations suggestive of required reform.

#### 4.1 An Introduction

The Australian Consumer Law (**ACL**) comprises Schedule 2 of the *Competition and Consumer Act 2010* (Cth) (**CCA**), and is generally regarded as successful,<sup>847</sup> well-administered<sup>848</sup> and (reasonably) internationally-comparative consumer protection legislation.<sup>849</sup> Effective on and from 1 January 2011,<sup>850</sup> it is largely technology neutral and prescribes certain normative foundational principles, together with specific consumer protections. This reflects that broad ‘safety net regulation’ still requires general and specifically prescriptive ‘rule-based’ protections to responsively fill gaps, and to address specific undesirable industry practice or forms of consumer detriment.<sup>851</sup> The principal provisions relevant to consumer IOT issues are prohibitions upon misleading and deceptive conduct and certain false representations, unconscionable conduct, unfair contract terms, consumer guarantees and product liability. Remedies available to both the regulator<sup>852</sup> and successful plaintiffs, are creative, effective and extensive.<sup>853</sup>

---

<sup>845</sup> See for example, the 2016 review: Stephen Corones, Stephen, Sharon Christensen, Justin Malbon, Allan Asher & Jeannie Marie Paterson, ‘Comparative analysis of Overseas Consumer Policy Frameworks’ (April 2016 accessed 26 Jun 2016) < [http://consumerlaw.gov.au/files/2016/05/ACL\\_Comparative-analysis-overseas-consumer-policy-frameworks-1.pdf](http://consumerlaw.gov.au/files/2016/05/ACL_Comparative-analysis-overseas-consumer-policy-frameworks-1.pdf)>

<sup>846</sup> Manwaring cites Bennet-Moses, above n 836: 4-5 but adds in an additional refinement to include “practical” uncertainty to capture whether the law can practically respond, as opposed to “legal uncertainty which is Bennet-Moses’ focus.

<sup>847</sup> Productivity Commission, ‘Draft Consumer Law Enforcement and Administration’ (8 Dec 2016 accessed 8 Dec 2016) <http://www.pc.gov.au/inquiries/current/consumer-law/draft/consumer-law-draft-overview.pdf>

<sup>848</sup> Ibid. See also the ACCC self-assessment under this framework which records few failures: Australian Government, ‘Regulator performance framework’ (2014 accessed 29 Nov 2016) <[https://www.cuttingredtape.gov.au/sites/default/files/files/Regulator\\_Performance\\_Framework2.pdf](https://www.cuttingredtape.gov.au/sites/default/files/files/Regulator_Performance_Framework2.pdf)>

<sup>849</sup> Australia, the UK, US, Canada and Singapore have “high levels of convergence” in their consumer policy frameworks: Corones, above n 845. Note this enquiry was limited to four issues: unconscionable/ unfair trading practices; e-commerce/ peer-to-peer regulation; institutional structures as to administration and enforcement; and consumer access to justice.

<sup>850</sup> The object... is to enhance the welfare of Australians through the promotion of competition and fair trading and provision for consumer protection: *Competition and Consumer Act 2010 (Cth)* (CCA) section 2 ‘Objects’. The unfair contract terms provisions of the ACL commenced effective 1 July 2010.

<sup>851</sup> For example, pyramid selling, door-to-door or unsolicited sales.

<sup>852</sup> In addition to the remedies below, ACL Part 5-1 contains non-court imposed enforcement powers including powers to accept undertakings, substantiation notices and the power to issue public warning notices. Section 134A CCA enables the ACCC to issue infringement notices in lieu of civil penalty proceedings as well.

<sup>853</sup> ACL Ch 5 powers include injunctive relief, pecuniary penalties and compensation orders.

#### 4.1.1 Threshold concepts – definitions & other complications...

The ACL will only apply if various threshold matters are satisfied: firstly, the definitions of ‘person’ and ‘in trade or commerce’, and secondly, certain jurisdiction and enforcement criteria. Other terms such as ‘consumer’ and ‘goods’ apply to certain provisions. These warrant a brief discussion for background:

‘**person**’ includes corporations under CCA section 131, which captures most CIOT device suppliers and natural persons such as company directors under CCA s. 6(3)(b). Section 6(3)(a) also provides that Parts 2-1 (s. 18) and 3-1 (s. 29) apply to corporations as to conduct involving the use of the internet as a “telephonic” service<sup>854</sup> - which means that individuals and corporations operating overseas-hosted internet sites intended for Australian consumer access are also within ACL scope;<sup>855</sup>

‘**in**<sup>856</sup> **trade or commerce**’<sup>857</sup> is defined as “trade or commerce within Australia or between Australia and places outside Australia<sup>858</sup> and includes any business or professional activity (whether or not carried on for profit)”.<sup>859</sup> As Australian CIOT purchases or downloads usually occur via local retail stores or online from Australia, the criteria are usually satisfied. Grey areas as to “free” devices or software (4.1.3 below) may arise, or if an Australian purchases a CIOT device or downloads an app whilst overseas, as ACL jurisdiction may not apply (especially where overseas devices are not intended for sale or sold into the Australian market).

‘**engage in conduct**’ includes ‘doing or refusing to do any act...’<sup>860</sup> or any deliberate omission – “...refraining (otherwise than inadvertently) from doing that act...”<sup>861</sup> This element is often

---

<sup>854</sup> Representations made on the internet fall within the Commonwealth constitutional power as to “postal, telephonic services” so the ACL applies: *Seafolly Pty Ltd v Madden* (2012) 297 ALR 337 at [76]-[79] (Tracey J); *ACCC v Jutsen (No 3)* (2011) 206 FCR 264 at 287 [100] (Nicholas J); *ACCC v Jones (No 5)* [2011] FCA 49 at [6] and [10] (Logan J); *Australian Competition and Consumer Commission v Homeopathy Plus! Australia Pty Limited* [2014] FCA 1412 [

<sup>855</sup> *ACCC v Chen* [2003] FCA 897; *ACCC v Hughes* [2002] FCA 897. The former concerned an individual and the latter, a corporation.

<sup>856</sup> The word “in” qualifies and limits the prohibition to the “... ‘central conception’ of trade or commerce and not to the ‘immense field of activities’ in which corporations may engage in the course of, or for the purposes of, carrying on some overall trading or commercial business.”: *Concrete Constructions (NSW) Pty Ltd v Nelson* (1990) 169 CLR 594: 603 (per Mason, CJ, Deane, Dawson and Gaudron, JJ). In that case conduct as to employment conditions was “with respect to “trade and commerce but not “in” trade and commerce; such that the Trade Practices Act 1974(Cth) section 52 (now s. 18 ACL) did not apply.

<sup>857</sup> Australian Constitution clause 51(i) empowers the Commonwealth to make laws with respect to trade and commerce among the States and with other countries. In *ACCC v Homeopathy Plus! Australia Pty Ltd* [2014] FCA 1412 an argument that website articles (supportive of its business activities)

<sup>858</sup> CAC section 4(1) definition.

<sup>859</sup> ACL section 2(1) definition, which came into effect on 1 January 2011. *Re Ku-ring-gai Co-operative Building Society (No 12) Ltd* (1978) 22 ALR 621 the Court held that “trade or commerce” are words of “the widest import”, not restricted to profit-making activities.

<sup>860</sup> CCA section 4(2)(a)

<sup>861</sup> CCA section 4(2)(c)

satisfied by *representations*: "...a statement made orally or in writing or which is implied from words or conduct." <sup>862</sup> These may appear in the device or app terms and conditions, or in any other form (online or off) whether supplied with a device or software or not, including by device website, marketing materials, advertising or any other claims as to its performance;

**"carrying on a business in Australia"**: *Valve*<sup>863</sup> has recently affirmed that businesses located in a foreign jurisdiction, without a physical presence in Australia, but which supply goods to Australia and make representations as to those goods<sup>864</sup> into Australia, is "carrying on a business" and "engaging in conduct" subject to the ACL [see **4.2** below].

**'goods'** are defined in section 2 to include "computer software" (e.g. apps) and "any component part of, or accessory to, goods" (g). It also comprehends tangible "things" such as smart cars, home and fitness devices. The distinction is most relevant in considering which consumer guarantees apply (**4.4** below);

**'consumer'** was discussed in **chapter 1** but for ease of reference, includes where the amount payable for goods is \$40,000 or less; or the goods are of a kind ordinarily acquired for personal domestic or household use or consumption, subject to certain exceptions. The recent ACL Review has recommended the threshold be increased to \$100,000 which seems sensible given it has not been raised for many years.

#### 4.1.2 *Choice of law and jurisdiction*

International CIOT device and app providers commonly rely upon contracts with an overseas choice of law reflective of their own location, preferred jurisdiction or to deter international litigants – unless a consumer's usual place of residence is the mandated law, as in the EU.<sup>865</sup> ACL section 67 (a) provides that if the 'proper law' of a contract for goods or services to a consumer is Australian, it shall apply

---

<sup>862</sup> *Given v Pryor* (1978) 39 FLR 437 at 440-441

<sup>863</sup> *Australian Competition and Consumer Commission v Valve Corporation* (No. 3) [2016] FCA 196 per Edelman, J 24 Mar 2016 accessed at <<http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2016/2016fca0196>>

<sup>864</sup> Note the case concerned Valve's representations as to its warranties, refund rights (etc.) and so the question as to whether or not goods were "supplied" into Australia was not relevant. However, the court found that even if Valve did not engage in "conduct" in Australia, it engaged in trade or commerce in Australia, and so was subject to the ACL - it liaised with 2.2 million customers in Australia; had servers for which it paid in Australia; earned significant ongoing revenue from Australians; stored consumer data in Australia; had significant personal property in Australia; relied on third party content delivery providers in Australia who provide services and content around the world including Australia.

<sup>865</sup> To the extent that the protections under the selected law do not derogate from the protections of the laws of their home jurisdiction, consumers are permitted to select the applicable law of a contract: Council Regulation 593/2008 on the Law Applicable to Contractual Obligations (Rome I) cited in James J. Healy, 'Consumer Protection Choice Of Law: European Lessons For The United States' *Duke Journal of Comparative and International Law* 19: 535 558.

regardless of any contrary contractual term.<sup>866</sup> and that (b) despite any term purporting to substitute the laws of another country, the non-excludable (section 64) consumer guarantees apply regardless. As to (a), the court must still consider the proper law, based upon the facts of the case, including the parties' location, where the goods or services are provided, where the contract was formed, the location of the goods, as well as the contractual terms. For example, *Valve* held that consumers purchasing an online license to stream games may enforce the ACL against a supplier in a foreign jurisdiction, regardless of any contrary 'proper law' clause in that license,<sup>867</sup> and that the proper law is Australian where a foreign corporation carries on business in Australia and engages in 'conduct' with sufficient Australian context.<sup>868</sup> So while it is not definitive that the ACL applies to all Australian CIOT purchases, most (if not all) Australian-based purchases are covered and the courts seem likely to lean towards finding jurisdiction for Australian consumers dealing with international entities online. Australia is obviously a preferable forum for cost, convenience and enforcement reasons.

As **Schedule 1** suggests, jurisdiction clauses which uniformly favour the CIOT provider are commonplace. Given the possibility that these may infringe section 67 as well as constitute unfair contract terms, an ACL sweep of enforcement activity seems required.

#### 4.1.3 'Free' apps & supplier liability

ACL provisions governing unconscionable conduct or unfair terms<sup>869</sup> have higher thresholds, which raise several contentious legal issues: firstly, whether there is a defined "consumer"<sup>870</sup> and "supply [or acquisition] of goods or services", and secondly, whether the supply of a 'free' CIOT device, or app falls under the ACL. As Ch. 1 suggests, CIOT acquirers are usually 'consumers' as defined,<sup>871</sup> and usually, each of a CIOT device manufacturer/ supplier, app provider, cloud and data analytics providers are

---

<sup>866</sup> See *Laminex (Aust) v Coe Manufacturing Co* [1999] NSWCA 270

<sup>867</sup> *Australian Competition and Consumer Commission v Valve Corporation* (No. 3) [2016] FCA 196 per Edelman, J 24 Mar 2016 accessed at < <http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2016/2016fca0196>>

<sup>868</sup> [178].

9. *Ibid.*, at [179]- [182].

10. *ACCC v Valve*, above n 863 at [178- 182], [205] per Edelman, J.

<sup>869</sup> Note that false representations (section 29) and statutory guarantees (Part 3-2) could also apply in the event of the thresholds being satisfied. These are discussed below as they apply to CIOT.

<sup>870</sup> ACL section 3 defines a 'consumer' by reference to acquiring (1) goods, which in this case would include by "exchange" (section 2); or (2) services by way of acceptance (section 2). Consumer in terms of acquiring 'goods' means (in summary) if and only if the amount paid does not exceed \$40,000 or the goods were of a kind ordinarily acquired for personal, domestic or household use or consumption.

<sup>871</sup> ACL section 3 defines 'consumer' as to both 'goods' and 'services'. In the latter case, the definition provides a person is a 'consumer' if the services do not exceed \$40,000 or are of a kind ordinarily acquired for personal, domestic or household use or consumption. There seems little doubt that the former would apply to an arguably 'free' contract, or even one where information is exchanged for access; but even if not, CIOT devices exceeding \$40,000 are of a kind objectively, ordinarily acquired for 'personal, domestic or household use or consumption': *Carpet Call v Chan* (1987) 55 ASC 55-553.

corporations operating “in trade or commerce”. The second question concerns ‘freemium’ practices; that is, whether ‘free’ CIOT goods are supplied in ‘trade or commerce’. Business models suggest that free devices or apps are provided to consumers as the monetized component is data collation, use and analytics – the latter of which may involve a paid service (or premium version) in any case.<sup>872</sup> Alternatively, all elements may be free – in return for consumer data access, and broad (monetizable) use. In a social media environment, consumers are repeatedly told that data collation and ads support ‘free’ services, but Hoofnagle for example, argues (correctly) that personal information is valuable<sup>873</sup> and tradeable.<sup>874</sup> Economically, it is a unique consumer asset in a transactional cost sense, which on website, device or app (warranty or other) registration, and is exchanged in a bilateral trading relationship online. Behavioural economists argue that consumers are not “rational” as presupposed by traditional economic analysis: they bear transaction costs, are subject to significant information asymmetry<sup>875</sup> and bounded rationality<sup>876</sup> in online contracting, and bear burdens such as targeted marketing, fraud and identity theft, as well as transferred costs (time, effort or money) to reduce privacy impacts.<sup>877</sup> Risks also transfer through widespread data misuse and breach, where personal information is disclosed to or traded with entities which fail to observe information use and privacy preferences.<sup>878</sup> For this reason, it seems likely that freemium devices and apps (in exchange for consumer data) are provided in connection with a business activity, and will still satisfy the ‘trade or commerce’ requirement, such that relevant ACL provisions will apply. An example might be a free fitness device and app provided by a fitness wear company; these collect consumer data, are provided as a marketing tool for the business and collect customer data, which can be bundled with customer lists to improve marketing and customer profiling - and so, should fall within the ACL. Conversely, a free device and app which is completely unrelated to a business and confidentially donated<sup>879</sup> for non-promotional purposes, without any business data collation or use, is less likely to be captured. This is relevant both to regulating paid and “unpaid” CIOT providers,

---

<sup>872</sup> One US decision says that a free (Apple iOS4) software update download is neither. Note however that the case turned on very narrow definitions within the relevant legislation as to what constitutes ‘goods’ or ‘services’ and the fact that a free upgrade did not fall under the relevant sale or lease laws: Woffard, *ibid*.

<sup>873</sup> Hoofnagle, above n 55: 633.

<sup>874</sup> *Ibid*.

<sup>875</sup> *Ibid*.

<sup>876</sup> This means that all decision-makers face three constraints: (1) limited and often unreliable information as to possible alternatives and their consequences; (2) the limited human ability to evaluate and process information; and (3) the limited decision-making time. “...Therefore even individuals who intend to make rational choices are bound to make satisficing (rather than maximizing or optimizing) choices in complex situations. These limits (bounds) on rationality also make it nearly impossible to draw up contracts that cover every contingency” :Business Dictionary.com, ‘Bounded Rationality’ (undated accessed 10 Apr 2015) < <http://www.businessdictionary.com/definition/bounded-rationality.html>>

<sup>877</sup> Hoofnagle above n 55: 625.

<sup>878</sup> Hoofnagle above n 55.

<sup>879</sup> Note ACL s. 5 provides that donations are not ‘supplies’ or ‘acquisitions’ unless for “promotional purposes” except for Parts 3-3, 3-4, 4-3 and 4-4 as to product safety, recall (etcetera) where they are supplies or acquisitions.

together with the overall supply chain when it comes to products liability, device-related data use, and to the terms under which the CIOT industry deals with consumers generally.

#### 4.2 Parts 2-1 & 3-1: Misleading conduct & false representations

ACL section 18<sup>880</sup> provides that a ‘person’<sup>881</sup> shall not in trade or commerce<sup>882</sup> engage in conduct which is misleading or deceptive or which is likely to mislead or deceive’. To this norm of conduct is added the narrower section 29, which is narrower than section 18, but invokes the same elements as to representations made “in trade or commerce” which are “misleading”.<sup>883</sup> Those representations must be “in connection with the supply or possible supply of goods or services or their “promotion by any means of the supply or use” and must fall within any of the specific scenarios described in subsections (a) – (n),<sup>884</sup> which (broadly) relate to product-related quality, ‘sponsorship approval performance characteristics, accessories, uses or benefits’, testimonials, repair, place of origin, need, guarantees or paid warranties. These representations are usually made in product marketing or informational materials or websites, and as ‘false or misleading’ is synonymous,<sup>885</sup> sections 18 and 29 are often pleaded in concert. Misleading or deceptive or false means that the conduct (including representations) involves a real or not remote chance of leading a consumer into error,<sup>886</sup> as a question of fact<sup>887</sup> - irrespective of

---

<sup>880</sup> The ACL is found in the *Competition and Consumer Act 2010* (Cth) (CCA) Schedule 2. Note that it is a national law, and as state fair trading and related legislation mirror the national provisions, it is not dealt with separately here.

<sup>881</sup> CIOT device-suppliers and app providers are usually corporations which are ‘persons’ under the ACL and are usually regarded as ‘carrying on business within Australia’, either through business with an Australian consumer online or through physical presence (for example, by representative offices or data centres). Note that as a Commonwealth law, the ACL applies to any trading or financial corporation formed within Australia or incorporated within a territory of Australia, or a foreign corporation (or a holding company of any of these): *Competition and Consumer Act 2010* (Cth) sections 4 and 13(1).

<sup>882</sup> ACL section 2 provides that ‘*In trade or commerce*’ means within Australia or between Australia and any place(s) outside, and includes ‘any business or professional activity (whether or not carried on for profit)’.

<sup>883</sup> Courts have confirmed that this phrase has the same meaning as “misleading and deceptive”:

<sup>884</sup> The most CIOT-relevant of these are: as to false representations made in connection with the supply, acquisition or promotion of goods or services, and which prohibits false or misleading representations, inter alia, (a) that goods are of a particular standard, quality, value, grade, composition, style or model... (b) or that services are of a particular standard, quality, value or grade; or (g) have a sponsorship, approval, performance characteristics, accessories, uses or benefits; or (i) as to price; or (l) the need for any goods or services; or (m) concerning existence, exclusion or effect of any condition, warranty, guarantee, right or remedy; or (n) concerning a requirement to pay for a contractual right (including statutory guarantee or other legal right).

<sup>885</sup> See *ACCC v Coles Supermarkets Australia Pty Ltd* [2014] FCA 634; *Comite Interprofessionnel du Vin de Champagne v Powell* [2015] FCA 1110 (per Beach, J). The main difference is that contravention carries criminal penalties unlike section 18.

<sup>886</sup> *ACCC v TPG Internet Pty Limited* [2013] HCA 54; (2013) 250 CLR640; 88 ALJR 176; *Parkdale Custom Built Furniture Pty Ltd v Puxu Pty Ltd* [1982] HCA 44.

<sup>887</sup> *Campomar Sociedad Limitada v Nike international Ltd* (2000) 202 CLR 45; [2000] HCA 12; *Google Inc. v ACCC* (2013) 249 CLR 435; [2013] HCA 1. The court must decide two issues: whether the pleaded representations were conveyed by the conduct in question; and if yes, whether the representations were misleading and deceptive, likely to mislead or deceive or were false or misleading. Where conduct is directed to the public at large (for example, advertising) rather than to specific individuals (for example, purchasers of the device), then the court will assess the conduct by reference to the class or classes to whom the conduct was directed.

whether this has occurred or not.<sup>888</sup> In a CIOT context, this means that terms may mislead whether or not a consumer has read them, which is significant given findings as to low read-rates. Examples might include app terms and conditions which are inaccurate as to the nature or extent of data gathering, its storage or use, or which misrepresent how the ACL applies to those terms and conditions. Others might include false representations as to device operation, security levels or activities, or a smart self app which (covertly) provides that consumer's data to his or her health insurance provider.<sup>889</sup> As is evident, sections 18 and 29, and unfair terms laws may overlap.

The ACCC has not instituted any CIOT-related proceeding under sections 18 or 29.<sup>890</sup> Given the likelihood that large corporations are involved, many consumers are or will be affected and the potentials for industry educative benefits and significant penalties,<sup>891</sup> the ACCC might well consider action early in the Australian CIOT market to establish an aggressive regulatory foothold.

#### 4.2.1 *Smart cases*

Selected international CIOT cases are considered next. Device (in)accuracy and testing, data collection, product performance and related misrepresentations are common in CIOT cases. Recent examples across smart self, home and car include:

---

<sup>888</sup> *Taco Co of Australia Inc. v Taco Bell Pty Ltd* (1982) 42 ALP 177; [1982] FCA 170 [199]. Section 18 refers to conduct which is "likely to mislead or deceive" which has long been viewed as meaning that it is not necessary to prove that the conduct misled or deceived anyone: *Parkdale*; above 886. In *Valve*, the ACCC has cross-appealed arguing that Justice Edelman erred in ruling that certain of Valve's online chats to individual consumers were not misleading, in part because by correctly asserted their ACL rights to Valve, the consumers were not 'misled'.

<sup>889</sup> An example might be a fitness app which collects data, and assigns consumers to an achievement level based upon their fitness 'level'. Knowledge as to the consumer's 'level' rating may convey inferable information.

<sup>890</sup> Note the VW/ Audi cases exemplify alleged software which functions as a defeat device, without consumer knowledge, falsifying green marketing claims and in breach of Australian emissions Standards. Many of these vehicles are level 2 smart cars. Cases are emerging as to other marques in 2016-7.

<sup>891</sup> Remedies are extensive, including injunctions, damages and ancillary orders under ACL Chapter V. The ACCC may also seek fines of up to \$1.1 million for corporations and \$220,000 for individuals. Note that the CCA uses the term 'pecuniary penalties' to avoid the criminal standard of proof.

(a) *Data inaccuracy & testing deceits (smart self)*

In *FTC v Breathometer*,<sup>892</sup> the FTC<sup>893</sup> alleged false claims as to device accuracy and testing<sup>894</sup> of a low-reading blood alcohol concentration detection device, which by app,<sup>895</sup> provided 'safe'-driving recommendations.<sup>896</sup> The case also alleged an unreasonable delay in warning consumers,<sup>897</sup> and disabling the app. The settlement required a recall, \$5.1 million buy-back, and an injunction. In Australia, ACL sections 18 and 29 (a) and (g), as to false device accuracy would apply, as well as a breach of Australian Standard AS3547 under ACL section 136. It may also have a 'safety-related' defect under Part 3-4 requiring recall if it led legally 'intoxicated' people to drive, and were anyone killed, injured or property damaged, Part 3-5 may allow redress. A subtler case concerns underperforming consumer expectation. Two ongoing Fitbit class actions illustrate this: *McLellan*<sup>898</sup> as to heart rate accuracy and *Brickman*,<sup>899</sup> as to sleep measurement. *McLellan* alleges that the heart rate monitoring systems on the Fitbit Charge HR

---

<sup>892</sup> *Federal Trade Commission v. Breathometer, Inc.*, and Charles Michael Yim, FTC Matter/File Number: 162 3057, Federal Court: Northern District of California, Case No. 3:17-cv-314-LB, Stipulated Final Order for Permanent Injunction and Other Equitable Relief, Filed 23 Jan 2017 < [https://www.ftc.gov/system/files/documents/cases/170123breathometer\\_dkt\\_4-1-\\_stipulated\\_order.pdf](https://www.ftc.gov/system/files/documents/cases/170123breathometer_dkt_4-1-_stipulated_order.pdf)>

<sup>893</sup> Section 5(a) of the FTC Act, 15 U.S.C. §45(a) prohibits unfair or deceptive acts or unfair practices in or affecting commerce. Misrepresentations or the deceptive omission of material facts are included within that definition. Acts or practices are unfair if the cause or are likely to cause "substantial injury to consumers" that they cannot reasonably avoid and that is not outweighed by countervailing benefits to consumers or competition.

<sup>894</sup> The FTC alleged the company falsely claimed it had "rigorous government lab-grade tests" verifying its claims.

<sup>895</sup> The complaint was filed under s. 13(b) of the *Federal Trade Commission Act*, 15 U.S.C. § 53(b) alleging violation of section 5(a) of the FTC Act, 15. U.S.C. §45(a).

<sup>896</sup> These included calling a cab if required.

<sup>897</sup> The case alleged Breathometer became aware that its v2 app was yielding low readings by late 2014, upgraded it to elevate readings, but by early 2015, testing revealed flaws resulting in potentially thousands of consumers being misled as to their reading. Despite this, Breathometer traded for another year and consumers were still buying the device in February 2016, the company also failed to notify or warn retailers and failure to email registered owners a month later – and did not disable the feature until May 2016: *Ibid*.

<sup>898</sup> *McLellan et al., v Fitbit, Inc.*, Case No. 3:16-cv-00036, Calif Nthern Dist (5 Jan 2016). The case concerns the Fitbit Charge HR, a wireless heart rate and activity wristband, and Fitbit Surge fitness watch that consists of a GPS watch, heart rate tracker, activity tracker, and smartwatch. The products are sold through retailers and distributors.

<sup>899</sup> The case, involving Californian and Floridian plaintiffs, survived an application to dismiss in 15 July 2016 based upon the technology accuracy, as Brookman, J said the consumer issues relate to product representations, not just the disputed research. The plaintiffs claim they paid US\$30 more for the function. *Brickman v Fitbit Inc.*, Class Action Case No. 3:15-cv-2077

<[https://www.manatt.com/uploadedFiles/Content/4\\_News\\_and\\_Events/Newsletters/AdvertisingLaw@manatt/BrickmanvFitbitInc.pdf](https://www.manatt.com/uploadedFiles/Content/4_News_and_Events/Newsletters/AdvertisingLaw@manatt/BrickmanvFitbitInc.pdf)>

and Surge dangerously under-record rates,<sup>900</sup> posing serious user health risks.<sup>901</sup> The claims include<sup>902</sup> unfair, deceptive and fraudulent advertising, and intentional concealment of material facts. Recent CHOICE research confirmed fitness devices lack accuracy<sup>903</sup> - with Fitbit at a positive 95%,<sup>904</sup> the expert still suggests it will “diminish” workout results.<sup>905</sup> *Brickman* alleges device accelerometer technology overstates sleep by 43- 67 minutes, thereby posing serious long-term health concerns.<sup>906</sup> Both cases also allege unconscionable ‘post’ contractual app terms including mandatory arbitration,<sup>907</sup> choice of law, a class action ban and claims period limitation, which are unfair and fraudulent trading acts and practices. The Australian unfair terms regime, (or less likely) unconscionability may address this, though there is no ‘unfair trading provision. Both cases continue at pre-trial stage – meanwhile, a shareholder class action commenced, alleging Fitbit’s stock fell 5.8% “as a result of the [McLellan] news”.<sup>908</sup>

It is perhaps problematic that these cases require researchers to identify flaws which consumers do not expect, and that consumer redress will depend upon the misleading nature of product marketing and other representations, rather than some concrete standard as to reasonable accuracy or some more

---

<sup>900</sup> The Complaint alleges that Fitbit ‘Purepulse’ uses LED lights to detect changes in capillary volume, then applies “finely tuned algorithms” to measure heart rate automatically and continuously” and allow users to “accurately track workout intensity”:[22].

<sup>901</sup> It alleges that the “PurePulse technology,” is not accurate, as confirmed by its study, nor does it perform as well as Fitbit marketing claims. Fitbit denies the claim and asserts the study is biased and is not precise evidence. The study found that Fitbit’s heart rate accuracy is 20 beats per minute inaccurate (on average) during moderate to high-intensity exercise. Dr. Edward Jo, claims: “This inaccuracy that we’ve seen can definitely pose a danger to not only the clinical population, but those population of individuals who may not know that they have any cardiac related conditions... It can definitely put them at risk.” Fitbit respond that the study was “lacks scientific rigor and is the product of flawed methodology.”: Paul Lamkin, ‘Fitbit heart rate tech ‘puts consumers at risk’ according to lawsuit scientist’, *WAREABLES* (May 2016 accessed 2 Aug 2016) <<https://www.wearable.com/fitbit/fitbit-hrm-heart-rate-tech-health-risk-2764>>

<sup>902</sup> Others alleged include common law fraud, fraud in the inducement, unjust enrichment, revocation of acceptance, breach of express warranty, violation of Magnuson-Moss and other statutes as to implied warranty (and others).

<sup>903</sup> Of 14 tested, only five had an acceptable heart rate margin of error. Sydney University tested 14 fitness tracker heart rate monitor functioning using a 12-lead electrocardiography (ECG) monitor mapping a professional athlete’s real-time heart rate running on a treadmill. One-minute interval readings were taken for five minutes to compare tracker accuracy versus that of the ECG. To compare sudden changes in intensity like those in interval training – researchers took readings at ten-second intervals in the first minute of warming up, and then the sixth minute when cooling down. The ECG monitor readings were compared to the fitness trackers. Dr Edwards asserts that ECG is “the most accurate heart rate monitor, capable of identifying an immediate change in heart rate”: Ibrahim, above n 334.

<sup>904</sup> While some achieved high (95%+) accuracy, others were poor performing: Apple Watch Sport (67%), Samsung Gear S2 (53%) and Sony SmartBand 2 (27%). The high performers included the defendant Fitbit: 99% (Mio) and 95% (Fitbit, Mio Alpha 2 and Garmin Forerunner 235).

<sup>905</sup> Dr Kate Edwards, cited in Ibrahim, above n 334.

<sup>906</sup> Mannatt Phelps and Phillips LLP, ‘Fitbit can’t sleep on false advertising suit over sleep measurement claims’ *Lexology* (29 May 2015 accessed 2 Oct 2016) <<http://www.lexology.com/library/detail.aspx?g=0193042e-7c61-45bc-85c7-54deccb42579>>

<sup>907</sup> There is UK authority to the effect that clauses mandating arbitration may be “unfair”, especially if they seek to limit consumer access to the courts: *Mylcrist Builders Ltd v Mrs G Buck* [2008] EWHC 2172.

<sup>908</sup> Kessler Topaz Meltzer Check LLP, ‘Shareholder Class Action Filed Against Fitbit Inc’ <<https://www.ktmc.com/new-cases/fitbit-inc>> It alleges that Fitbit “... made materially false and/or misleading statements and/or failed to disclose that: (i) Fitbit’s heart rate monitoring technology was inaccurate and did not consistently deliver accurate heart rate readings during exercise; (ii) the inaccuracy of Fitbit’s heart rate monitoring technology posed serious health risks to users of Fitbit’s products; and (iii) as a result of the foregoing, Fitbit’s public statements were materially false and misleading” from IPO to the claim date.

discriminating scale. Consumer and product reviews may assist, but this may be an area appropriate either for ACCC guidance or industry standards to better clarify or disclose device accuracy, and so better align product performance with consumer expectation and industry communications.

(b) *Data gathering deceits (smart self and home)*

The We-Vibe case<sup>909</sup> discussed in **Ch. 5** involves an app collecting sensitive ‘personal’ and device data without disclosing this to users: section 18 can still apply where a non- inadvertent<sup>910</sup> omission is misleading, but section 29 requires an oral, written or implied representation,<sup>911</sup> (which may occur without intent<sup>912</sup>) through an overall impression conveyed by (for example) device marketing. Three recent app cases impugn device accuracy and representations: the Runtastic heart rate monitor was allegedly inaccurate and had not been fully tested to medical device standard so required a clear consumer disclaimer upon first use to that effect, as well as opt-in for tracking and other undisclosed data use practices;<sup>913</sup> Cardio Heart-rate monitor likewise made accuracy (mis)representations and clarification that a “potential life expectancy” feature<sup>914</sup> was hypothetical only. Both required device accuracy and performance warnings, as did the “Baby Heart Monitor” app which conveyed a false “medical-grade” impression.<sup>915</sup> These cases are likely caught by sections 18 and 29(1)(a) as to false representations concerning “standard, quality... grade” or (g) as to “performance characteristics, uses or benefits”.

As to ‘default’ deception, *FTC v VIZIO Inc.*<sup>916</sup> has just paid USD\$2.2 million<sup>917</sup> to settle charges that it installed smart TV software which covertly collected viewing data<sup>918</sup> from 11 million TVs without

---

<sup>909</sup> *N.P. & Ors v Standard Innovation (US) Corp dba We-Vibe*, Case No 1:16-cv-8655, United States District Court of Illinois (Filed 2 Sept 2016) <<https://www.cnet.com/news/internet-connected-vibrator-we-vibe-lawsuit-privacy-data/>>

<sup>910</sup> Inadvertent omissions are not sufficient.

<sup>911</sup> A “representation is an oral or written or implied statement from words or conduct, representing a matter of fact: Given v Pryor (1979) 39 FLR 437 It is an open question as to whether mere breaches of contract – such as a failure to comply with security representations or other terms - constitute a “representation”:

<sup>912</sup> *Attorney General of the State of New York, In the Matter of Runtastic GmbH*, Assurance No.: 16-174, Assurance of Discontinuance under executive Law Section 63, Subdivision 15 (23 Jan 2017) <[https://ag.ny.gov/sites/default/files/runtastic\\_aod\\_executed\\_0.pdf](https://ag.ny.gov/sites/default/files/runtastic_aod_executed_0.pdf)>

<sup>913</sup> *Attorney General of the State of New York, In the Matter of Cardio, Inc.*, Assurance No.: 16-173, Assurance of Discontinuance under Executive Law Section 63, Subdivision 15 (23 Jan 2017) <[https://ag.ny.gov/sites/default/files/cardio\\_aod\\_executed.pdf](https://ag.ny.gov/sites/default/files/cardio_aod_executed.pdf)>

<sup>914</sup> *Attorney General of the State of New York, In the Matter of Matis Ltd*, Assurance No.: 16-101, Assurance of Discontinuance under executive Law Section 63, Subdivision 15 (13 Feb 2017) <[https://ag.ny.gov/sites/default/files/matis\\_aod\\_executed.pdf](https://ag.ny.gov/sites/default/files/matis_aod_executed.pdf)>

<sup>915</sup> *Ibid.*

<sup>916</sup> *Federal Trade Commission, et al v. VIZIO INC. and VIZIO Inscap Services, LLC*, Case 2:17-cv-00758, Filed 6 Feb 2017 <<https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc>>

<sup>917</sup> The payment comprises \$1.5M to the FTC and \$1M to the New Jersey Consumer Affairs (with \$300,000 of that amount ‘suspended’: *FTC & Ors v. VIZIO & Ors, ‘Permanent Injunction and Monetary Judgment’* <[https://www.ftc.gov/system/files/documents/cases/170206\\_vizio\\_stipulated\\_proposed\\_order.pdf](https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf)>

<sup>918</sup> The FTC allege this included consume viewing date, time, channel, live/ recorded status.

consumer consent. This occurred via an on-by-default ‘Smart interactivity’ feature,<sup>919</sup> which it represented provided program suggestions only, but which collected viewer data. VIZIO then attached consumer age, sex, income, education level, marital status, household size, home ownership and household value, connected to the consumer’s IP address, and sold the data. While a prima facie privacy breach, section 18<sup>920</sup> also applies to deceit by omission, and depending upon appropriate facts, sections 29(1)(a) and (g). Even had privacy consents been obtained through terms (for example, through an opt out) it is still possible that an ACL breach might be found if the method or disclosure mode was misleading. An analogous claim against Bose alleges that all music and audio files<sup>921</sup> on their app-controlled<sup>922</sup> wireless devices<sup>923</sup> and personal registration data,<sup>924</sup> is shared “along with other personal identifiers to third-parties—including a data miner—without its customers’ knowledge or consent”.<sup>925</sup> The claim alleges music selection is “sensitive”: revelatory of politics, religious views, thoughts, sentiments and emotions”.<sup>926</sup> Bose denies liability, but has changed to an ‘opt out’ of data collection, de-identified data collected and updated its privacy policy.<sup>927</sup>

---

<sup>919</sup> This feature enabled program “offers and suggestions”.

<sup>920</sup> Competition and Consumer Act 2010 (Cth) section 4(2) defines ‘engaging in conduct’ to mean ‘doing or refusing to do any act’ and section 4(2)(c) states that ‘refusing to do an act’, must be intentional, that is, done other than inadvertently: *ACCC v Homeopathy Plus! Australia Pty Ltd* [2014] FCA 1512

<sup>921</sup> These included music, radio broadcasts and Podcasts, and lecture choices. The case argues these “provide an incredible amount of insight into his or her personality, behavior, political views, and personal identity. In fact, numerous scientific studies show that musical preferences reflect explicit characteristics such as age, personality, and values, and can likely even be used to identify people with autism spectrum conditions”: DM Greenberg, S Baron-Cohen, DJ Stillwell, M Kosinski and PJ Rentfrow, ‘Musical Preferences are Linked to Cognitive Styles’ (2015) *PLoS ONE* 10(7): e0131151. <<https://doi.org/10.1371/journal.pone.0131151>>

<sup>922</sup> The Complaint states the Bose Connect app “allows customers to “pair” (connect) their Bose Wireless Products to their smartphones using a Bluetooth connection, and access essential product functionality. Specifically, through the Bose Connect app, customers can (i) download and install firmware updates to the Bose Wireless Products, (ii) manage the connections between the Bose Wireless Products and mobile devices, (iii) adjust the Bose Wireless Products’ noise cancellation settings, (iv) customize the Bose Wireless Products’ “Auto-Off” settings (for purposes of conserving the product’s battery life), and (v) share music between two Bose Wireless Products.”

<sup>923</sup> The case pleads the following: “QuietComfort 35, SoundSport Wireless, Sound Sport Pulse Wireless, QuietControl 30, SoundLink Around-Ear Wireless Headphones II, and SoundLink Color II”.

<sup>924</sup> Name, email address, phone number and device serial number.

<sup>925</sup> *Kyle Zak et al v. Bose Corp.* Case No. 17-cv-2928 (Filed 18 Apr 2017) Northern District of Illinois, Case: 1:17-cv-02928 (Filed: 18 Apr 2017) <<https://assets.documentcloud.org/documents/3673948/Zak-v-Bose.pdf>>. The causes of action include the US Wiretap Act which generally prohibits the intentional “interception” of “wire, oral or electronic communications.” 18 U.S.C. § 2511(1)(a), and their intentional disclosure: 18 U.S.C. § 2511(1)(c) and Illinois Eavesdropping and Consumer Fraud and Deceptive Business practice statutes, intrusion upon seclusion, and unjust enrichment. See also Peter S. Vogel, ‘IoT Privacy Lawsuit- Bose sued for taking headphone data without consent!’, *Gardere Blog* (25 Apr 2017 accessed 26 Apr 2017)

<<http://www.lexology.com/library/detail.aspx?g=19ce5f62-b7ac-4ba6-83b4-82658f1efddd>>

<sup>926</sup> Complaint above 925: [24]

<sup>927</sup> Bose Australia, ‘A message to our Bose Connect App customers’ (20, 23 and 25 Apr 2016) <[https://www.bose.com.au/en\\_au/landing\\_pages/bose\\_corporation\\_updates.html](https://www.bose.com.au/en_au/landing_pages/bose_corporation_updates.html)>

These cases may imply a trend involving firstly, CIOT device devices/ software or updates which record and transfer consumer data without disclosure, or by default<sup>928</sup> or at best, allow settings-based consumer opt-out; and secondly, linked third party data handling practices, for which most manufacturers deny liability and direct consumers to read additional terms governing the device/ app use. As to the first scenario, collating data without disclosure is an ACL issue which is likely to infringe sections 18 and 29(g) performance characteristics, and possibly 29 (l) need, though creative approaches may muddy the waters, and whether certain forms of disclosure (once in off or online or in manual only forms, for example) will suffice. Collating data by default is also possibly misleading, if the default is not clearly disclosed to and consented to by consumers, especially where no prompt to check or change settings occurs. Settings with automatic opt-ins are more problematic; the NZ Commerce Commission obtained court-enforceable undertakings to prevent Jetstar misleading consumers as to price “or the nature of kind of services” provided in online or in-app airfare purchasing.<sup>929</sup> While there is no precedent as to data collection or contexts beyond an online sale, in principle, it is likely that regulators will expand the ambit, as the consumer harm of ongoing data collection is significant and long-lasting - albeit less price-related. Best practice suggests mandating a separate, informed opt in approach<sup>930</sup> for each type of data collected and each intended use, to facilitate consumer consent.<sup>931</sup> Given the scope of the problem, it would seem sensible for the ACCC to recommend it by guideline, with the Privacy Commissioner. The second ‘trend’ is third party sharing, which is not necessarily an ACL deficiency, but requires consistency. If data collectors share data, they are best placed to ensure that their business partner/ recipient maintains at least equivalent standards with respect to data use and privacy. This chain of responsibility approach influences APP 8 (Ch 5). Examples of such practices evidence emerging large-scale consumer

---

<sup>928</sup> Updates may be especially pernicious if they reset consumer preferences requiring another opt out or settings change.

<sup>929</sup> Jetstar Airways Pty Limited, ‘Undertakings to the Commerce Commission under s46A of the Fair Trading Act 1986 (NZ)’ (16 Mar 2016 accessed 5 Dec 2016) <<http://www.comcom.govt.nz/fair-trading/enforcement-response-register/detail/928>> The Commission alleged that the practice was misleading based upon equivalent provisions to ss 18, 29(i) as to price, and specific misrepresentations (equivalent to s 33) for conduct liable to mislead as to “kind” of services, and their “nature, characteristics, suitability for a purpose or quantity...”[ss 13 (b) and (g) NZ Fair Trading Act 1986]. Examples were prevalent across all budget airlines in Australia and included pre-checked boxes selecting travel insurance, seat selection, luggage fees and charity donations: Tilly South and Brent Savage, ‘Ticked off with sneaky costs’ *CHOICE* (2 Dec 2016 accessed 5 Dec 2016) <<https://www.choice.com.au/travel/on-holidays/airlines/articles/preselected-extras-increase-airfare-costs>>

<sup>930</sup> See the GDPR Arts 7 and 9. The ACCC has recently conducted cases against airline “drip-pricing”, a practice where upfront prices are added to as consumers purchase their seat, luggage, insurance etc – meaning that the initial price is artificially low: ACCC v Jetstar Airways Pty Ltd [2015] FCA 1263 Jetstar was fined \$545,000 for two offences and Virgin Australia \$200,000 – the former are protesting the differential which relates to them employing the practice via multiple fora (website and mobile) and Virgin mobile only, plus Virgin received a discount for cooperating at the penalty (not liability) stage;; *Australian Competition and Consumer Commission v Jetstar Airways Pty Limited* (No 2) [2017] FCA 205 and *Australian Competition and Consumer Commission v Virgin Australia Airlines Pty Ltd* (No 2) [2017] FCA 204. A more pernicious practice is the habit of pre-checked boxes purchasing insurance (requiring consumer opt-out):

<sup>931</sup> Where data collected is sensitive personal information, express consent is required unless it may be implied: see Ch 5.

detriment: the exploitation of information asymmetry and deceptive practices, to automate consumer data collection without consent or disclosure.

(c) *Product performance deceits (smart car)*

The infamous VW emissions-cheating defeat-device ‘conspiracy’ illustrates how 11 million consumers suffered detriment from ‘latent’ software which rendered marketing representations false and misleading. The \$16 billion US settlement;<sup>932</sup> precedes ongoing criminal trials,<sup>933</sup> international (including shareholder suits,<sup>934</sup> and multiplying regulator fines internationally.<sup>935</sup> VW argue that there is no “defeat device” in Australia,<sup>936</sup> and in Europe, have used limitations statutes to reject consumer claims, while regulators search their offices.<sup>937</sup> International actions proliferate,<sup>938</sup> and the ACCC have served proceedings

---

<sup>932</sup> The settlement terms include a buy back, lease termination or retrofit fix (at consumer option) and all consumers will receive compensation of between US\$5100- 10,000 each. It affects some 482,000 diesel vehicles sold between 2009-2015. The total payout includes up to \$18 billion to cover legal claims but excludes any civil or criminal penalties levied by Justice Dept. It stipulates that 85% of affected 2 litre vehicles must be off road or rectified by June 2019. There is also a \$2.7 environmental remediation fund and another \$2 billion for zero emissions vehicle technology. VW has set aside over \$18B to cover the settlement: *In re Volkswagen “Clean Diesel” Marketing, Sales Practices, and Products Liability Litigation, Case No. 3:15-md-2672 (N.D. Cal.)*. See also William Boston, ‘Emissions Cases Against VW Heating Up Around the Globe’ *Morningstar Dow Jones* (23 Aug 2016 accessed 10 Sept 2016)

<<http://www.news.com.au/technology/innovation/motoring/volkswagen-back-in-federal-court-over-diesel-emissions-scandal/news-story/d6b4f88cb2502c896e715cc7a6daf0b9>>;

<sup>933</sup> In Michigan, Volkswagen AG formally pled guilty to three felony criminal charges, conspiracy to commit fraud, entry of goods by false statement and obstruction of justice. In a settlement with the Dept of Justice (DOJ), it has agreed to pay \$4.3 billion (\$2.8B criminal fine and 1.5 B civil fine) in penalties: *U.S. v. Volkswagen, 16-CR-20394, Volkswagen Diesel Engine Vehicle Matters, Case No. 2:16-cr-20394-SFC-APP (E.D. Mich.)* <<https://www.justice.gov/usao-edmi/us-v-volkswagen-16-cr-20394>> The DOJ has also indicted six VW executives and employees, alleging they knew of the fraud and conspired to mislead federal regulators and consumers as to diesel emissions between 2006- 2016. In September 2016, former engineer James Liang pleaded guilty to charges he conspired to defraud the government and violate the US Clean Air Act, and VW’s former lead regulatory compliance officer Oliver Schmidt pleaded likewise in January 2017. Both are cooperating with authorities. The US cannot extradite German executives directly: Beth Dalbey, ‘Volkswagen Agrees to \$4.3B Settlement in Emissions Cheating Scandal: Feds’ (11 Jan 2017 accessed 20 Jan 2017) <<http://patch.com/michigan/detroit/vw-group-close-4-3b-settlement-feds-reports>>

<sup>934</sup> Volkswagen AG is defendant to (approx.) 1,400 investor/ shareholder lawsuits claiming about €8.2 billion (AUD\$12.01 billion) in damages, alleging investors were defrauded by the diesel emissions standards cheating scheme. VW shares have fallen 11% in 2016: Karin Matussek, ‘VW Sued for Record \$9.2 Billion in German Investor Lawsuits’ *Bloomberg Markets* (22 Sept 2016 accessed 23 Sept 2016) <http://www.bloomberg.com/news/articles/2016-09-21/vw-investors-sue-for-8-2-billion-euros-in-germany-over-diesel>> In Sept 2016, VW also settled US\$1.2 billion with 650 franchisee dealers who claimed businesses losses arising from the scandal.

<sup>935</sup> In December 2016, the South Korean fair trade agency fined VW’s Korean company US\$32 million for false emissions advertising and will file five criminal complaints against current or former company executives.

<sup>936</sup> Foster, J is hearing the open class action in the NSW Federal Court: *Richard Cantor v Audi Australia Pty Ltd & NSD1308/2015 – Josephina Tolentino v Volkswagen Group Australia Pty Ltd*; NSD1459/ 2015 – *Alister Dalton & Anor v Volkswagen AG & Anor* [matter relates to NSD1307 & 1308/15 above]

<sup>937</sup> Boston, above n 932.

<sup>938</sup> There are currently class action suits and regulatory investigations in “Australia, Brazil, Canada, Germany, Ireland, Italy, the Netherlands and Spain”: Boston, above n 932.

against VW<sup>939</sup> and Audi.<sup>940</sup> That case pleads breaches of sections 18 and 29(1)(a) and (g), and seeks declarations,<sup>941</sup> pecuniary penalties,<sup>942</sup> corrective advertising<sup>943</sup> and sealed findings under section 137F.<sup>944</sup> There are also Australian class actions underway,<sup>945</sup> pleading breach of consumer guarantees and diminished vehicle value. While denying liability, VW offers a “simple software solution” as a “best outcome”, but admits: “we ... need to regain trust...”<sup>946</sup> It is probable that the ACL actions will succeed based upon international evidence and findings, which should set a smart car software precedent, as well as found evidence upon which consumer actions may also succeed. Consumers do not understand vehicle software capabilities - as comically illustrated by a driver jailed after car called 911, revealing that she had illegally left an accident scene.<sup>947</sup> However the real legal risk lies not in overt functionality which is explainable, but rather in the VW-like case, or software updates which may quietly alter settings, change preferences and otherwise deceive and disempower consumers.

#### 4.2.2 Penalties & expanding section 29

Having regard to possible legal uncertainties as to its application, and detriments identified, section 29 could be expanded to explicitly prohibit false representations as to ‘goods’ safety, privacy, security or related data collection and use practices.<sup>948</sup> For example, there seems little consistency in a website featuring a celebrity testimonial which contains false privacy or data collection representations being

---

<sup>939</sup> ACCC, ‘ACCC update on VW enforcement investigation’ (1 Oct 2015 accessed 10 Oct 2016) <<https://www.accc.gov.au/media-release/accc-update-on-vw-enforcement-investigation>> The ACCC says defeat devices are specifically prohibited under the Australian Design Rules, which are mandatory safety standards, enforceable under the ACL.

<sup>940</sup> *Australian Competition and Consumer Commission v Audi Aktiengesellschaft & Ors* NSD 322/2017 filed 8 March 2017. The case alleges that VW manufactured the vehicles using defeat software which “designed to reduce NOx emissions produced by the Vehicles during testing to below the limits specified in the Standards.” [para 7] The case is pleaded under ACL sections 18(1), 29(1)(a) and (g) and s 33 (suitability for purpose) and s 106 (failure to comply with an Australian Safety Standard – then ADR 79).

<sup>941</sup> Section 21 Federal Court of Australia Act 1976 (Cth).

<sup>942</sup> ACL section 224.

<sup>943</sup> ACL section 246.

<sup>944</sup> CCA section 137H allows sealed reasons for judgement to be retained on the court file for possible use in later proceedings under section 83 as prima facie evidence of those facts, by any person seeking damages or compensation orders.

<sup>945</sup> Maurice Blackburn and Bannister law have a class action suit under way in NSW: <https://www.mauriceblackburn.com.au/current-class-actions/volkswagen-class-action/>> There are seven potential actions in the UK and 30 launched in the US, according to Bannister Law.

<sup>946</sup> Joshua Dowling, (5 Jul 2016 accessed 2 Sept 2016) <<http://www.news.com.au/technology/innovation/motoring/volkswagen-back-in-federal-court-over-diesel-emissions-scandal/news-story/d6b4f88cb2502c896e715cc7a6daf0b9>>

<sup>947</sup> Shirleen Allicott, ‘Car auto-dials 911 to report accident after driver allegedly commits hit-and-run’ *ABC News* (4 Dec 2015 accessed 25 Apr 2016) <<http://abc7chicago.com/technology/car-auto-dials-911-to-report-accident-after-driver-allegedly-commits-hit-and-run/1109554/>>

<sup>948</sup> Baker, above n 776; Allens suggest section 18 is too unclear to attract criminal penalties relying upon it as a norm of conduct. The latter recommends expanding section 29 to catch specific misconduct.

unequivocally actionable under section 29(e), when those same representations minus the celebrity, may fail the requirements within s29 (a) as to ‘quality, value, grade [etc.]...’ or section 29(g) if not “benefits’. Obviously, the facts are critical, and existing inclusions often overlap, but false representations in these areas are often egregious, affect many consumers, and given low data protection enforcement generally, a specific ACL provision is justified to incentivize better corporate conduct and to redress consumer harm. Finally, while s. 18 is the most used of all ACL provisions, the inconsistent penalties regime presents an illogical regulatory gap. Section 18 penalties are limited to civil sanctions<sup>949</sup> whereas section 29 attracts criminal penalties.<sup>950</sup> these should be harmonised to improve consumer redress under section 18 and overcome gaps between sections 18 and 29 in this regard.<sup>951</sup>

### 4.3 Part 2-2 Unconscionable conduct & unfair trading

Unconscionable conduct is prohibited under ACL section 21 in relation to goods or services, or where inapplicable, by statutory incorporation of equitable unconscionability. This latter form applies requires a ‘special disability’, which unless implied by device use (for example, a smart home device directed towards persons with an intellectual disability), data collected or a consumer is identifiably under a disability, is difficult to establish in a CIOT (often online) context.<sup>952</sup> In contrast, providing its threshold criteria is met, section 21 might apply to a CIOT scenario.<sup>953</sup> Section 22 sets out a range of non-exclusive criteria:<sup>954</sup> the most relevant include the parties’ relative bargaining strength;<sup>955</sup> whether the CIOT device

---

<sup>949</sup> These include injunctions, damages, compensatory orders, non-party consumer orders and non-punitive orders.

<sup>950</sup> These are \$1.1million for a body corporate and \$22,000 for an individual, plus a range of civil remedies: ACL section 151.

<sup>951</sup> While historically, this proposal appears to ignore the history and purpose of section 18 (formerly s. 52) there is divided legal opinion as to whether those original factors remain compelling when considering ACL reform. ACL Review submissions which adopted this point include those of Minter Ellison, the Consumer Action Law Centre, above n 840 c/f Baker & McKenzie; Allens, Minters and Allens suggest that section 18 would need clarification as to the type of conduct which would rise to the level of seriousness/ culpability to attract criminal penalties, but this departs by definition from its principles-based nature.

<sup>952</sup> ACL section 20 prohibits unconscionable conduct “within the meaning of the unwritten law from time to time” and applies if section 21 does not. It applies to conduct which does not involve the supply or acquisition of goods or services. Note that equitable unconscionability is interpreted by the courts to mean where an innocent party acts under a ‘special disadvantage’, the other party has actual or constructive knowledge of that disadvantage and unfairly or unconscientiously exploits that disadvantage. In these circumstances, the courts have traditionally placed the onus upon the stronger party to show that the transaction was fair, just and reasonable. ‘Special disadvantage’ means a serious disadvantage beyond just an inferior bargaining position or commercial vulnerability and extends beyond mere inequality of bargaining power (such as that which exists between a consumer and an entity such as Google). See *Blomley v Ryan* (1956) 99 CLR 362; *Commercial Bank of Australia v Amadio* (1983) 151 CLR 447.

<sup>953</sup> Section 20(2) provides that equitable unconscionability does not apply to situations under which section 21 applies (i.e. unconscionable conduct in connection with the supply or acquisition of goods and services).

<sup>954</sup> The ACL provides that the court *may* consider the contract terms, the manner in which and the extent to which it was carried out and is “not limited” to considering the contract formation circumstances.

<sup>955</sup> ACL s 22(1) (a). Note that the High Court has stated that inequality of bargaining power alone cannot constitute equitable unconscionability – which may be persuasive as to s. 21 statutory unconscionability: *ACCC v Berbatis* (2003) 214 CLR 51.

or app supplier required the consumer to comply with conditions not reasonably necessary to protect its legitimate interests;<sup>956</sup> whether the consumer was able to understand terms and policies;<sup>957</sup> any undue influence or pressure or unfair tactics exerted,<sup>958</sup> the extent to which the CIOT entity fails to disclose any intended conduct which might affect the consumer's interests or any foreseeable risks not apparent to the consumer;<sup>959</sup> and the extent to which the CIOT entity acted in good faith.<sup>960</sup> In addition, section 22(1)(j) includes the extent to which the CIOT entity was prepared to negotiate the contract, the contract terms and conditions, including any unilateral right of variation<sup>961</sup> the party's conduct in complying with its terms and any post-contractual conduct of either party; all of which may be relevant in a CIOT context.

There is no authority in Australia applying unconscionability to a CIOT sales or contracting context.<sup>962</sup> There are telemarketing cases involving systemically unfair sales pressure and terms,<sup>963</sup> and concerns as to children's rights online,<sup>964</sup> but no online contracting scenario yet. However, the recent confirmation that businesses may be treated unconscionably in *ACCC v Coles*<sup>965</sup> suggests that it remains an "open-ended concept",<sup>966</sup> such that the categories of potential victims are open and even, that procedural unconscionability – for example, a corporation that exploits consumer behavioural economics factors (**Ch 6**) - is a possibility. An argument might be constructed under section 21 whereby multiple contractual factors might establish unconscionability: for example, where contractual terms are (procedurally)<sup>967</sup> difficult to locate or access, are lengthy and complex requiring a high reading age, exhibit 'unfair tactics' in exploiting consumer technical ignorance, or fail to explain CIOT device or app risks not foreseeable to

---

See also the recent *ACCC v Coles Supermarkets Australia Pty Limited* [2014] FCA 1405 in which s. 21 was held to apply to Coles in its business dealings and contracts with its commercial (manufacturer) suppliers, resulting in \$10 million in penalties.

<sup>956</sup> ACL s 22(1) (b).

<sup>957</sup> ACL s 22(1) (c).

<sup>958</sup> ACL s 22(1) (d).

<sup>959</sup> ACL s 22(1) (i).

<sup>960</sup> ACL s 22(1) (l).

<sup>961</sup> ACL s 22(1) (k).

<sup>962</sup> There is authority pertaining to online advertising: *ACCC v Zanok Technologies Pty Ltd* [2009] FCA 1124; *Caspi v Microsoft Network LLC* 323 N.J. Super 118 (NJ Super App Div 1999). Note also that factually, the recent *Australian Competition and Consumer Commission v Coles Supermarkets Australia Pty Limited* [2015] FCA 330 case involved some elements of ongoing online contracting as between small supplier companies and Australia's second largest supermarket chain.

<sup>963</sup> *ACCC v Excite Mobile Pty Ltd* [2013] FCA 1405 c/f *ACCC v EDirect Pty Ltd (in Liq)* [2012] FCA 976

<sup>964</sup> ACMA, above n 827; FTC, 'Mobile apps for kids: Disclosures still not making the grade' Text of the Commission *Staff Report* (2012) <https://www.ftc.gov/reports/mobile-apps-kids-disclosures-still-not-making-grade>

<sup>965</sup> *Australian Competition and Consumer Commission v Coles Supermarkets Australia Pty Ltd* [2014] FCA 1405 (22 December 2014), Federal Court of Australia, 22 December 2014  
<<http://www.austlii.edu.au/au/cases/cth/FCA/2014/1405.html>>

<sup>966</sup> *ACCC v Seal-a-Fridge Pty Ltd* [2010] FCA 525

<sup>967</sup> ACCAN suggests following D. Clapperton and S. Coronas, 'Unfair Terms In 'Clickwrap' And Other Electronic Contracts' (2007) 35 *Australian Business Law Review* 154, that section 21 requires some procedural element in addition to substantive (terms-based for example) evidence of unconscionability. The courts do not seem to have taken that line since the 2007 article was authored.

an average consumer<sup>968</sup> or where the consumer is exploited as a result of a personal vulnerability of which the other party is (through device or otherwise) somehow aware.<sup>969</sup> An interesting scenario might arise where smart self device manufacturer should be aware that a user has a specific vulnerability through (post contractual) device use or by data collected or fused, or related data analytics. Another example might be smart home devices tailored for elderly or intellectually-disabled people seeking independent living, but who may lack capacity pre, or post contractually. Further, it is not inconceivable that sign-up processes entailing long and legalistic online terms and conditions, requiring ill-explained consents to excessive or unnecessary data collection<sup>970</sup> might also be actionable either alone or in concert with unconscionable marketing, contractual terms or conduct, in the right conjunction of circumstances.<sup>971</sup> But such optimistic thoughts should not ignore that establishing unconscionability is difficult, especially via online transactions. Consumer groups claim that it is too legalistic for most consumers, and its high threshold has created “regulator uncertainty”.<sup>972</sup> Where it requires ‘moral obloquy’<sup>973</sup> or conduct “against conscience” by reference to social norms,<sup>974</sup> even the Full Federal Court has complained of the lack of “fixed” elements or rules in the “... agonised search for definition, for distilled epitomes or for short hands of broad social norms and general principles, will lead to disappointment... and to the likelihood of error”.<sup>975</sup> Reflecting this legal uncertainty, the courts have made slim decisions confined to the facts, which leaves consumers “exposed to unfair, predatory business practices”:

---

<sup>968</sup> *ACCC v Keshow* [2005] FCA 558 is analogous as to sales of educational materials to indigenous Australians who it seems, did not understand what was being sold to them or how direct debit authorisations would work.

<sup>969</sup> Note that many apps allow children to provide consent. This does not mean that age could not be used to justify an action in unconscionability, as it is arguable that a 13-year-old may be unable to understand certain terms and conditions which require a higher reading age - and if signed up with an accurate birth date, the supplier is in a position to know their age. Note there is also technology to verify age consent now which few sites seem to use.

<sup>970</sup> Note however, pre-ACL authority held that unconscionability requires some circumstances beyond mere contractual terms that would render reliance upon them unreasonable, unfair, wrong or immoral: *Hurley v McDonald's Australia Ltd* (2000) ATPR 41-741 [31] as discussed in Dan Jerker Svantesson, 'Unconscionability: Consumer Ecommerce' *Commercial Law Quarterly: The Journal of the Commercial Law Association of Australia* 25:1 (Mar/May 2011 accessed 23 May 2014) [11] <<http://search.informit.com.au.ezproxy.bond.edu.au/documentSummary;dn=043279687656685;res=IELHSS>> ISSN: 0819-4262> It is possible that this case would be distinguished given the franchise context – the earlier case of *George T Collings (Aust) Pty Ltd v H F Stevenson (Aust) Pty Ltd* (1991) ATPR 41-104 [52,622 – 3] found that an onerous standard form contract term was unconscionable, and so void.

<sup>971</sup> In *Video-Ezy International Pty Ltd v Sedema Pty Ltd* [2014] NSWSC 143, Harrison AJ found an “accumulation of incidents” relating to an reasonable, unfair and bullying franchise behaviour.

<sup>972</sup> CALC, above n 840 (Submission: 10).

<sup>973</sup> *Attorney General (NSW) v World Best Holdings Ltd* [2005] 63 NSWLR 557 (per Spiegelman, J); *Director of Consumer Affairs (Vic) v Scully (No 3)* [20-13] VSCA 292; *DPN Solutions Pty Ltd v Tridant Pty Ltd* [2014] VSC 511. For equivocal support of moral obloquy, see the High Court's decision in *Kakavas v Crown Melbourne Limited* [2013] 250 CLR 392.

<sup>974</sup> *Ibid.*

<sup>975</sup> *Paciocco v Australian and New Zealand Banking Group Ltd* [20-15] GCAFC 50 at para [304].

*[Section 20-22 is] dependent on the ... facts and circumstances of individual cases. Findings that they have been breached ... rarely set a general rule or precedent... at best [it is] an imperfect tool for a regulator seeking to address systemic or widespread issues.*<sup>976</sup>

Aside from the evidential pressures, CIOT model complexity - with its multiple supply chain – may insulate key actors from liability: for example, where data is shared without contractual privacy requirements or re-identified through fusion, brokers may elude responsibility for uses for which the collector may be liable. Again, this impacts the law’s effectiveness in disrupting systemic issues.<sup>977</sup> A general prohibition against unfair business practices is recommended, which may better address CIOT behaviours, especially with respect to vulnerable persons and children,<sup>978</sup> and as to certain ‘unfair’ data gathering and use practices. While this may entail some duplication, and statutory unconscionability cases may expand its impact, there seems little reason from a consumer policy perspective not to adopt this course, especially as it will address specific deficiencies via a principles-based approach. Fairness is, in principle, an unarguable concept consistent with the Framework, and one otherwise, not wholly addressed. Notably, the ACL Review did not recommend this course but proposes to investigate it further.<sup>979</sup>

ACL remedies for unconscionability are flexible and extensive.<sup>980</sup> It is probable that were any such action to be pleaded, it would appear in conjunction with a claim under the unfair terms regime considered next.<sup>981</sup>

---

<sup>976</sup> ASIC, ‘Senate enquiry into the performance of the Australian Securities and Investment Commission – Submission by ASIC on reforms to the credit industry and ‘low’doc’ loans’, (Oct 2013 accessed 20 Jan 2016) < <http://download.asic.gov.au/media/1311541/ASIC-Submission-on-credit-reform--to-Senate-inquiry.pdf>>

<sup>977</sup> See for example, *Perpetual Trustee Company v Burniston* (No 2) [2012] WASC 383. An example is the finance broking industry where lenders were (originally) not held liable for the acts of brokers- prior to the *National Consumer Credit Protection Act 2009* (Cth).

<sup>978</sup> See case examples such as the Apple and Amazon in-app purchases without parental consent: FTC, ‘Apple Inc.: Analysis of Proposed Consent Order to Aid Public Comment; Proposed Consent Agreement’ Federal Register, 79: 15 (23 Jan 2014) < <https://www.ftc.gov/policy/federal-register-notice/apple-inc-analysis-proposed-consent-order-aid-public-comment>> See also ‘Dissenting Statement of Commissioner Joshua D. Wright’, ‘Concurring Statement of Commissioner Maureen K. Oehlhausen’ and ‘Statement of Chairwoman Edith Ramirez and Commissioner Julie Brill’; and *Federal Trade Commission v Amazon.com Inc.*, Case No C14-1038-JCC, United States District Court, Seattle, ‘Order granting Amazon’s Motion for Partial Summary Judgement and granting the FTC’s motion for Summary Judgment (redacted)’ filed 22 Jul 2016 <https://www.ftc.gov/system/files/documents/cases/160427amazonorder.pdf> per Coughenour, J.

<sup>979</sup> ACL Review, above n 832: 6 [2.3].

<sup>980</sup> Depending upon who institutes the action (a ‘customer’ or the ACCC), remedies include undertakings (s. 218); substantiation notices (s. 219); public warning notices (s. 223); pecuniary penalties (s. 224); injunctions (s. 232); damages (s. 236 subject to CCA s. 137B); compensation or other orders (s. 237); non-punitive orders (s. 246); adverse publicity orders (s. 247); disqualification orders (s. 248) and infringement notices (s. 134A CCA).

<sup>981</sup> In *Paciocco v Australia and New Zealand Banking Group Limited* [2015] FCAFC 50 [363] – [364], Allsop CJ emphasized the evaluative nature of the unfairness assessment, and observed that “unjustness and unfairness are of a lower moral or ethical standard than unconscionability”.

#### 4.4 Part 2-3 Unfair contract terms

...many potentially unfair contract terms are still appearing in standard contracts... - ACCC<sup>982</sup>

ACL unfair contract term provisions render void any unfair term in most<sup>983</sup> 'standard form'<sup>984</sup> 'consumer contracts'<sup>985</sup> made, renewed or varied after 1 July 2010,<sup>986</sup> and "small business contracts"<sup>987</sup> and terms<sup>988</sup> accepted from 12 November 2016 or renewed thereafter.<sup>989</sup> A term is unfair if it:

- would cause a significant imbalance<sup>990</sup> in the parties' rights and obligations under the contract;<sup>991</sup>

---

<sup>982</sup> Quoted in ACCC, 'Unfair contract terms under scrutiny' *Media Release* (28 Mar 2017 accessed 28 Mar 2017) <<http://www.accc.gov.au/media-release/unfair-contract-terms-under-scrutiny>>

<sup>983</sup> Insurance contracts for health, home and cars are excluded: See the *Insurance Contracts Act 1984* (Cth) which regulates car insurance (inter alia). Other exclusions include shipping contracts, company or other body constitutional documents, and those in sectors declared by the Minister (none to date). Note that financial services contracts are regulated by equivalent terms in the Australian Securities and Investments Commission Act 2001 (Cth).

<sup>984</sup> ACL s. 27 imposes a presumption that the contract is standard form, unless the other party proves otherwise – by reference to ss (2) which lists factors the court may take into account in so deciding: (a) whether one party has most of the bargaining power; (b) whether the contract was pre-prepared by one party; (c) whether one party was required to "accept or reject" those terms; (d) whether there was effective opportunity to negotiate the terms; whether the terms take into account the specific characteristics of another party; and (f) any other matter prescribed in the regulations. Clearly this would apply to most consumer CIOT contracting, much if not all of which, occurs online.

<sup>985</sup> 'Consumer contract' means a contract for the supply of goods or services to an individual who subjectively acquires them for personal, domestic or household use or consumption. It has always included an unincorporated sole trader, who for example, who might purchase goods or services for an acquisition which is predominantly for personal, domestic or household use or consumption, even if partly for business purposes: Australian Government Solicitor, 'Australian Consumer Law' Fact Sheet No. 12 (March 2011 accessed 28 June 2014) <[http://www.ags.gov.au/publications/fact-sheets/Fact\\_sheet\\_No\\_12.pdf](http://www.ags.gov.au/publications/fact-sheets/Fact_sheet_No_12.pdf)>

<sup>986</sup> These provisions came in force 6 months earlier than other ACL provisions. As to the Commonwealth, contracts entered into or varied after 1 Jul 2010 are covered, and those varied or renewed apply only to the extent of the renewal or variation: *Trade Practices Amendment (Australian Consumer Law) Act (No 2) Schedule 7, section 8(2)*.

<sup>987</sup> *Treasury Legislation Amendment (Small Business and Unfair Contract Terms) Act 2015* (Cth) No 147, 2015. This provision is an extension of the UK system. Section 23(4) defines a *small business contract* as one where: (a) the contract is for a supply of goods or services, or a sale or grant of an interest in land; and (b) at the time the contract is entered into, at least one party is a "small business" meaning it employs less than twenty people (excluding casuals not employed on a regular or systemic basis) - provided the upfront price payable for the contract is \$300,000 or less, or where the contract exceeds 12 months, one million dollars.

<sup>988</sup> Terms that define 'the main subject matter of the contract', or set 'the upfront price payable' or are 'required, or expressly permitted, by a law of the Commonwealth, a State or a Territory' are excluded by ACL s 26(1). "Upfront price" means consideration disclosed at or before the contract is entered into and is provided, or to be provided, for the supply, sale or grant under the contract. It excludes 'any other consideration that is contingent on the occurrence or non-occurrence of a particular event': ACL section 26(2). UK authority suggests that to preserve the purpose of the legislation, similar exclusions should be interpreted narrowly: *Director General of Fair Trading v First National Bank PLC* [2001] UKHL 52; [2002] 1 AC 481; *Office of Fair Trading v Abbey National Plc* [2010] 1 All ER 667 (per Lord Walker J). Note such terms are excluded in the UK only to the extent they are clearly expressed; the ACL contains no such restriction.

<sup>989</sup> It seeks to protect "time-poor small businesses entering into contracts for day-to-day transactions" whilst retaining small business self-responsibility for higher-value contracts: Commonwealth Parliament, House of Representatives, Treasury Legislation Amendment (Small business and unfair contract terms) Bill 2015, Explanatory memorandum [2.7] <[http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5497\\_ems\\_b35077f3-dbb6-4c5a-81b0-7b885634fd81/upload\\_pdf/503040.pdf;fileType=application%2Fpdf](http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5497_ems_b35077f3-dbb6-4c5a-81b0-7b885634fd81/upload_pdf/503040.pdf;fileType=application%2Fpdf)>; Treasury Legislation Amendment (Small Business and Unfair Contract Terms) Act 2015 (Cth) No 147, 2015.

<sup>990</sup> Finding a 'significant' imbalance is a question of fact. It has been held to mean one quantitatively substantial in Victoria

<sup>991</sup> Note the UK excludes this in favour of a 'good faith' test: regulation 5(1). The European Council Directive 93/13/EEC on Unfair Terms in Consumer Contracts (5 April 1993) is found in the UK Unfair Terms in Consumer Contracts Regulations 1999.

- is (by rebuttable presumption)<sup>992</sup> not reasonably necessary to protect the ‘legitimate interests’ of the advantaged party; and
- would cause financial or other detriment to the other party were it relied upon.

The court must consider the extent of term ‘transparency’<sup>993</sup> (*is it expressed in reasonably plain language, legible and presented clearly, and readily available to any party affected by the term?*) and the whole contract,<sup>994</sup> plus such other factors as it thinks relevant. Terms found to be ‘unfair’ are void and severable,<sup>995</sup> and the contract continues in binding force if capable of operating without the unfair term.<sup>996</sup>

CIoT device, website and app software terms and related (usually incorporated) privacy terms are commonly provider-biased, non-negotiable,<sup>997</sup> standard form consumer contracts within the meaning of the ACL, and are commonly lengthy, viewed (if at all) via multiple locations online and sometimes off, and often after a consumer has purchased a device or during a related smartphone app purchase or download. It is a complicated context, featuring international providers for whom Australia is a minor market, a hybrid legal/ technical environment generating complicated device, software and privacy terms for consumer comprehension, and yet relatively low value products with (in some cases) relatively high risk potentials. CIOT contracting has both substantive and procedural unfairness, much as yet judicially unidentified in Australia.

#### 4.4.1 Identifying ‘unfair’ terms

In 2013, the ACCC selectively reviewed contracts across six industries and found potentially unfair terms in eight key areas: unilateral variation, unfair liability limitation, restrictions upon consumer termination rights, suspension/ cessation of services, consumers liability for things beyond their control, prohibitions upon consumer reliance upon supplier/ agent’s representations, and purported limitation to consumer guarantee rights.<sup>998</sup> That review also found “the use of customer’s personal details for a broad range of

---

<sup>992</sup> ACL s. 24(4) imposes a presumption against the party advantaged by the term.

<sup>993</sup> ACL s.24(3) ‘Transparency’ means a term expressed in reasonably plain language, legible and presented clearly, and readily available to any party affected by the term.

<sup>994</sup> ACL s. 24(2). Section 23 does not apply to any term which defines the ‘subject matter’ of the contract (that is, under s. 26(2), consideration payable disclosed when the contract is entered into, but excludes any consideration contingent upon the happening or non-happening of any particular event) or sets the upfront price payable under it; or is a term expressly required by law.

<sup>995</sup> ACL s. 23(2).

<sup>996</sup> ACL s. 23(2).

<sup>997</sup> Most CIOT notice terms are issued on a take-it-or-leave-it basis which reflects administrative convenience as well as (inequality of) bargaining power. The consumer who wants a smart self device cannot usually call Fitbit to amend data collection terms. They can however, select another device – many of which may be substitutable market-wise – though most if not all, offer the same standard form approach.

<sup>998</sup> ACCC, ‘Unfair contract terms review’ (2013 accessed 2 Feb 2016)

<<https://www.accc.gov.au/system/files/Unfair%20Contract%20Terms%20-%20Industry%20Report.pdf>>

reasons not strictly linked to the supply of services”;<sup>999</sup> suggestive that the ACCC regards terms offending data minimisation principles as potentially unfair. The review also found that contractual complexity and length “hampered transparency and accessibility”.<sup>1000</sup> In 2016, the ACCC reviewed 46 business-to-business contracts used by major firms<sup>1001</sup> across seven industries, with similar findings. The most commonly-occurring ‘problem’ terms exceed reasonable protection of a provider’s legitimate interests: unilateral variation of important or detriment-causing terms; excessively broad indemnities and liability limitation; and finally, unreasonable unilateral termination rights.<sup>1002</sup> The findings reflect those of other regulators.<sup>1003</sup>

#### 4.4.2 Schedule 1: a selective study<sup>1004</sup>

**Schedule 1** as to smart self and home devices supports ACCC findings. It uses the fourteen ACL ‘examples’,<sup>1005</sup> and ACCC analysis,<sup>1006</sup> to review six devices and finds *potentially* unfair terms in all contracts considered.<sup>1007</sup> Two important preliminary points: firstly, the schedule has limitations.<sup>1008</sup> It does

---

<sup>999</sup> Ibid: 16.

<sup>1000</sup> Ibid.

<sup>1001</sup> These included Australia Post, Bakers Delight, Coca-Cola Amatil, Facebook, Fairfax, Google, News Limited, Optus, Scentre Group (owner of Westfield shopping centres), Uber, Vicinity Centres, and Vodafone.

<sup>1002</sup> ACCC, ‘Unfair Terms In Small Business Contracts’ (10 Nov 2016 accessed 10 Nov 2016): 2

[http://acc.gov.au/system/files/B2B%20UCT%20-%20Final%20-%20Unfair%20terms%20in%20small%20business%20contracts%20%20A%20review%20of%20selected%20industries\\_0.PDF](http://acc.gov.au/system/files/B2B%20UCT%20-%20Final%20-%20Unfair%20terms%20in%20small%20business%20contracts%20%20A%20review%20of%20selected%20industries_0.PDF)

> Industry sectors were selected based upon complaints. 46 contracts were reviewed. Businesses participated consensually.

<sup>1003</sup> For example, the UK CMA recently audited the consumer cloud storage industry, finding unfair terms in a wide range of contexts, plus pre-contractual information deficits [1.17]. It also found consumer trust and confidence issues: Competition and Markets Authority, ‘Consumer law compliance review: cloud storage’ *Findings Report* (27 May 2016 accessed 2 Jun 2016) <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/526447/cloud-storage-findings-report.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/526447/cloud-storage-findings-report.pdf)> These included unilateral variation, termination/ suspension, automatic renewal, limitation of liability, jurisdiction and choice of law, as well as transparency of contract terms. As to other sectors, CHOICE has collected case studies from the travel and insurance sectors which it says highlight consumer detriment across the airline, or and campervan hire and travel agent industries.

<sup>1004</sup> **Important Schedule 1 Note: All comments on and placement of the terms is illustrative only and does not mean or imply ACL contravention. Some devices do not have Australian versions or are not yet in the Australian market; in either case, UK terms were used if available, but obviously, these will not address specific ACL requirements. The Schedule is thus for academic and illustrative purposes only.**

<sup>1005</sup> Section 25 ACL.

<sup>1006</sup> See for example, the table in *Ozsale Pty Limited, Undertaking to the ACCC* (27 June 2016 accessed 2 Sept 2016)

<<http://registers.acc.gov.au/content/item.phtml?itemId=1197453&nodeId=3cfd5bc647e386a7aaa760ff17f06e99&fn=Undertaking%20-%20s87B%20-%20Ozsale%20Pty%20Limited%20-%20signed%2027%20July%202016.pdf>>

<sup>1007</sup> Those selected were based upon market positioning which is suggestive of sales volume and consumer use, subject to the important rider that where devices are not in the Australian market yet or no ‘Australian’ terms exist, UK versions are reviewed if available. These are subject to the EU Unfair Contract Terms Directive and related, derivative UK legislation. Several manufacturers did not have those terms accessible online or seemed to exclusively use US versions. These are identified in the schedule. Given the unreliability of this, it is suggested that the findings be viewed as illustrative only and not as evidence of breach on the part of any one CIOT supplier.

<sup>1008</sup> See **above n 1004**. Note also that section 25 examples are just that; as such the analysis ignores other terms which may potentially be unfair but not fit the categories used. For example, one required consumers to “acknowledge they provide

not imply or evidence illegality, as some of the terms used may not be Australian-market specific, so placement in the table and 'comments' are mere illustrations only. As smart car terms are not readily available, the Canadian FIPA's privacy analysis is adapted, but is not sufficiently detailed to tabulate.<sup>1009</sup> Secondly, CIOT device terms may be long, inter-linked and involve multiple document sets.<sup>1010</sup> While Part 2-3 does not respond to general unfairness, nor render entire contracts void,<sup>1011</sup> it seems intuitive that such volume and complexity of form is inherently unfair.<sup>1012</sup> While other ACL provisions may respond in specific contexts, there is no clear legal disincentive to this prevalent online practice.

Given proposals to create a general 'unfairness' approach were rejected by CAANZ as unnecessary, it seems apposite to call upon the ACCC to test sections 21 and 24 in this context in the courts.

Schedule 1 identifies terms which:

- confer unilateral variation rights upon providers, without obligation to provide consumers advance notice or use of low-level website notice which consumers may never see;
- confer unilateral variation, assignment,<sup>1013</sup> termination or suspension rights upon providers, who unilaterally determine (often undefined) consumer breach;<sup>1014</sup>
- fail to compensate consumers if the provider unilaterally varies or terminates the contract, thereby denying or suspending its operation, or if the consumer does not accept new terms imposed;
- disclaim device accuracy and fitness for purpose in a manner which may infringe non-excludable consumer guarantees;<sup>1015</sup>

---

personal information at their own risk", which again, may be unfair especially where providers control security and are best placed to manage data breach detriment. It may also breach privacy legislation or at least, misrepresent its application.

<sup>1009</sup> 'The Connected Car: Who's in the driver's seat? A Privacy Analysis', Annexure to Lawson, above n 36.

<sup>1010</sup> CHOICE recently claimed one of the Alexa suite of consumer device contracts is 73,189 words long and takes 8.59 hours to read: CHOICE, 'Nine hours of 'conditions apply' *Media release* (15 Mar 2017 accessed 15 Mar 2017) <https://www.choice.com.au/about-us/media-releases/2017/march/nine-hours-of-conditions-apply>

<sup>1011</sup> ACL section 243, unless they are unable to continue in operation without identified unfair term(s).

<sup>1012</sup> The ACL Review considered and rejected a general unfairness provision, pointing to the requirement to consider transparency and the contract as a whole plus other ACL provisions, such as section 18 should offer sufficient redress.

<sup>1013</sup> This may impede 'device migration', that is, reconnecting CIOT devices upon moving properties or 'device transfer' to other parties or simply by leaving them in situ when an owner moves: GSMA, 'Competition Policy in the Digital Age: A Practical Handbook' (Oct 2015 accessed 2 Aug 2016) <<http://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/Competition-Policy-Handbook.pdf>>the disparate devices which may inhabit an IoT home, for example, when a consumer moves houses. The US National Association of Realtors and Online Trust Alliance have a specific guide to address this issue and to inform realtors as to advising consumers.

<sup>1014</sup> Note consumers are permitted to cancel their contract at any time but regardless of fault, it is stated or implied that the "remedy" is ceasing to use a device for which they have paid, and may entail detriments such as loss of data, portability and so on.

<sup>1015</sup> eg: ss 54 acceptable quality and s 55 fit for purpose which are non-excludable: s64;

- may mislead consumers as to the ACL application and remedies, including compensation rights;<sup>1016</sup> (especially where the regulation 90 text<sup>1017</sup> is omitted or not obvious) in warranty, limitation of liability and no liability clauses;
- include broad unilateral consumer indemnities, not necessary to protect the provider's legitimate interests;
- exclude liability for (affiliated) third party products and terms, despite recommending them as within their CIOT ecosystem;<sup>1018</sup>
- use of choice of law or compulsory arbitration provisions to restrict a consumer's rights to commence proceedings, impose evidential burdens or limit evidence admissible.

Numerous other terms which may be unfair but not within the specific categories are not identified. One interesting example was a disclaimer as to information security whereby the consumer accepts the (subjective) "transparency" assessment also suggests that most terms lack reasonably plain language, are not presented as clearly as possible, but positively, are legible and readily available. Perhaps reflecting the relative risk profile, smart self examples used simpler terms and were more transparent than those for smart homes. It should also be mentioned that terms all expressly incorporate lengthy privacy policies (**Ch 6**), which may also offend section 24. For example:

- *A term consenting to broad PI collection, retention and usage rights*  
 Australian Privacy Principles 3 and 6 require data minimisation. ACCC sweep reports suggest that failures in this regard could also be misleading and deceptive and unfair to a consumer, who may be misled into believing that broad collection and use is necessary when it is not, or that extensive collection is reasonably required to provide the service. FIPA found car manufacturers offend both data minimisation and informed consent requirements in (for example) requiring vast, unnecessary data to use smart car services.<sup>1019</sup> However, as the contracts reviewed suggest, data minimisation is poorly observed, and 'use' is privileged over consumer control. That there is no OAIC or ACL judicial authority impugning such collection does not promote minimising data take.
- *A term suggesting a consumer consents to PI disclosure to overseas recipients (without more);*

---

<sup>1016</sup> ACL: ss. 259 and 271.

<sup>1017</sup> "our goods come with guarantees that cannot be excluded by the Australian Consumer Law..."

<sup>1018</sup> The ACL refers to "agents" which may not comprehend these third parties, but as this practice is common in CIOT smart home contracts, it is flagged.

<sup>1019</sup> FIPA, above n 480: 6.

While common, this term is designed to disclaim provider's liability for personal information sent overseas.<sup>1020</sup> If a clause fails to explain this clearly then it may be unfair as consumers are effectively providing consent to extinguish an extant right. It is also questionable whether a bundled consent – such as a one-click contract - is sufficient to provide consent in this context or whether an express opt-in is required.<sup>1021</sup>

**Sched. 1** may suggest CIOT contracts<sup>1022</sup> share issues consistent with ACCC findings across other industries. It may be that as the CIOT market matures, cases may emerge voiding unfair terms, but absent other ACL breach, remedies may not incentivize compliance, especially where unilateral term variation rights are common, effective immediately, and many apply with little consumer notice, by implied consent.

#### 4.4.3 Cases

There are no cases concerning unfair CIOT contract terms in Australia, and few overall since 2010.<sup>1023</sup> Of these, cases include four terms in an ISP contract,<sup>1024</sup> consumer liability for hire car damage irrespective of fault;<sup>1025</sup> and a term requiring consumer 'opt out' of automatic direct debits were "unfair".<sup>1026</sup> In Victoria, trivial VCAT matters are routine: from a no refund hire deposit term (not unfair),<sup>1027</sup> to severance of parts of a hair studio termination;<sup>1028</sup> to a "moral victory" when an unfair arbitration clause was severed, but no contract breach found entitling a remedy.<sup>1029</sup> This should perhaps be viewed against

---

<sup>1020</sup> Relevant provisions are PA section 16C and APP8 which create a regime whereby APP entities are responsible for privacy protections unless a consumer consents to disclosure "after having been informed that the supplier will not be liable for any overseas' recipient's data misuse".

<sup>1021</sup> Gordon Hughes and Lisa Di Marco, 'Online privacy policies – it's not just about the Privacy Act' *Internet Law Bulletin* (April 2015 accessed 2 May 2015) 38- 40: 40.

<sup>1022</sup> The author subsequently searched out an example of 'good' cloud contracting and at least in terms of transparency, concludes that Dropbox has adapted a consumer-friendly approach: dropbox 'Terms of Service' (20 Feb 2014 effective 24 March 2014 accessed 19 June 2014) <https://www.dropbox.com/terms>

<sup>1023</sup> Consumer Affairs Victoria instituted proceedings against AAPT, World Swimming Championships 2007, 2006 Formula 1 Fosters Australian Grand Prix and Foxtel after its analogous legislation was introduced in 2003. See also *Jetstar Airways Pty Ltd v Free* [2008] VSC 539 <<https://www.consumer.vic.gov.au/businesses/fair-trading/contracts/unfair-contract-terms/case-studies-unfair-contract-terms>>

<sup>1024</sup> *ACCC v Bytecard Pty Limited* (Federal Court, 24 July 2013, VID301/2013) In that case, unfair terms included a unilateral price variation without a customer right to terminate the contract; an indemnity applying even where the contract has not been breached, or caused by ByteCard's breach; and unilateral termination.

<sup>1025</sup> *Australian Competition and Consumer Commission v CLA Trading Pty Ltd (t/as Europcar Australia)* [2016] FCA 377

<sup>1026</sup> *ACCC v Chrisco Hampers* [2015] FCA 1204, per Edelman, J

<http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2015/2015fca1204> While no pecuniary penalties are available for breach, the ACCC can take action under other ACL provisions as well.

<sup>1027</sup> *Aboud v Krystal Limousines Pty Ltd* (Civil Claims) [2017] VCAT 459 (2 Apr 2017)

<sup>1028</sup> *Dharmawardena v Advanced Hair Studio* (Civil claims) [2016] VCAT 1036 (6 July 2016)

<sup>1029</sup> *Mastos v Advanced Hair Studio* (Civil claims) [2016] VCAT 57 (12 January 2016)

the extensive ACCC sweeps referred to earlier, which targeted large consumer-sensitive industries, and so resolved potential cases cooperatively.

Norwegian CIOT work is thus of interest: their Consumer Council reviewed four smart fitness devices<sup>1030</sup> and two smart toys<sup>1031</sup> and have formally complained that the failure to notify term changes in advance is an unfair term.<sup>1032</sup> The consequence is that consumers may be locked-in to devices, prevented from data portability or termination and also, from changing providers, before the new terms apply.<sup>1033</sup> Apple responded to their similar complaint by changing its worldwide terms. They also found that contract length, failure to give advance notice of (material) changes as to functionality, user interface or rights, were deficient. European cases also reveal some significant victories:<sup>1034</sup> *In re Google, Inc.*<sup>1035</sup> held that 25 terms in Google's online 2013 Terms of Use and Privacy Statement, were unenforceable.<sup>1036</sup> The Berlin District Court ruling addressed three areas which arguably, remain Australian legal uncertainties: firstly, it held that online terms and privacy statements create legally enforceable contracts even where (for example) related app services are 'free'.<sup>1037</sup> The court found that consent to terms upon registration created an exchange for value, whereby Google receives commercially-valuable personal data for its

---

<sup>1030</sup> FORBRUKERRÅDET (Norwegian Consumer Council), Formal Complaint' (3 Nov 2016 accessed 2 Dec 2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/11/2016-11-03-formal-complaint-wristbands-final1.pdf>

<sup>1031</sup> FORBRUKERRÅDET, 'Report: Investigation of privacy and security issues with smart toys' (2 Nov 2016 accessed 15 Jan 2017) <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf>; FORBRUKERRÅDET, '#Toyfail' (Dec 2016 accessed 15 Jan 2017) <<https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf>>

<sup>1032</sup> They point to their previous Apple complaint which led Apple to modify its international terms in this regard: FORBRUKERRÅDET (Norwegian Consumer Council), Formal Complaint' (3 Nov 2016 accessed 2 Dec 2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/11/2016-11-03-formal-complaint-wristbands-final1.pdf>; and FORBRUKERRÅDET, 'Complaint regarding user agreements and privacy policies for internet-connected toys – the Cayla doll and i-Que robot' (6 Dec 2016 accessed 15 Jan 2017) <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/complaint-dpa-co.pdf>

<sup>1033</sup> *Ibid*: 6.

<sup>1034</sup> See also the Belgian Report into Facebook (Mar 2015) which concluded that "...Facebook... violates the EU Unfair Contract Terms Directive" which covers 'free' services. Those violations relate to (inter alia) major contractual terms, which included liability limitations, indemnities, unilateral variation, forum, choice of law and termination: EMSOC & SPION, 'From social media service to advertising network' Draft Report on Facebook (31 March 2015 accessed 13 Apr 2015) <<https://www.law.kuleuven.be/icri/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf>> :25 [fn 63]. The Report also concludes Facebook breaches the e-Privacy Directive Art 5(3) as to obtaining free, specific, informed and unambiguous/explicit prior consent for users (despite high-level disclosure) and tracks non-users improperly. Article 5(3) requires prior informed, specific, freely given consent for storage of or access to information stored on a user's terminal equipment.

<sup>1035</sup> *In re Google, Inc.*, LG Berlin, No. 15 O 402/12, 11/19/13. There is no English translation of this case available, nor does a search reveal that Google's appeal was successful. This discussion relies on secondary sources.

<sup>1036</sup> Note the German unfair contract terms legislation specifies that terms which conflict with the "main elements of German law and unfairly disadvantage consumers" are invalid. Here the German *Federal Data Protection Act* and the *Telemedia Act* were allegedly infringed (although Googles challenged their application). There is no equivalent to this provision in the ACL, but one would expect terms which increase inequality of bargaining power through which breaching other laws to be *prima facie* unfair.

<sup>1037</sup> Google argued that as their services are 'free', there was no valid contract subject to the unfair contracts regime.

various purposes.<sup>1038</sup> In a CIOT context, even were there no ‘official’ registration, the implicit promise of term-prescribed data use upon device connection, might be sufficient alone. The court’s approach would satisfy the ACL “in trade or commerce” requirement<sup>1039</sup> – as the obtaining and use of such data is clearly a part of the CIOT business model, although in most CIOT scenarios, consumer contractual dealings bear a commercial character<sup>1040</sup> whether selling devices and providing app services in any case. Based upon the German authority, the ‘business activities’ of obtaining consumer information for use or with the intention of analytics or creating saleable data sets<sup>1041</sup> via free service offerings<sup>1042</sup> should suffice, even where the device seller and app provider are different corporate entities. Secondly, the Google case confirms certain unfair term types: unilateral termination, unilateral services change; unilateral variation to terms of use without consent and the (mutual) limitation for liability as to statutory product liabilities. The final interesting aspect was that as Google’s privacy disclosures were inadequate, check-box consents were void.<sup>1043</sup>

The case is potentially, very significant were elements of its findings adopted in Australia, and arguably, with greater regulator focus in 2017, there may be more cases emerge to test that possibility.

#### 4.4.4 Some recommendations

Unfair terms are an ACCC priority for 2017<sup>1044</sup> - perhaps reflecting two gaps evidenced here: firstly, the law is largely untested and so lacks clarity and clear examples of breach; and secondly, companies are

---

<sup>1038</sup> Karin Retzer, ‘German Court Finds 25 Provisions in Google’s Online Terms of Use and Privacy Policy to Be Unenforceable’ *Morrison & Foerster LLP* (20 Dec 2013 accessed 10 Aug 2014) <<https://www.jdsupra.com/legalnews/german-court-finds-25-provisions-in-goog-45359/>>

<sup>1039</sup> The ACL definition includes ‘any business or professional activity whether or not carried on for profit’: ACL s 2.

<sup>1040</sup> *Hearn v Rourke* [2003] FCAFC 78 per Dowsett, J the focus must be on the conduct in question – which on the facts of *In re Google*, above n 237 included the terms enabling the commercial use of the consumer information.

<sup>1041</sup> A similar though not analogous fact situation is solicitation by mail for subscribers for UK books etc., which conduct was held to be “in trade or commerce”: *Swan v Downes* (1978) 34 FLR 36 *cf E v Australia Red Cross Society* (1991) 27 FCR 310 where the provision of free blood was held to be not “in trade or commerce”.

<sup>1042</sup> An extension of the argument might be to suggest that promoting such services as “free” breaches ACL section 18 insofar as whilst there is no apparent cost, the consumer is supplying data which has commercial value to the cloud provider. This would be an unlikely extension to the law (which tends to focus directly upon the representation with respect to whether a consumer must pay or lose money directly in some way) but would more realistically reflect the exchange between the parties – and seems open on the reasoning of the German case.

<sup>1043</sup> Spain and Germany are threatening financial sanctions because the privacy terms fail to comply with their privacy laws: Loeb Essers, ‘Berlin court rules Google privacy policy violates data protection law’ (20 Nov 2013 accessed 10 Aug 2014) <<http://www.cio.com/article/2380759/legal/berlin-court-rules-google-privacy-policy-violates-data-protection-law.html>>; France also took legal action.

<sup>1044</sup> In 2016, the ACCC published a B2B report: ACCC, ‘Unfair Terms On Small Business Contracts’ (10 Nov 2016 accessed 10 Nov 2016) <[http://acc.gov.au/system/files/B2B%20UCT%20-%20Final%20%20Unfair%20terms%20in%20small%20business%20contracts%20%20A%20review%20of%20selected%20industries\\_0.PDF](http://acc.gov.au/system/files/B2B%20UCT%20-%20Final%20%20Unfair%20terms%20in%20small%20business%20contracts%20%20A%20review%20of%20selected%20industries_0.PDF)> Then in early 2017 announced that it has a number of “in-depth investigations” underway into B2B unfair terms, which it will (presumably) presumably act on in 2017: Dr Michael Shaper, ACCC deputy Chair quoted in ACCC, ‘Unfair contract

not complying and/ or perceive breaching the law as an acceptable risk.<sup>1045</sup> These enforcement ‘gaps’ confirm the ACCC’s emphasis to highlight (and test) the law and to incentivize compliance. But there are also exacerbating legal ‘gaps’:

➤ Unfair ‘contracts’: extend the law to contracts unfair ‘overall’

While this is partly duplicative,<sup>1046</sup> there seems little logic in finding unfairness in a term, or allowing that unfairness to void an entire contract if it cannot operate otherwise, as distinct from multiple terms combining to create an overall unfair effect. Few companies dread severance when terms can so simply be rectified online, so a broader scope may increase compliance. CAANZ rather unpersuasively rejecting this proposal,<sup>1047</sup> which would address a gap and strengthen the regime;

➤ Monetary penalties:<sup>1048</sup> to incentivize compliance and the increase the risk of infringement.

Given the regime presupposes a standard form non-negotiable contract and ‘unfairness’ requires terms that do not reflect the ‘legitimate interests’ of the advantaged party, significantly imbalance rights and obligations and cause consumers ‘detriment’, there is a clear argument for penalties where such egregious conduct can be established, especially were it repeated conduct;

➤ Representative actions should be available to regulators.

This would increase exposure should the law be breached and enhance widespread consumer rights and redress, especially if CAANZ increases investigative powers as it proposes;<sup>1049</sup> and

➤ Capture insurers: extend unfair contract terms to cover the Insurance Contracts Act 1984 (Cth).

Insurers are not subject to the unfair terms regime<sup>1050</sup> – aside from sound public policy issues,<sup>1051</sup> CIOT data may assume a greater role in insurer decision-making, insurance policies may (for

---

terms under scrutiny’ *Media release* (20 Mar 2017 accessed 28 Mar 2017) <http://www.accc.gov.au/media-release/unfair-contract-terms-under-scrutiny>. Note its earlier consumer review here: ACCC, above n 998.

<sup>1045</sup> In *Valve*, the judge was very critical of the US General Counsel’s failure to redraft the terms and conditions in such a way as to meet Australian law, especially as terms had been changed to meet NZ requirements.

<sup>1046</sup> Unfairness may underlie actions under sections 18 and 21 – but it may also not. The Law Council pointed to unfairness as one of the relevant indicia of unconscionability though acknowledged the latter requires something more. They seem to suggest that a contract should not be struck down for unfairness if it is not unconscionable, which seems logically flawed: Law Council of Australia, ‘Australian Consumer Law Review’ Submission (23 Jun 2016 accessed 4 Sept 2016) 36- 37 < [http://consumerlaw.gov.au/files/2016/07/Law\\_Council\\_of\\_Australia.pdf](http://consumerlaw.gov.au/files/2016/07/Law_Council_of_Australia.pdf)>

<sup>1047</sup> For example, the Law Council put several arguments: these included freedom of contract (which of course has little relevance in a standard form contract scenario), plus the contract as a whole and transparency are part of the matters a court must consider: *Ibid*: 23- 24.

<sup>1048</sup> CALC advocated for this in the ACL review: above n 840: 46.

<sup>1049</sup> CAANZ Proposal 11 suggests that regulators should be allowed to access existing investigative powers to better assess if any term is unfair: ACL Review, above n 840: 6.

<sup>1050</sup> CCA section 131A. An alternative would be to mirror the provisions within the *Insurance Contracts Act 1984 (Cth)*, as sections 14, 35 and 37 are criticised as not equivalent. Note section 15 prevents judicial review of insurance contracts on the grounds of unfairness. CAANZ has recommended that the unfair term provisions be extended to include the Insurance Contracts Act 1984 (Cth): above n 840: 6.

<sup>1051</sup> Public policy and clear regulation in this area is urgently required given the value of smart health, home and car data to insurers, and the costs to the community if the elderly or poor are unable to take out insurance

example) unfairly compel or unfairly incentivize privacy-intrusive data sharing used for potentially discriminatory practices<sup>1052</sup> (see 3.2.1 above).

These changes would strengthen the regime, facilitate ‘headline grabbing’ enforcement and incentivize proactive behaviour change, as revealed by the obvious fact that despite clear legislation, online unfair terms proliferate.

#### 4.5 Consumer Guarantees<sup>1053</sup>

CIOT contracts for the supply of goods or services to a consumer in trade or commerce contain consumer guarantees<sup>1054</sup> which despite many contrary online terms, cannot be excluded, restricted or modified by contract.<sup>1055</sup> There are nine guarantees as to ‘goods’ and three as to ‘services’<sup>1056</sup>: the former cover good title,<sup>1057</sup> undisturbed possession,<sup>1058</sup> no undisclosed securities,<sup>1059</sup> acceptable quality,<sup>1060</sup> fitness for disclosed purpose,<sup>1061</sup> correspondence with description or sample,<sup>1062</sup> availability of repairs and spare

---

<sup>1052</sup> An example in a life insurance context was a Total Permanent Disability policy which did not cover a certain ‘type’ of heart attack resulting in the insured receiving only \$25,000 of the \$1million he was supposedly insured for: Adele Ferguson, ‘Cominsure exposed’ *Sydney Morning Herald* (8 Mar 2016 accessed 2 Dec 2016) <<http://www.smh.com.au/interactive/2016/comminsure-exposed/heart-attack/>>

<sup>1053</sup> EU policy is found in Directive 1999/44/EC <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0044:en:HTML>>

<sup>1054</sup> Vulkanovski, above n 110 suggests that the consumer guarantees do not apply to CIOT as it excludes a “telecommunications service” under s. 65 (1)(b). ‘Telecommunications Service’ is defined as a “service for carrying communications by means of guided or unguided electromagnetic energy or both”: ACL section 65(2). Legal analysis confirms that this section does not apply, as nothing of that “kind [is] specified in the regulations”: ACL s. 65(1)(a). Consumer groups have called for this exemption to be removed from the ACL: ACCAN, Submission, above n 840.

<sup>1055</sup> ACL section 64 prohibits express terms which exclude, restrict or modify the guarantees or any term which is inconsistent with a guarantee – subject to section 64A. This latter provision allows limitation of liability with respect to goods not of a kind ordinarily acquired for personal, domestic or household use or consumption. As discussed, this paper assumes that consumer IoT goods are, in general, of the sort which would be found to be for ‘personal domestic or household use or consumption’.

<sup>1056</sup> Applicable guarantees are that the supplier will render those services with due care and skill (s. 60), and that the services and any product resulting from them, will be reasonably fit for that purpose (s. 61). This guarantee requires that the consumer makes known ‘expressly or by implication’ that purpose including a “result that the consumer wishes to achieve”, and then there is a guarantee that the services and product will be of “such nature, and quality, state or condition, that they might reasonably expected[,] to achieve that result...” (s. 61(2)). Given the prevalence of free app provision, it is arguable that subscription (whether paid or free) involves by implication, making known an expectation that the services and products will meet the service levels and performance promoted by the app provider. The third guarantee is that services will be provided within a ‘reasonable time’ but it does not apply where there is a ‘manner’ for determining time frames agreed to by the consumer and supplier. CIOT contracts may cover this field.

<sup>1057</sup> ACL section 51 (unless the supply is expressly for limited title or by hire or lease). In the circumstances of IoT devices and software, the terms and conditions will dictate this aspect.

<sup>1058</sup> ACL section 52 (only for the period of hire or lease).

<sup>1059</sup> ACL section 53.

<sup>1060</sup> ACL section 54.

<sup>1061</sup> ACL section 55.

<sup>1062</sup> ACL section 56.

parts,<sup>1063</sup> and mandatory compliance with express warranties.<sup>1064</sup> These apply to CIOT devices and software as 'goods', such that breach entitles consumers to specified remedies. As such, this section considers only those guarantees involving especial CIOT interest: sections 54, 58 and Regulations 90 - 91.

Section 54 *acceptable quality* requires the device/ software to be:

- fit for all reasonable purposes for which goods of that kind are commonly supplied,<sup>1065</sup>
- acceptable in appearance, and
- free from defects, and
- safe and durable

as a reasonable consumer, fully acquainted with the state of the goods (and any hidden defects), would regard as 'acceptable' on the date of supply,<sup>1066</sup> having regard to goods' nature and price, supplier representations (marketing, advertising, packaging information etc.) and any other relevant circumstances. Consumers may thus sue a manufacturer or supplier of a defective CIOT device or software supplied which (for example) is damaged, fails to work, or which fails to conform with description, advertised features or performance levels. 'Safe'<sup>1067</sup> is undefined but interesting in a CIOT context, given security is a complex question and hacking, a known possibility. There is no authority as to whether "safe" means "secure"- although given known security incidents, a consumer may have a right to expect designed-in security in 'acceptable' online devices - or whether a hack might constitute a "defect" as opposed to a known product vulnerability.<sup>1068</sup> Ironically, there is potentially an argument for CIOT providers to assert a *lower* consumer expectation standard generally across IT devices having regard to the nature of the industry, its well-publicised security and privacy issues, the common experience of software glitches and hacking, and thus, the nature of the products supplied. However, one suspects that such an argument is unlikely to succeed except in extreme cases: designers/ manufacturers arguably should understand and secure devices and software against known risks and further, devices intended

---

<sup>1063</sup> ACL section 57.

<sup>1064</sup> ACL section 58. Note Regulation 90 of the Competition and Consumer Regulations 2010 (Cth) specifies a text which must appear, as well as mandates information as to who provides the warranty, its duration and how to claim under it.

<sup>1065</sup> The purpose of acquisition is irrelevant: *Petersen v Merck Sharpe & Dohme (Aust) Pty Ltd* [2010] FCA 180

<sup>1066</sup> *Medtel Pty Ltd v Courtney* [2003] FCAFC 151. But this does not preclude subsequent relevant information as to the goods being considered by the court, in its determination of objective reasonable expectation.

<sup>1067</sup> CAANZ proposes to work with stakeholders to provide more specific guidance on the terms 'safe' and 'durable': above n 840: 5.

<sup>1068</sup> By analogy, a consumer failed to prove that Vioxx arthritic pain relief medication was not of 'merchantable quality' (the previous formulation for acceptable quality) even though it was known that it might double the risk of cardiac arrest: *Merck Sharp & Dohme (Australia) Pty Ltd v Peterson* [2011] FCAFC 128.

for home use may reasonably be expected to meet normative social values as to that space and as to vehicles, consumers have long built-up safety expectations in that industry.

ACL Regulation 90(2)<sup>1069</sup> prescribes a specific consumer guarantee text<sup>1070</sup> which must be included with any goods (or oddly, services)<sup>1071</sup> which are supplied with a 'warranty against defects'.<sup>1072</sup> That term is broadly applied such that most suppliers with any manufacturer's warranty must comply, including software or devices purchased online. Regulation 91 prescribes a repair notice applicable to devices containing user-generated data,<sup>1073</sup> - including CIOT devices - which must state that "repair may result in loss of data". While a serious issue, it seems odd to absolve the IT industry generally from the obligation to design products which are repairable, or to provide 'backup' services to consumers such that they do not lose valuable data stored on-device. The risk is reduced given CIOT cloud backup is commonplace, but from a consumer convenience perspective, the regulation is flagged for obsolescence: arguably it may lower rather than lift reasonable consumer expectation. Similarly, section 58 obliges broadly-defined<sup>1074</sup> manufacturers to "take reasonable action" to provide repair facilities and reasonable parts availability for a "reasonable period" after which goods are supplied. Like s. 54, "reasonable" is unclear as to either repair facility or parts availability or time, so presumably this becomes a question of contemporary standards.<sup>1075</sup> The section is mentioned not because it is outdated for all goods: clearly a smart(ish) car still needs hands-on servicing, but rather, to highlight its obsolescence in a hybrid device: software context. While "parts" is undefined, it includes CIOT device 'parts', and may include on-device

---

<sup>1069</sup> Competition and Consumer Regulations 2010 (Cth). From 1 January 2012, any document containing a warranty against defects as to the supply of goods or services or a representation that such a warranty applies, is prohibited if it does not comply with regulation 90: ACL s. 102. Failure to comply with the requirements from 1 January 2012 may result in penalties up to \$50,000 per offence for corporations and \$10,000 per offence for individuals.

<sup>1070</sup> "Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure."

<sup>1071</sup> CAANZ Proposal 4 includes clarifying this text to address "services bundled with goods" and 'services', which are ACL 'gaps'. Miller (at page 1763) suggests that this would presumably never be prosecuted (as no services-specific text exists) and argues it would be an "unintended absurdity" in the ACL. He cites *BMW Australia Pty Ltd v ACCC* [2004] FCAFC 167, a case where BMW failed to adopt precise Standards terminology as in their (correct) view, their instructional language for jacks was more accurate. They lost and were fined: R. V Miller, '2016 Miller's Australian Competition and Consumer Law Annotated' Thomson Reuters Lawbook Co., 2016.

<sup>1072</sup> 'Warranty against defects' means a "representation communicated to a consumer in connection with a supply of goods or services, at or about the time of supply, to the effect that a person will (unconditionally or on specified conditions): (a) repair or replace the goods or part of them; or (b) provide again or rectify the services or part of them; or (c) wholly or partly recompense the consumer; if the goods or any part of them are defective, and includes any document" evidencing that representation: ACL s. 102(3).

<sup>1073</sup> Regulation 91 cites files on a computer hard drive, mobile phone telephone numbers, songs on a portable media player, games stored on a console or files on a USB memory stick.

<sup>1074</sup> 'Manufacturer' includes persons who produce, process or assemble goods, hold themselves out as such, permit others to use their name/ brand as to the goods, cause or allow themselves to be held out as such or import goods where the overseas 'manufacturer' lacks a place of business in Australia.

<sup>1075</sup> Miller, above n 1071: 1732.

software as a component,<sup>1076</sup> but seems likely to exclude related CIOT app software upgrades or patches, which are by nature (partly) repair. It is also possible that such repair might be unreasonably delayed, leaving consumer IOT devices exposed<sup>1077</sup> – but this provision will presumably not apply.

The consumer guarantees have flaws – indeed, the laws are confusing and despite simple language, are difficult to apply.<sup>1078</sup> The distinction between ‘major’ and ‘minor’ failures<sup>1079</sup> is unclear, the ‘reasonable’ time for minor defect repairs is nebulous<sup>1080</sup> and consumers precluded from a replacement in that case, despite repeated minor failure.<sup>1081</sup> Further determining the ‘extent’ of defect in a CIOT device or app will often require expert technical review, which is expensive and makes seeking redress potentially prohibitive in most smart self and home scenarios. Even in a smart car context, the manufacturer will possess complex vehicle and diagnostics data to which, absent court order, consumers have little access, and costs of appraisal are high. Further, third party service software lock-out<sup>1082</sup> may mean product-protective dealer-retailers will largely control smart car defect investigations, thereby increasing information asymmetry, and reducing legal action and regulator information.

---

<sup>1076</sup> Ibid: 1723. “The ACL draws no distinction between products and the component parts of products, each may therefore be regarded separately as ‘goods’ for the purposes of this [s. 54] guarantee”.

<sup>1077</sup> It is suggested that the android phone industry was very slow in its response and that different suppliers at different levels across different phones, caused consumers problems: Jason Bourne, ‘One in three cloud services was susceptible to Heartbleed, research shows’ *Cloudtech* (12 May 2014 accessed 7 June 2014) <http://www.cloudcomputing-news.net/news/2014/may/12/one-three-cloud-services-was-susceptible-heartbleed-research-shows/>

<sup>1078</sup> See critical submissions to the ACL Review from a range of entities: Allens, CHOICE, ACCAN, Baker & McKenzie, etc. The CAANZ Interim Report summarizes these to suggest that while consistent laws are positive, ‘acceptable quality’ as a flexible principle-based text is subject to what constitutes “reasonable durability”, and what a ‘major failure’ is. CAANZ suggest that regulator guidance can address these issues and suggests that industry-specific approaches are best dealt with through compliance and enforcement activities, as well as soft law options such as best practice guidelines or codes of conduct: CAANZ, above n 832: 43- 44.

<sup>1079</sup> ACL s. 260: A major failure means one where a reasonable consumer would not have acquired the goods had s/he been fully aware of the failure or the goods are any of unsafe, substantially unfit for purpose or departed significantly from a demonstration model/ sample. CAANZ Proposal 2 will clarify that multiple “minor” failures can become a ‘major failure’: CAANZ, above n 832: 4.

<sup>1080</sup> CAANZ Proposal 1 would insert a specified time, so that upon expiry, remedies for refund and replacement become available without needing to show a major failure: CAANZ, above n 832: 4.

<sup>1081</sup> CAANZ Proposal 2 will clarify that multiple “minor” failures can become a ‘major failure’: CAANZ, above n 832: 4.

<sup>1082</sup> AAAA, above n 401. The AAAA contend that the Code of Practice has failed to free up after-market vehicle data access and that the OEMs are not ‘playing ball’. They persist in seeking legislation: AAAA, ‘Agreement on Access to Service and Repair Information for Motor Vehicles 2014, Code of Practice’ (2014 accessed 30 June 2016) <https://www.aaaa.com.au/files/issues/Signed%20Agreement%20-%20Access%20to%20Service%20and%20Repair%20Information%20151214.pdf>; For a full summary of the AAAA concerns and their view as to the Code’s failure, see: AAAA, ‘Heads of Agreement for Access to Service Information and Repair of Motor Vehicles and Related Voluntary Codes Of Practice (Feb 2017 accessed 2 Mar 2017) <<https://www.dropbox.com/s/v79cbsncat7itm8/170228-AAAA-HOAandCodes-Opt.pdf?dl=0>>

#### 4.5.1 Cases

Consumer guarantee application is challenged by the “hybridisation” of physical goods, software ‘goods’ and analytics ‘services’.<sup>1083</sup> In *Valve*,<sup>1084</sup> the Federal Court ruled that licensed, subscribed games software and associated services, internet-streamed internationally<sup>1085</sup> and playable on or offline, is the supply<sup>1086</sup> of a “good”, and so subject to the ‘acceptable quality’ guarantee and remedies, which the Steam agreement and refund policies falsely misrepresented. It seems that had games not been accessible “offline”, had the non-executable data (music, etc.) and other services<sup>1087</sup> not been “incidental”, then the transaction may lose the character of ‘goods’. As such, *Valve* illustrates that from a consumer guarantee perspective, online acquisition<sup>1088</sup> or CIOT software provision is not necessarily straightforward. Arguably, the whole enquiry perpetuates an ongoing legal uncertainty which would be better resolved by statute: for example, an amendment which expressly states that ‘goods’ includes software inclusive of any related features such as data analytics or cloud storage. In December 2016, Valve was ordered to pay \$3 million in penalties.<sup>1089</sup> Valve has appealed, and the ACCC cross-appealed findings that misleading representations to consumers (who were not personally misled) did not constitute conduct breaching section 18.<sup>1090</sup> Based upon well-established precedent, the ACCC seem likely to succeed.

Consumer guarantee cases more often concern false representations as to when guarantees and remedies apply,<sup>1091</sup> and the misrepresented interaction between statutory and manufacturer (voluntary)

---

<sup>1083</sup> CI, above n 44; ACCAN, Submission, above n 840.

<sup>1084</sup> *Australian Competition and Consumer Commission v Valve Corporation (No. 3)* [2016] FCA 196 per Edelman, J 24 Mar 2017 accessed at <<http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2016/2016fca0196>>

<sup>1085</sup> The case was also significant in that it clarified that a corporation incorporated in Washington State and which lacked a physical presence in Australia, was still subject to the ACL – despite a choice of law clause which purported to exclude local jurisdiction. The court found that Valve “carried on business” in Australia as it had over 2 million subscribers, owned and used servers there, generated millions of dollars in revenue and paid Australian companies to run its business in Australia: Valve, *Ibid*: 4.

<sup>1086</sup> The ACL defines a “supply of goods” to include “...supply (including re-supply) by way of sale, exchange, lease, hire or hire purchase”.

<sup>1087</sup> For example, Steam Guard, Play or Videos.

<sup>1088</sup> It should also be noted that many CIOT app ‘acquisitions’ are either licensed free or by subscription and as Valve suggests, the inclusive definition of “acquire” under the ACL is broad enough to include this concept - ‘acquire’ includes (a) in relation to goods – acquire by way of purchase, exchange or taking on lease, on hire or hire purchase; and (b) in relation to services – accept: ACL section 2. Under section 11 references to acquisition ... include Section 5 provides an exception under the safety standards provisions (Parts 3-3, 3-4, 4-3 and 4-4) where a donation of goods or services is a ‘supply’ unless for “promotional purposes”.

<sup>1089</sup> *Australian Competition and Consumer Commission v Valve Corporation (No. 3)* [2016] FCA 196 per Edelman, J 24 Mar 2016 <<http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2016/2016fca0196>>

<sup>1090</sup> ACCC, ‘ACCC cross-appeals Valve Federal Court judgment’ *Media Release* (7 Mar 2017 accessed 8 Mar 2017) <<https://www.accc.gov.au/media-release/accc-cross-appeals-valve-federal-court-judgment>>

<sup>1091</sup> See for example, the first consumer guarantees case, *Australian Competition and Consumer Commission v Hewlett-Packard Australia Pty Ltd* [2013] FCA 653. Remedies included pecuniary penalty of \$3 million (maximum penalty \$6.6 million); \$200,000 for ACCC's costs; Injunction against similar false representations for 3 years; HP letter to resellers; Consumer rights notice on its website and online store for three years; Corrective advertising on website homepage for 3

warranties,<sup>1092</sup> and often heavily-spruiked (questionable) extended warranty products.<sup>1093</sup> These are common in smart self and home<sup>1094</sup> retailing and in the second-hand car industry. One of the more relevant ‘cases’, settled by undertaking, was that Apple falsely represented its consumer guarantee obligations, and that refunds, replacement or repair was not available for third party products purchased via iTunes or the App Store. The undertaking highlighted how Apple refund policies breached the ACL, which Apple acknowledged, accepting a suite of consumer education, training, data verification and improved reseller returns practices. Apple’s ‘Consumer Law’ Australia webpage is now best practice and a model for transparent disclosure.<sup>1095</sup> A 2017 Apple case<sup>1096</sup> confirms the point: an iOS9 update during installation ‘bricked’ iphones and ipads which had undergone an ‘unauthorised’ repair, service or replacement,<sup>1097</sup> via ‘Error53’. Apple then falsely represented that it was not responsible to rectify the error without cost, nor must it honour its voluntary recall. The ACCC alleges these representations as to acceptable quality and fitness for purpose and remedies under Part 5-4 breach ACL section 29(1)(m) which prohibits false or misleading representations as to any “guarantee, right or remedy” and section 18. The case – and recent proceedings against LG - illustrates how large CIOT companies, supplying sophisticated products online to vast numbers of consumers, can still (repeatedly) fail to comply with the ACL.

---

years and in major newspapers; Consumer Redress of complaints process; independent review and report thereof; and a compliance program for 3 years. More recently, smart TV manufacturer LG was taken to court: ACCC, ‘ACCC takes action against LG for alleged false or misleading representations relating to consumer guarantees’ Media release (15 Dec 2015 accessed 2 Feb 2016) <<https://www.accc.gov.au/media-release/accc-takes-action-against-lg-for-alleged-false-or-misleading-representations-relating-to-consumer-guarantees>>

<sup>1092</sup> Smart TV manufacturer LG was taken to court by the ACCC (again): Ibid.

<sup>1093</sup> CAANZ Proposal 3 addresses enhanced disclosure requiring written agreements, clarification as to the ACL, and a 10 day cooling off period: CAANZ, above n 840: 4. See for example, *Australian Competition and Consumer Commission v Bunavit Pty Ltd* [2016] FCA 6. As at 2016, the ACCC had obtained \$286,000 in penalty orders against ten Harvey Norman franchisees as to false or misleading representations regarding consumer guarantees: ACCC, ‘Harvey Norman franchisee ordered to pay penalties of \$52,000 for false or misleading representations about consumer rights’ (14 Jan 2016 accessed 20 Mar 2016) <<https://www.accc.gov.au/media-release/harvey-norman-franchisee-ordered-to-pay-penalties-of-52000-for-false-or-misleading-representations-about-consumer-rights>> In contrast, this case failed as it relied upon in-store conversations which the court regarded to be vague, and salespeople handed out brochures as to the ACL – despite the salespeople emphasising manufacturer’s warranties over ACL guarantees : *Director of Consumer Affairs Victoria v The Good Guys Discount Warehouses (Australia) Pty Ltd* [2016] FCA 22. In *ACCC v Fisher & Paykel Customer Services Pty Ltd* [2014] FCA 1393 an extended warranty sales letter was a “financial product” regulated under the ASIC Act. Penalties of \$400,000 were imposed.

<sup>1094</sup> Ibid.

<sup>1095</sup> <https://www.apple.com/au/legal/statutory-warranty/>

<sup>1096</sup> *Australian Competition and Consumer Commission v Apple Pty Ltd* [2017] FCA 416 (21 Apr 2017). This hearing concerned an ACCC application for substituted service upon Apple US, which was granted there being a prima facie case to answer. See also ACCC, ‘ACCC takes action against Apple over alleged misleading consumer guarantee representations’ (6 Apr 2017 accessed 6 Apr 2017) <<https://www.accc.gov.au/media-release/accc-takes-action-against-apple-over-alleged-misleading-consumer-guarantee-representations>>

<sup>1097</sup> Unauthorised repair means a repair, service or replacement by anyone other than Apple Australia or its authorized Service providers: Ibid [18]

#### 4.5.2 Recommendations

To succinctly summarize this section, the following recommendations are made:

A model ACL disclosure format by comparative table such as that on Apple's Consumer Law webpage, should be required by regulation to be notified to consumers. The frequency of egregious infringement by large companies breaching their disclosure obligations is such that legislative action is required.

Regulation 90 and 91 require amendment to enhance clarity as identified above.

CAANZ proposals seem sensible minor corrections to clarify the consumer guarantees.

It is not proposed to explore the consumer guarantees further, save to support ACL Review submissions that legal uncertainty and practical enforcement<sup>1098</sup> are 'gaps'. From a CIOT angle, the guarantees will likely be tested by the hybrid nature of the product, and in determining where reasonable consumer expectation across the electronics versus software industries reasonably falls.

#### 4.5.3 Conclusion

Consumer guarantees apply to suppliers, such as CIOT device manufacturers<sup>1099</sup> or retailers (online or off), and statutorily 'deemed manufacturers'<sup>1100</sup> or 'deemed importers'.<sup>1101</sup> CIOT devices are also subject to products liability law, which is considered next.

---

<sup>1098</sup> As to consumer disclosure requirements, see *Director of Consumer Affairs Victoria v The Good Guys Discount Warehouses (Australia) Pty Ltd* [2016] FCA 22 where despite salesperson representations as to extended warranties which allegedly breached sections 18, 29(1)(l) and (m), the court found the conversations were "vague and general" and as a brochure explaining the consumer guarantees was provided, the conduct was not misleading or deceptive. This is despite the fact the consumer guarantees were not drawn to customer's attention, and discussions as to (time limited) manufacturer's warranty did not clearly distinguish the two.

<sup>1099</sup> ACL section 7 inclusively defines a manufacturer to include those who produce, grow, extract, process or assemble goods" and who hold themselves out to the public to be manufacturer or allow other(s) to do so.

<sup>1100</sup> ACL section 7 also defines a manufacturer to include one who causes or permits another to hold them out to the public as the manufacturer, either in connection with the supply or possible supply or promotion of the supply or use of goods.

<sup>1101</sup> ACL section 7 defines an importer a deemed manufacturer if they did not manufacture the goods but at the time of importation, the manufacturer did not have a place of business in Australia.

## 4.6 Product liability & safety

*“While we look to the future, we must also maintain our focus on safety today.”*<sup>1102</sup>

The ACL has no express prohibition on selling unsafe products.<sup>1103</sup> ‘Acceptable quality’ (s. 23) requires that products are ‘safe’ and the first case finding breach of sections 18 and 33<sup>1104</sup> by the knowing marketing of unsafe products,<sup>1105</sup> was handed down in 2016. Edelman, J found that a supplier’s failure to withdraw and recall “once a reasonable period... in which it could have identified, assessed and responded to this safety hazard had elapsed” constitutes “silence” which is misleading and deceptive. It is a valuable precedent, and one which illustrates that even “household name” national retailers have flawed product safety assessment systems.<sup>1106</sup> The principal ACL focus consists of Parts 3-3 to 3-5 which contain a products liability and safety regime, comprised of principle-based regulation and strict liability enforcement of consumer product safety standards,<sup>1107</sup> in conjunction with educative materials

---

<sup>1102</sup> Mark R. Rosekind, Ph.D., Administrator, NHTSA, U.S. Department of Transportation, Before the House Energy and Commerce, Subcommittee on Commerce, Manufacturing and Trade (14 April 14, 2016 accessed 6 Jul 2016) <<http://www.nhtsa.gov/About+NHTSA/Congressional+Testimony/testimony-mr-house-04142016>>

<sup>1103</sup> The Australian Consumer Survey found that poor quality, faulty and unsafe products are the most common (30%) consumer problems in Australia CAANZ, Interim Report, above n 840: 73.

<sup>1104</sup> A person must not, in trade or commerce, engage in conduct that is liable to mislead the public as to the nature, the manufacturing process, the characteristics, the suitability for their purpose or the quantity of any goods”. Note that “liable” to mislead is a narrower range of conduct than s 18, requiring proof of actual probability that the public would be misled: *ACCC v Coles Supermarkets Australia Pty Ltd* [2014] FCA 634. Remedies include civil damages proceedings, remedial orders, injunction or pecuniary penalties.

<sup>1105</sup> *ACCC v Woolworths Ltd* [2016] FCA 18 <<http://www.austlii.edu.au/au/cases/cth/FCA/2016/44.html>> The Court declared that Woolworths as the retailer/importer (deemed manufacturer) engaged in misleading and deceptive conduct by selling unsafe products after it had become aware of safety concerns. Note the judge rather amusingly defined Woolworths conduct in failing to withdraw a potentially dangerous fryer, as the “Deep Fryer Silence Conduct”. The outcome of the conduct was however, far from amusing.

<sup>1106</sup> Woolworths has over 300 Australian stores. Despite this Edelman, J found: “Although Woolworths had product quality processes and a compliance system in place, it failed to prevent product safety issues from occurring and continuing to occur during 2013 and 2014. In the period from January 2012 to November 2014, Woolworths issued 47 non-food product recalls for its house brand goods (i.e. 18 recalls in 2012, 8 recalls in 2013 and 20 recalls in 2014).”: Ibid: [19]

<sup>1107</sup> Under ACL Part 3-1, the Commonwealth Minister may declare Australian Standards as product safety standards as to “consumer goods” [Section 2(1): Goods intended for use or of a kind likely to be used, for “personal, domestic or household use or consumption’.] and/ or related services if necessary to reduce or prevent the risk of injury. Supply of goods or related services which conflict with such standards is prohibited under the ACL and in the event of loss or injury, third parties may in certain circumstances, be deemed ‘supplied’. Part 3-3 Div 2 allows the Minister to impose interim (s 109) or (revocable) permanent bans (ss. 114 & 117) upon consumer goods or services, where the Minister decides that they are of a kind that may or will cause injury or that reasonable foreseeable use will have that result. (s 114) Failure to comply is also an offence, and any person injured because of the defect or reasonable foreseeable use of the goods, may recover damages or seek compensation: ACL ss 118 re goods and s 119 re product related services; section 197 provides fines are up to \$1.1 million for a corporation or \$220,000 for an individual and the court may order goods be destroyed under section 133H. Consistent with these powers, Subdivision A allows the Minister to mandate a consumer goods recall [ACL Division 3 ss 122 – 126] and the supplier must cease supplying the goods and comply with the notice [ s. 127] Subdivision B section 128 enables the supplier to initiate a voluntary recall. Note Supply’ includes sale, exchange, lease, hire or hire purchase. In the recent valve case discussed above, the court also found software supplied under a license was a supply: ACL section 2. Note there is a defence where the supplier was in turn supplied by an Australian entity and the supplier did not know, could not reasonably determine with due diligence, or relied in good faith upon a representation from the original supplier that there was no relevant standard: ss. 252 (re goods)) and 253 (re services) and ss 210 (as to civil penalties) and 211 (re goods/ services as to criminal penalties). Under ACL section 206. Penalties include \$1.1 million for a corporation (s 224) and \$220,00 for an individual: (s 194).

and standards.<sup>1108</sup> The product safety framework seeks to identify, prevent and remove unsafe goods and product-related services from the market, while the defective goods regime focusses upon consumer redress for loss or damage.<sup>1109</sup> The laws reflect harm minimisation principles and employ post-market controls such as mandatory reporting,<sup>1110</sup> supply bans<sup>1111</sup> and defect-rectification through voluntary or mandatory recall. The ACL has less focus upon pre-market controls such as safety standards,<sup>1112</sup> design rules and explicit safety obligations, though strictly enforces penalties for breaches of industry-specific mandatory safety standards, design rules and voluntary recall notification compliance. So, for example, should any CIOT device or software manufacturer fail to comply with any Australian Standard, or fail to initiate a voluntary recall upon detecting a safety related defect, then the regulator may act. Further, should any CIOT product be defective such that its “safety” is not such as “persons generally are entitled to expect”, resulting in death, personal injury or property damage, a consumer may institute proceedings for redress. Examples might include a smart home device which initiates actions causing a fire, a supposedly- ‘accurate’ smart self device which underreports fatal heart issues or a smart car with technology failures which cause a crash.

In locating product safety ‘gaps’ pertinent to the consumer IOT, the changing market context is important to understand. ACMA found that globalisation, overseas manufacture and online shopping “present regulators with enforcement and compliance challenges”.<sup>1113</sup> Health Canada point to increasing materials complexity, speedier innovation to market, new source countries for products, and increased consumer information demand, which “require a 21st century approach”.<sup>1114</sup> CIOT fits entirely within this space: with global manufacture and (significant) e-commerce purchasing and supply.<sup>1115</sup> Further the increasing role of software in safety-related products such as smart cars injects a new element. Half of all Australian

---

<sup>1108</sup> See for example, the ACCC Product Safety Australia website, Standards Australia Product Safety Framework: Handbook 295, ISO standards on safe products and recall and related ISO Guides.

<sup>1109</sup> CAANZ, Interim Report, above n 840: 71.

<sup>1110</sup> ACL section 131.

<sup>1111</sup> ACL ss 129 and 130. The bans process is essentially an administrative one whereby the Commonwealth Minister must notify suppliers, provide them with an opportunity to request a conference, accept written submissions and then consider a permanent ban. CAANZ cites the small powerful magnets ban, which required the states to impose interim bans for safety reasons whilst the Commonwealth process occurred. In Canada in contracts, Health Canada relied upon a general prohibition upon unsafe products in the Consumer product safety Act (SC. 2010, c. 21) ss &(a) and 8 (a). See the case study in CAANZ, Interim Report, above n 840: 77- 78.

<sup>1112</sup> ACL Part 3-4 Information standards.

<sup>1113</sup> ACMA, ‘Submission to the ACL review’ (2016): 8.

<sup>1114</sup> Health Canada, (2016) ‘Consumer Product Safety Act (CCPSA)’ <http://www.hc-sc.gc.ca/cps-spc/legislation/acts-lois/ccpsa-lcspc/index-eng.php> Note the CCPSA came into force on 20 June 2011.

<sup>1115</sup> The car industry has largely retained its franchised dealer sales model, which enables revenue through sales, but also through lucrative parts and service operations. Tesla has introduced online ordering through has opened factory-owned outlets for consumers to test drive their vehicles. It seems likely, as cars evolve into smart cars and virtual reality sales expand, that sales and servicing facilities may contract somewhat, though of course, parts and consumables such as tyres will presumably still require service outlets. It is an odd thought that VR may substitute for a test drive and that cars will ultimately drive themselves to be serviced.

safety-related *software defect* motor vehicle recalls for instance, have occurred from 2014 – March 2016 inclusive, and the author’s study (**Sched. 3**)<sup>1116</sup> reveals that 40 recalls – or 13% – involved thousands of consumers and resolution (mostly) by dealer-installed software update. While such recalls are gradually increasing,<sup>1117</sup> it seems likely that a software-driven smart(er) fleet coupled with inexpensive over-the-air updates/ recalls, will positively increase the “fix” rate. But while voluntary recalls require mandatory notification, manufacturers may be less likely to formally notify borderline ‘safety’ fixes, or may circumvent the process by bundling safety (including security) with non-safety “updates” - mimicking smartphone industry practice. Such updates are quietly cheap, but may degrade “pre-market” safety and security by design approaches.<sup>1118</sup> It also raises a question of increasing manufacturer control – over the product, its operation and performance data, consumer product information and over defect transparency and fixes – which may potentially diminish regulatory oversight, consumer information and the product liability regime itself. Indeed, consumer stakeholders argue that the law does not clearly incentivize design safety prioritisation, and that the regime is too reactively reliant upon post-market mechanisms; rather than pre-market legal incentives. Graphic 4.1 shows Australian reliance upon post-market recall is significant and contrasts the significantly-larger UK market to illustrate that a general safety provision appears to incentivize pre-supply safety.<sup>1119</sup>

---

<sup>1116</sup> Australian Government and ACCC, ‘Product Safety Australia’ (n.d. accessed 6 Mar 2017)

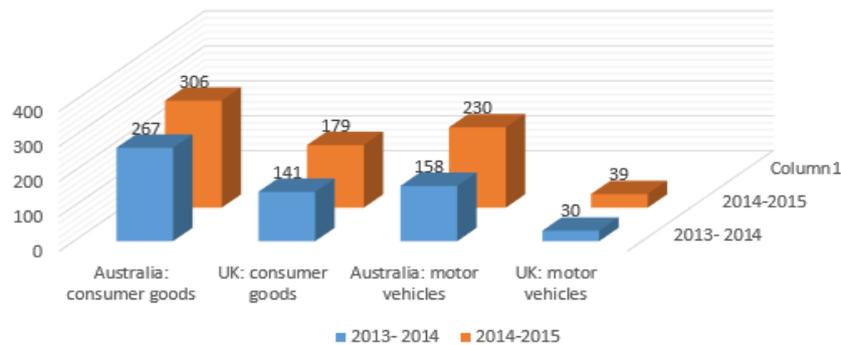
<<http://www.productsafety.gov.au/recalls?source=recalls>>

<sup>1117</sup> From 5 (2013) to 12 (2015, 2016). Note that only “safety-related” recalls are counted. From the author’s experience in the car industry, manufacturers apply rigorous assessment processes in making that determination. Less serious fixes with no “safety” element are often conducted by “field actions” or the like.

<sup>1118</sup> While this seems logical, it should be noted that product testing will become infinitely more efficient and accurate using computer simulations based upon real-time vehicle data. However, most of that data is accrued post product release, which is precisely the point. Consider for example, the Google minor crash which led to a rerun of software to learn from the car’s “mistake”. Overall however, testing and fix resolution time should improve.

<sup>1119</sup> CHOICE suggest that Australia’s recall rate is “abnormally high”, justifying adoption of a UK-style general safety provision: CHOICE Submission Table 2, cited in CAANZ, Interim Report, above n 840: 73. It may be that the rate positively reflects post-supply recall assessment practices, absent the pre-supply ‘safety provision’ which in the UK incentivizes safety pre-supply, so reduces that necessity. What is incontrovertible, is that a safety provision provides a clear incentive to manufacturers, suppliers and importers (deemed manufacturers).

## Consumer recalls: Australia & United Kingdom comparison



Graphic: 4.1 Consumer recalls: Australia & UK comparison  
 Source: Author-adapted from CHOICE data<sup>1120</sup>

Given the changing market context and the emerging role of hybrid CIOT products, reliance upon post-market mechanisms such as voluntary manufacturer recall may become a critical weakness in preventing consumer information asymmetry, ensuring manufacturer transparency and in incentivising safety by design. These weaknesses may be addressed through inserting a general safety provision into the ACL, to oblige manufacturer/ suppliers to only place “safe” products in the market,<sup>1121</sup> and to support existing safety-premised provisions as to ‘acceptable quality’ and the defective goods regime.

Further, regulators may need to adapt their role to scrutinise data handling and software updating practices, and to reduce increasing informational asymmetry by ensuring continued consumer and regulator ‘recall’ notification and regulatory capacity to oversee the market.

These issues and others are fleshed out further through the following smart car hypothetical.

<sup>1120</sup> CHOICE Submission Table 2, cited in CAANZ, Interim Report, above n 840: 73.

<sup>1121</sup> This terminology reflects the European Commission General Product Safety Directive (EC GPSD). Capturing the ‘supply chain’ reflects the need to incentivize all players to report back product issues and consumer feedback, and to have responsibility commensurate with their role in the product distribution process. See Ministerial Council of Consumer Affairs, ‘Review of the Australian Consumer Product Safety System’ *Options Paper* (Aug 2005 accessed 2 Nov 2016) <<http://www.pc.gov.au/inquiries/completed/product-safety/optionspaper>>

#### 4.6.1 A smart(ish) car hypothetical: Tesla Model S<sup>1122</sup>

““What we’ve got will blow people’s minds, it blows my mind...” – Elon Musk<sup>1123</sup>

This discussion borrows from real facts and rumours surrounding a tragic 2016 Tesla US fatality. Multiple long-running investigations<sup>1124</sup> have concluded that Tesla has no liability nor was there a ‘safety defect’ under US law; as such this discussion is **strictly hypothetical only**.<sup>1125</sup> Systems are as publicly described at the time of the accident.<sup>1126</sup> Tesla have since released APv8 (+) software, which Elon Musk says, would avoid the accident which killed Joshua Brown.<sup>1127</sup>

##### (a) What was (smart system) Autopilot as at May 2016?

Autopilot is a computer-controlled safety system designed to enable highway driving without drivers steering, braking or accelerating.<sup>1128</sup> It changes lanes upon driver signal, and has four elements: a forward

---

<sup>1122</sup> Tesla’s Model S is a beautifully elegant, electric passenger motor vehicle. It is a leading smart(ish) car on road, and is supplied into Australia.

<sup>1123</sup> Fred Lambert, ‘Elon Musk on Tesla fully autonomous car: ‘What we’ve got will blow people’s minds, it blows my mind... it’ll come sooner than people think’ *Electrek Blog* (3 Aug 2016 accessed 10 Aug 2016) <<https://electrek.co/2016/08/03/elon-musk-tesla-fully-autonomous-car-blows-mind/>>

<sup>1124</sup> The accident was investigated by the Florida Highway Patrol, the National Transportation Safety Board (NTSB) and the NHTSA Office of Defects Investigation.

<sup>1125</sup> One media report suggests that charges are likely to be laid against the truck driver, but this had not occurred as at 2016 end. The US Securities and Exchange Commission is also allegedly investigating Tesla for possible securities law breach in failing to disclose the fatal crash to investors as an event “material” to the share price, or a development a reasonable investor would consider important to the share value. Note that \$2 billion in stock was sold on 18 May after the crash but Tesla asserts that it only retrieved the vehicle data that same day after it sent a representative to retrieve the data. Again, the crash type limited Tesla’s capacity to retrieve vehicle data remotely, and Tesla claim that their investigation did not conclude until the end of May- after the financing round had occurred: Jean Eaglesham, Mike Spector and Susan Pulliam, ‘Tesla Owners Sue Over ‘Half-Baked’ Autopilot Software’ *The Wall Street Journal* (11 Jul 2016 accessed 6 Aug 2016) <<https://www.wsj.com/articles/sec-investigating-tesla-for-possible-securities-law-breach-1468268385>>

<sup>1126</sup> As at April 2017, the second-generation Autopilot has 8 cameras, all-around ultrasonic sensors, and a forward-looking radar. The new car systems are obviously upscaled upon those from just 12 months before: Fred Lambert, ‘Tesla updates data sharing policy to include collecting video in order to ‘make self-driving a reality’ *electrek* (6 May 2017 accessed 10 May 2017) <<https://electrek.co/2017/05/06/tesla-data-sharing-policy-collecting-video-self-driving/>>

<sup>1127</sup> See for commentary, Nick Whigham, ‘Tesla Autopilot update to improve ‘probability of safety,’ Musk says’ (12 Sept 2016 accessed 12 Sept 2016) <<http://www.news.com.au/technology/innovation/motoring/tesla-autopilot-update-to-improve-probability-of-safety-musk-says/news-story/70cfa99decd5209c4b52b0887a3e3e69>> A putative class action was filed in April 2017 as to the updated 2016-2017 models that allegedly contain “inoperative standard safety features, as well as faulty enhanced autopilot software for which customers paid a premium.” The complaint is that Tesla sold vehicles with self-driving hardware and charged customers for the software, which despite projections to the contrary has not yet been released As such vehicles are sub the previous model in terms of functionality: *Sheikh, Kelner and Milone & Ors v. Tesla Inc dba Tesla motors Inc*, Class Action Complaint for Violation of State Consumer Fraud Acts, Fraud by concealment and Unjust enrichment, United States District Court Northern District of California, Case No 5:17- cv -02193 (Filed 19 Apr 2017) <<https://electrek.co/2017/04/19/tesla-owners-class-action-lawsuit-tesla-autopilot-2-0/>>

<sup>1128</sup> **The Manual reviewed here is no longer the relevant version** – see Tesla Motors, ‘Model S Owner’s Manual US v 8’ (2016 accessed 2 May 2017)

<<[https://www.tesla.com/sites/default/files/model\\_s\\_owners\\_manual\\_north\\_america\\_en\\_us.pdf](https://www.tesla.com/sites/default/files/model_s_owners_manual_north_america_en_us.pdf)>> describes Driver Assist components to include front and rear bumper ultrasonic sensors, a forward-looking windshield camera and front grill radar, plus electrically-assisted brakes and steering systems. Tesla Motors, ‘Model S Owner’s Manual v 5.9’ (2015 accessed 22 May 2016): 65 <[https://forums.tesla.com/en\\_AU/forum/forums/new-owners-manual](https://forums.tesla.com/en_AU/forum/forums/new-owners-manual)>

long-range radar,<sup>1129</sup> a forward-facing camera with image-recognition software, 12 ultrasonic around-car sensors sending high-frequency pulses to detect objects,<sup>1130</sup> and a satellite-connected GPS feeding location data, speed limits, etc. to the vehicle computer.<sup>1131</sup> In the Manual, it is not a “safety feature”;<sup>1132</sup> it is a “convenience feature...to reduce driver workload”.<sup>1133</sup> For consumers, the difference is significant, from the name itself, to the “limitations”, “warnings” and vehicle alerts attached to its use and the general ‘safety’ entailed by those systems individually and overall.

(b) *Causation*

Marketed as the “safest car on the road”<sup>1134</sup> with Autopilot “beta technology” to make highway driving “not only safer, but stress free...”,<sup>1135</sup> Tesla quickly blogged its accident explanation:

“...a tractor trailer<sup>1136</sup> drove across the highway perpendicular to the Model S. Neither Autopilot nor the driver noticed the white side of the tractor trailer against a *brightly lit sky*, so the brake was *not applied*. The high ride height of the trailer combined with its positioning across the road and the extremely rare circumstances of the impact<sup>1137</sup> caused the Model S to pass under the trailer...<sup>1138</sup> [author emphasis]

---

<sup>1129</sup> It ranges up to 525 feet.

<sup>1130</sup> It ranges up to 16 feet.

<sup>1131</sup> Tesla, USA Today Research, as to the Model S, cited at Alexandra Mosher, ‘Tesla drivers play Jenga, sleep, using Autopilot in nerve-wracking videos’ USA TODAY (5 Jul 2016 accessed 6 Jul 2016) <<http://www.usatoday.com/story/tech/news/2016/07/01/drivers-play-jenga-sleep-using-tesla-autopilot-nerve-wracking-videos/86613484/>>

<sup>1132</sup> These are Lane Assist, Collision Avoidance Assist and Speed Assist.

<sup>1133</sup> Tesla Manual, above n: 1128: 67. Elements include Traffic Aware Cruise Control, Auto steer, Auto lane change, Auto park and Auto High Beam Headlights.

<sup>1134</sup> Tesla Motors Inc., Website (AU) (accessed 2 Sept 2016) [https://www.tesla.com/en\\_AU/models?redirect=no](https://www.tesla.com/en_AU/models?redirect=no) It has a five star safety rating from the NHTSA and ANCAP, and is ranked 99/ 100 points by US Consumer Reports.

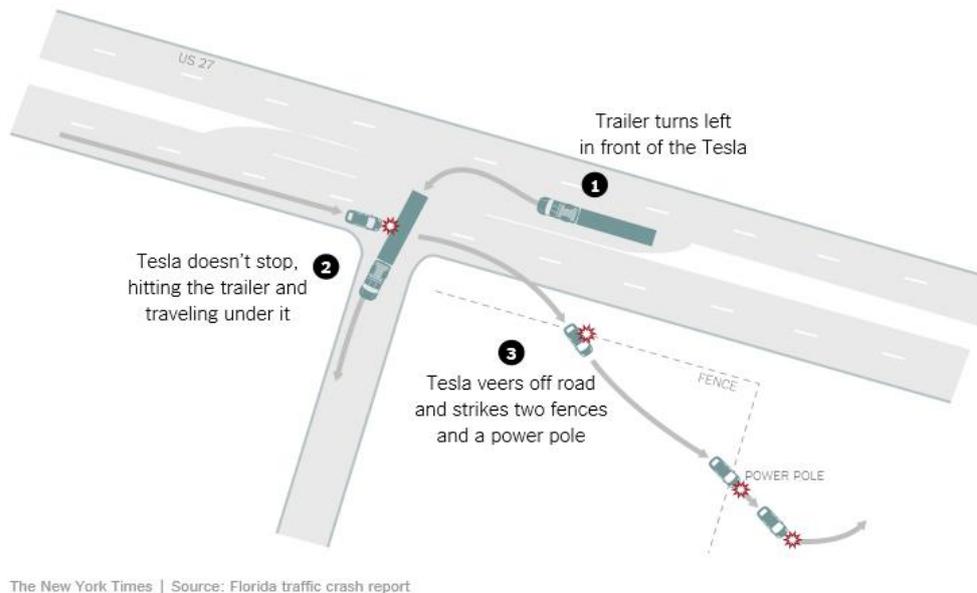
<sup>1135</sup> Tesla Motors Inc, Website (AU) (accessed 2 Sept 2016) <[https://www.tesla.com/en\\_AU/models?redirect=no](https://www.tesla.com/en_AU/models?redirect=no)>

<sup>1136</sup> In the US, this means an articulated truck.

<sup>1137</sup> Tesla claim: “Had the Model S impacted the front or rear of the trailer, even at high speed, its advanced crash safety system would likely have prevented serious injury as it has in numerous other similar incidents”: The Tesla team, ‘A Tragic Loss’ (30 Jun 2016 accessed 3 Jul 2016) <[https://www.teslamotors.com/en\\_AU/blog/tragic-loss](https://www.teslamotors.com/en_AU/blog/tragic-loss)>

<sup>1138</sup> Ibid.

The car was traveling on US27 at 74 mph (120 km); nine miles (15 km) over the speed limit.<sup>1139</sup> The brakes were not activated.<sup>1140</sup> Witnesses claim that they heard a dvd playing in the wreckage. Tesla describe the accident as a “statistical inevitability” for driver assist technology,<sup>1141</sup> though Autopilot should brake in response to “...any interruption of the ground plane in the path of the vehicle that cross-checks against a consistent radar signature,”<sup>1142</sup> In other words, despite multiple component technologies - cameras, radar and ultrasonic sensors, GPS and Tesla real-time connectivity - Autopilot did not ‘see’ a 16-wheel truck and failed to brake.<sup>1143</sup>



Graphic: 4.2 Florida traffic crash report  
Source: Florida Traffic Police<sup>1144</sup>

<sup>1139</sup> The NTSB investigation confirmed the speed despite witness’s assertions it was travelling at “high speed”. Frank Baressi was the driver of the other vehicle claimed that the car went “...so fast through my trailer I didn’t see him.” Another driver claims the car passed her earlier on the same highway when she was doing 85 mph (137 kmh): Teslarati, ‘Witnesses reveal new details behind deadly Tesla accident in Florida’ (1 Jul 2016 accessed 4 Jul 2016) < <http://www.teslarati.com/witnesses-details-deadly-tesla-accident/>> After the fatal collision, it travelled “hundreds of yards from the point of impact” through fences off road until colliding with a power pole: National Transport Safety Board, ‘Preliminary Report, Highway HWY16FH018’ (26 Jul 2016 accessed 2 Aug 2016) <<http://www.nts.gov/investigations/AccidentReports/Pages/HWY16FH018-preliminary.aspx>>. See also Neal E. Boudette, ‘Tesla Faults Brakes, but Not Autopilot, in Fatal Crash’ *The New York Times* (29 Jul 2016 accessed 2 Aug 2016) <[http://www.nytimes.com/2016/07/30/business/tesla-faults-teslas-brakes-but-not-autopilot-in-fatal-crash.html?\\_r=0](http://www.nytimes.com/2016/07/30/business/tesla-faults-teslas-brakes-but-not-autopilot-in-fatal-crash.html?_r=0)>; Teslarati, ‘Witnesses reveal new details behind deadly Tesla accident in Florida’ (1 Jul 2016 accessed 4 Jul 2016) < <http://www.teslarati.com/witnesses-details-deadly-tesla-accident/>>

<sup>1140</sup> Tesla later retrieved accident data manually on 15 June, as the vehicle did not transmit it, presumably as its roof was sheared off in the accident.

<sup>1141</sup> Tesla Motors Inc., ‘Misfortune’ *The Tesla Team* (6 July 2016 accessed 10 July 2016) < [https://www.tesla.com/en\\_AU/blog/misfortune](https://www.tesla.com/en_AU/blog/misfortune)>

<sup>1142</sup> Ibid. Auto Pilot has been available by software update (at additional cost) since January 2016 only. Tesla say that “the high, white side of the box truck” failed to interrupt the vehicle ground plane and according to Elon Musk on twitter, “combined with a radar signature... very similar to an overhead sign, caused automatic braking not to fire”: <https://twitter.com/elonmusk/status/748625979271045121>

<sup>1143</sup> Contrary to the Blog explanation, one media report suggests that in evidence to the Senate Commerce Committee, Tesla have asserted the accident was caused by a brake system failure, which they regard as separate from Auto Pilot: Boudette, above n 1139.

<sup>1144</sup> The Florida Highway Patrol report is here: Anjali Singhvi and Karl Russell, ‘Inside the Self-Driving Tesla Fatal Accident’ (updated 12 July 2016 accessed 2 Aug 2016) <<https://www.nytimes.com/interactive/2016/07/01/business/inside-tesla-accident.html>>; Anjali Singhvi and Karl Russell, ‘Inside the Self-Driving Tesla Fatal Accident’(UPDATED July 12, 2016

(c) *Applying the ACL*

Using the above accident causation,<sup>1145</sup> the following ACL questions arise:

- Did the vehicle have a safety defect under section 138?
- Do any of the defences under section 142 apply?
- Was the vehicle of 'acceptable quality' and 'fit for purpose' under the consumer guarantees?
- Did Tesla's Manual, in-car systems, marketing and other public representations breach sections 18 and/ or 29?

These first two are discussed in turn, although evidentially there is factual overlap between all four.

(d) *Section 138 "A safety defect"*

*"Just putting a sticker on it saying 'customer is responsible' is a nightmare..."<sup>1146</sup>*

Model S is a hybrid software/ physical good and has a safety defect if its safety is not such as persons generally are entitled to expect<sup>1147</sup> having regard to their marketing, any instructions or warnings, what might reasonably be expected to be done with them and the time of supply.<sup>1148</sup> The test is objective and the court asks what members of the requisite class<sup>1149</sup> to whom the product is marketed or directed, would "expect". This does not mean a car must be entirely free of risk,<sup>1150</sup> nor does it excuse a driver from taking "reasonable [care]".<sup>1151</sup> It requires a causal link between the alleged defect and injury,<sup>1152</sup> which may be *instructional, performance and/ or design-based*.<sup>1153</sup> For example, the designed interplay between the sensors failed to detect the truck and despite manual informational warnings as to "bright

---

accessed 2 Aug 2016) <<https://www.nytimes.com/interactive/2016/07/01/business/inside-tesla-accident.html>>; Jordan Golson, 'Read the Florida Highway patrol's full investigation into the fatal Tesla crash' *The Verge* (1 Feb 2017 accessed 20 Feb 2017) <<http://www.theverge.com/2017/2/1/14458662/tesla-autopilot-crash-accident-florida-fatal-highway-patrol-report>>

<sup>1145</sup> Absent any independent human, environmental or third party contribution and ignoring common law actions and Australian compulsory motor vehicle accidents schemes: such as the fault-based common law tort of negligence (for the manufacture or supply of faulty goods and services); and in contract, the supply of goods in breach of express or (common law) implied warranties.

<sup>1146</sup> Olivia Solon, 'Should Tesla be 'beta testing' autopilot if there is a chance someone might die?' *The Guardian* (7 Jul 2016 accessed 2 Aug 2016) <https://www.theguardian.com/technology/2016/jul/06/tesla-autopilot-fatal-crash-public-beta-testing>>

<sup>1147</sup> ACL section 9.

<sup>1148</sup> ACL section 9(2) (a) – (f).

<sup>1149</sup> The class will consist of those to whom the product is marketed /directed, and includes the "astute and the gullible, the intelligent and the not so intelligent, the well-educated and the poorly educated": Campomar, *Ibid*.

<sup>1150</sup> *Merck Sharpe and Dohme (Australia) Pty Ltd v Petersen* [2011] FCAFC 128; (2011) 196 FCR 145

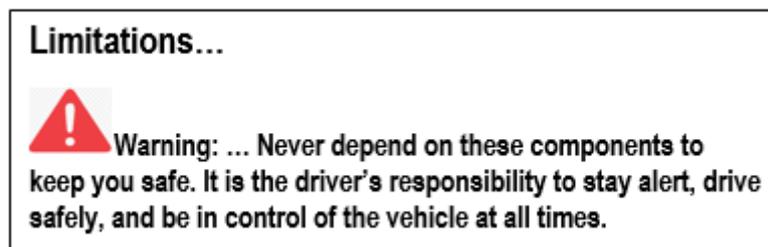
<sup>1151</sup> *Ransley v Black & Decker (A'asia) Pty Ltd* (1977) TPR 138 per Smithers, J at page 140.

<sup>1152</sup> *Carey-Hazell v Getz Bros and Co (Aust) Pty Ltd* [2004] FCA 853; [2004] ATPR 42-014.

<sup>1153</sup> The ACL Explanatory Memorandum describes three types of safety defect: design defects as those relating form, structure and composition; manufacturing defects are those which relate to the construction or assembly process, and instructional or warning defects are those caused by incorrect or inadequate product warnings or instructions: Cth of Australia, 'Explanatory Memorandum', Trade Practices Amendment Bill 1992' (Cth): 8.

light”,<sup>1154</sup> or mandating driver attention, would persons generally expect that the system would ‘see’ such a truck and apply (Auto)brake? It is a complex question.

Tesla’s Manual and numerous in-car systems describe Autopilot as driver assist only and warn drivers to remain in control. A manual may render a product defective in Australia if its instructions were unclear or inadequate,<sup>1155</sup> and causally related to the crash. Critics would argue that the Manual is too long, the non-exhaustive ‘bright light’ warning was inaccurate on the facts and Tesla alert systems were not ‘state of the art’ as known to Tesla (at least) - as evidenced by v.8 improvements.<sup>1156</sup>



Graphic 4.3 Limitations warning

Source: Author adapted from (former) Tesla Model S Manual<sup>1157</sup>

As to their marketing, there is an argument that Tesla over-hyped Autopilot: the name is hyperbolic<sup>1158</sup> and connotes autonomous<sup>1159</sup> systems capability from which the Manual, in-car and vehicle “warnings’

---

<sup>1154</sup> Tesla’s then applicable manual contained some long and unusual “non-exhaustive” “limitations” as to “driver assist”: including poor visibility caused by snow, fog, heavy rain; damage or obstructions caused by ice, mud or snow; narrow or winding roads; bumper damage or misalignment; ultrasonic wave interference; and extremely cold or hot temperature.

<sup>1155</sup> If the manual were instructionally defective, that is sufficient for both the manual and vehicle to be defective: *McDermott v Robinson Helicopter Company* [2014] QSC 34. As to the required causal connection see *Merck Sharp & Dohme v Peterson* [2011] FCAFC 128

<sup>1156</sup> These include more frequent steering wheel alerts, and turning off the AP system requiring the driver to stop the car and restart it. From youtube videos, the previous system has some time between alerts in highway conditions, such that quite long videos showed drivers hands-off the wheel. See for example this 2015 test drive:

<https://www.youtube.com/watch?v=DbPqIHwSHos> Note the driver is using AP in non-highway conditions which is contrary to manufacturer recommendations. As such it illustrates consumer over-confidence.

<sup>1157</sup> It is unclear if this Manual was current as at June 2016. It is thus used illustratively, as it provides Tesla’s warnings at some stage as to appropriate AP warnings. Note there are also in-car warnings, which the author has only viewed via youtube, so these are not expressly commented upon. A court would consider ALL warnings likely to have been seen by drivers collectively, and may find that even if drivers rarely read the Manual and even if the Manual was not instructively defective, the in-car warnings and alert-systems should have been sufficient. There is certainly an arguable case as to this. Note the driver (who was a Tesla aficionado) represented by his family will not apparently take legal action, though it seems likely this decision would be made post the NHTSA final report. Further the insurer may either avoid the claim alleging driver 100% contribution, or sue Tesla: Dana Hull, ‘Tesla owner in Autopilot crash won’t sue, but car insurer might’ *Automotive News, Bloomberg* (2016 accessed 28 Aug 2016) <<http://www.autonews.com/article/20160819/OEM06/160819822/tesla-owner-in-autopilot-crash-wont-sue-but-car-insurer-might>>

<sup>1158</sup> Consumer Reports describes the name as “exaggerated” not descriptive and warns that consumers are being sold “a pile of promises about unproven technology”: [US] Consumer Reports, ‘Tesla’s Autopilot: Too Much Autonomy Too Soon’ (14 Jul 2016 accessed 16 Jul 2016) <<http://www.consumerreports.org/tesla/tesla-autopilot-too-much-autonomy-too-soon/>> The systems which make up Auto pilot likewise use exaggerated terminology given the extent of use warnings attached to their operation: Traffic-Aware Cruise Control, Autosteer, Auto Lane Change, Autopark, and Auto High Beam.

<sup>1159</sup> Dictionary.com “autopilot,” in Collins English Dictionary - Complete & Unabridged 10th Edition. Source location: HarperCollins Publishers. <http://www.dictionary.com/browse/autopilot>. Available: <http://www.dictionary.com/>. Accessed: August 23, 2016.

then retreat. Elon Musk's public representations: "We tell drivers to keep their hands on the wheel just in case, to exercise caution in the beginning" and in good road conditions "...people may [remove their hands from the steering-wheel], but we don't advise that,"<sup>1160</sup> are lukewarm "warnings" at best.<sup>1161</sup> Some consumers allege hands-and-feet-off<sup>1162</sup> vehicle demonstrations and YouTube is peppered with consumers driving hands-off, which the media reported<sup>1163</sup> and of which Tesla is likely to have been aware. Consumer Reports (US) warned: "...consumers are being sold a pile of promises about unproven technology".<sup>1164</sup>



Graphic 4.4 Tesla Australian website  
Source: © Tesla Motors Inc., AU website, 2 December 2016<sup>1165</sup>

Competitors are even more critical and "beta software" is an oft-used basis for attack. In IT circles, this means pre-release software in test phase, (often) supplied on a no liability basis<sup>1166</sup> - a concept foreign

<sup>1160</sup> Fred Lambert, 'Tesla reveals all the details of its 'Autopilot' and its software v7.0 [slide presentation and audio conference]' *Electrek* (14 Oct 2015 accessed 2 Aug 2016) < <https://electrek.co/2015/10/14/tesla-reveals-all-the-details-of-its-autopilot-and-its-software-v7-0-slide-presentation-and-audio-conference/>>

<sup>1161</sup> Mr Musk is a hugely successful thought-leader internationally. He attracts great media attention as a result: Sam Levin, Julia Carrie Wong and Nicky Woolf, 'Elon Musk's self-driving evangelism masks risk of Tesla autopilot, experts say' *The Guardian* (2 Jul 2016 accessed 2 Jul 2016) < <https://www.theguardian.com/technology/2016/jul/02/elon-musk-self-driving-tesla-autopilot-joshua-brown-risks>> Interestingly in August 2016 he announced an intention to wind back his public/ media work to focus back on his businesses.

<sup>1162</sup> Ronan Glon 'Tesla owner blames Autopilot crash on bad marketing' *Leftlanenews* (11 Aug 2016 accessed 30 Aug 2016) < <http://www.leftlanenews.com/tesla-owner-blames-autopilot-crash-on-bad-marketing-92530.html>>

<sup>1163</sup> See for example, Davies, Alex, 'Obviously drivers are already abusing Tesla's Autopilot' (Oct 2015 accessed 20 Nov 2016) < <https://www.wired.com/2015/10/obviously-drivers-are-already-abusing-teslas-autopilot/>> and the videos listed here: Mui, Chunka, 'Is Tesla Racing Recklessly Towards Driverless Cars?' *Forbes* (19 Apr 2016 accessed 26 May 2016) < <http://www.forbes.com/sites/chunkamui/2016/04/19/is-tesla-reckless/#4f9b968c1a26>> See also Mosher, above n 1124. It is also reported that one of the videos was uploaded (purportedly) by Elon Musk's wife, Tallulah Riley- see [https://www.youtube.com/watch?v=iMilP6\\_YFbM](https://www.youtube.com/watch?v=iMilP6_YFbM) : Sam Levin and Nicky Woolf, 'Tesla driver killed while using autopilot was watching Harry Potter, witness says' *The Guardian* (2 Jul 2016 accessed 2 Jul 2016) < <https://www.theguardian.com/technology/2016/jul/01/tesla-driver-killed-autopilot-self-driving-car-harry-potter>>

<sup>1164</sup> Above n 1158.

<sup>1165</sup> Tesla Motors Inc., AU website, 2 December 2016 < [https://www.tesla.com/en\\_AU/models](https://www.tesla.com/en_AU/models)>

<sup>1166</sup> '...quality-control technique in which hardware or software is subjected to trial in the environment for which it was designed, usually after debugging by the manufacturer and immediately prior to marketing.' Dictionary.com "beta-test," in

to the automotive industry. Even assuming Tesla owners are more IT-savvy than average vehicle purchasers, the term is confusing: is it a test phase version so less safe, or as Musk asserts, an extensively internally-validated system<sup>1167</sup> inaccurately described to reduce consumer complacency?<sup>1168</sup> The German *Federal Office for Motor Vehicles* (KBA) has stated that had it been the EU assessor, it would not approve a “beta-phase version”.<sup>1169</sup> A chorus of experts,<sup>1170</sup> industry commentators<sup>1171</sup> and consumer groups<sup>1172</sup> concur: one analyst claimed that “traditional car manufacturers would never introduce a technology like this without it being fully tested,”<sup>1173</sup> and an engineering professor, opined:

*“The general impression among competitors is that Tesla was jumping the gun. It was doing what computer companies do – putting the product out there when it’s not even close to perfect.”*<sup>1174</sup>

Product perfection is of course not a legal standard. The ACL is modified by defences, which are considered next.

---

Dictionary.com Unabridged. Source location: Random House, Inc. <http://www.dictionary.com/browse/beta-test>. Available: <http://www.dictionary.com/>. Accessed: August 23, 2016.

<sup>1167</sup> Elon Musk, ‘Master Plan, Part Deux’ Tesla Blog (20 July 2016 accessed 2 Aug 2016)

<[https://www.tesla.com/en\\_AU/blog/master-plan-part-deux](https://www.tesla.com/en_AU/blog/master-plan-part-deux)>

<sup>1168</sup> For a view supportive of Tesla, see Zachary Shahan, ‘What Does Tesla Autopilot “Beta” Mean?’ *CleanTechnica* (11 July 2016 accessed 2 Aug 2016) <https://cleantechnica.com/2016/07/11/tesla-autopilot-beta-mean/> Note the author is a Tesla investor and electric car (and environment) enthusiast.

<sup>1169</sup> It is reported by Reuters that the KBA told the German newspaper *Welt am Sonntag* this. European approvals were granted in the Netherlands: Reuters, ‘German Authority Would Not Have Approved Beta-Phase Tesla Autopilot’ (10 Jul 2016 accessed 2 Aug 2016) *Fortune* <http://fortune.com/2016/07/10/german-beta-phase-tesla-autopilot/> See also <http://ecomento.tv/2016/07/11/kba-untersucht-tesla-autopilot/>

<sup>1170</sup> See for example, the comments here: Chunka Mui, ‘Is Tesla Racing Recklessly Towards Driverless Cars?’ *Forbes* (19 Apr 2016 accessed 26 May 2016) < <http://www.forbes.com/sites/chunkamui/2016/04/19/is-tesla-reckless/#4f9b968c1a26>; Matthew Dolan, ‘Why experts worry about the Tesla crash’ *Detroit Free Press* (2 Jul 2016 accessed 6 Jul 2016) < <http://www.freep.com/story/money/cars/2016/07/01/experts-worry-tesla-crash/86611662/>>; Krauss, Eric B., ‘Driverless Cars and the Law – The Tesla Accidents’ *Husch Blackwell* (8 Jul 2016 accessed 10 Jul 2016) < <http://www.tmtindustryinsider.com/07-08-2016-driverless-cars-and-the-law-the-tesla-accidents/#page=1>>; Sam Levin, Julia Carrie Wong and Nicky Woolf, ‘Elon Musk’s self-driving evangelism masks risk of Tesla autopilot, experts say’ *The Guardian* (2 Jul 2016 accessed 2 Jul 2016) <<https://www.theguardian.com/technology/2016/jul/02/elon-musk-self-driving-tesla-autopilot-joshua-brown-risks>>

<sup>1171</sup> “One auto industry analyst claimed that “traditional car manufacturers would never introduce a technology like this without it being fully tested”: Solon, above n 1146.

<sup>1172</sup> Above n 1158; Mark Rehtin, ‘NHTSA Opens Investigation into Tesla Self-Driving Fatality: Crash underscores Consumer Reports’ concerns about beta testing self-driving technology on public roads’, (30 June 2016 accessed 16 Jul 2016) < <http://www.consumerreports.org/tesla/nhtsa-opens-investigation-into-tesla-self-driving-fatality/>>

<sup>1173</sup> Solon, above n 1146.

<sup>1174</sup> Solon, above n 1146.

(e) ACL defences

Assuming a 'safety defect', defences may apply as follows:

Defence	Hypothetical facts and law	Outcome?
The defect did not exist at the time of manufacturer supply <sup>1175</sup>	The AP software was downloaded after vehicle delivery via an on-air activation update in January 2016.  Technically it did not exist when the vehicle was supplied in 2015. But as hybrid device/ software, it is a 'good' and as such the relevant supply date is when it was installed.	X
Defect caused by mandatory standard compliance	Not relevant	X
The state of the art defence: <sup>1176</sup>  The state of scientific or technical knowledge at the time supplied, was not such as to enable the safety defect to be discovered. <sup>1177</sup>  <i>This means that objectively,<sup>1178</sup> it was not such as to enable "anybody" to discover the defect.<sup>1179</sup></i>  <i>No adverse inference is drawn ONLY because the</i>	The test is not subjective. Given the accident scenario is a common driving situation, 'anybody' testing the vehicle under that normal situation could have discovered it.  Manual warnings suggest Tesla were aware of issue(s) with 'white light', but is it reasonable to expect consumers to appreciate how that issue might arise or to view what occurred as within that warning?  Consumers were warned to be alert – but vehicle reminder systems did not comport to the (highest) art at the time and have since been improved in v. 8. <sup>1182</sup> No adverse inference applies.	Possible defence

<sup>1175</sup> Note the ACL definition as to manufacturer includes importers as deemed manufacturers, save for determining this question – the date of supply by the (real) manufacturer is the relevant date: ACL s. 7.

<sup>1176</sup> ACL section 142(c). Others include a defect (b) only due to compliance with a mandatory standard; (d) if the defect is attributable only to the design of other goods (i.e. a component), or their markings or instructions or warnings given by another manufacturer, where the safety defect is comprised in other goods.

<sup>1177</sup> The defence succeeded in two cases: as to a drug Vioxx which doubled the risk of heart attack, something unknown at the time of supply and the state of the art (scientific and medical knowledge) did not enable its discovery: Peterson, above n 57. In *Graham Barclay Oysters Pty Ltd v Ryan* [2000] FCA 853, an action alleging the supply of contaminated oysters failed as technical knowledge at the time did not allow the defect to be discovered without destroying the oysters.

<sup>1178</sup> *Merck Sharp & Dohme (Australia) Pty Ltd v Peterson* [2011] FCAFC 128; (2011) 196 FCR 145.

<sup>1179</sup> The explanatory memorandum to the *Trade Practices Amendment Bill 1992*, cited in Merck case, *Ibid*.

<sup>1182</sup> See the testimony of Dr Mary (Missy) Louise Cummings, above n 394. She explains behavioural traits which may make consumers too complacent, such as behavioural adaptation and over-reliance, informational deficits, risk over-compensation, distraction, skill loss and driver vision research.

<p><i>standard adopted was not the “safest possible,<sup>1180</sup> or ONLY because Tesla later supplied safer goods.<sup>1181</sup></i></p>	<p>Driver vision research of which manufacturers should be aware suggests that the side-on tray truck crash scenario is a “well-known perceptual problem for human drivers”, so should have been a foreseeable issue for Tesla in its design and safety assessments.<sup>1183</sup></p>	
<p>If the goods were comprised in other goods, the defect is attributable to the design; or markings; or instructions and warnings given by the manufacturer of those other goods.</p>	<p>Tesla’s AP technology used (and possibly adapted, though reports are unclear) Mobileye technology, so this argument is likely more apposite were an action commenced against Mobileye. It illustrates a complex design chain, and how this defence might operate.</p> <p>After Tesla’s published accident explanation, Mobileye publicly denied that its system should have ‘fired’ at all:<sup>1184</sup></p> <p><i>Today’s collision avoidance technology, or Automatic Emergency Braking (AEB) is defined as rear-end collision avoidance, and is designed specifically for that. This incident involved a <b>laterally crossing vehicle</b>, which current-generation AEB systems are not designed to actuate upon.<sup>1185</sup></i></p> <p>Mobileye has since claimed it “expressed safety concerns regarding the use of Autopilot hands-free” to Elon Musk”.<sup>1186</sup> It has since ended their relationship because Tesla AP marketing and warnings were sending “mixed messages” and their design was “pushing the envelope in terms of safety”.<sup>1187</sup></p> <p>The author could not find any warning to consumers that AP was limited to rear-end collision avoidance only. Note that Tesla instruct that drivers must always</p>	<p>Unlikely</p>

<sup>1180</sup> ACL section 9 (4).

<sup>1181</sup> ACL section 9(3).

<sup>1183</sup> Michael Flanagan, Research Associate Professor in human factors Group at U-M Transportation research Institute who researches driver vision, cited Ibid.

<sup>1184</sup> Golson, above n 1143.

<sup>1185</sup> Streetinsider, ‘Mobileye (MBLY) Issues Statement on Fatal Tesla (TSLA) Model S Autopilot’ (1 Jul 2016 accessed 15 Jul 2016)

[http://www.streetinsider.com/Corporate+News/Mobileye+\(MBLY\)+Issues+Statement+on+Fatal+Tesla+\(TSLA\)+Model+S+Autopilot+Crash/11793789.html](http://www.streetinsider.com/Corporate+News/Mobileye+(MBLY)+Issues+Statement+on+Fatal+Tesla+(TSLA)+Model+S+Autopilot+Crash/11793789.html) The statement goes on to indicate the system will include “ Lateral Turn Across Path (LTAP) detection capabilities beginning in 2018, and the Euro NCAP safety ratings will include this beginning in 2020”. Note that Mercedes Benz warn against their PRESAFE® brake system not reacting to “crossing traffic” using the WARNING symbol in their C-Class Model Manual: Daimler AG, C-Class Owner’s Manual at page 87: Author’s own (2016).

<sup>1186</sup> Dana Hull, ‘Tesla Breakup with Mobileye Turns Ugly’ *Bloomberg* (16 Sept 2016 accessed 20 Sept 2016)

<<https://www.bloomberg.com/news/articles/2016-09-16/tesla-says-mobileye-tried-to-block-its-auto-vision-capability>>

<sup>1187</sup> Eric Auchard and Tova Cohen, ‘Mobileye says Tesla was ‘pushing the envelope in terms of safety’ (14 Sept 2016 accessed 20 Sept 2016) *Reuters* <http://www.reuters.com/article/us-mobileye-tesla-idUSKCN11K2T8> Note Tesla issued a statement that Mobileye could not keep pace with their product changes.

	<p>remain in control and alert as AP is driver assist technology only.</p> <p>Consumer groups had called for Tesla to change the AP name given its aircraft connotations imply self-driving.</p>	
--	--	--

Table 4.1 ACL defences applied to certain facts  
Source: author

As the table suggests, the defences require a factually complex analysis and judgement as to the balance of evidence. Some of the relevant factors as to ‘state of the art’ were considered by US regulators, but it remains possible that an Australian court, considering Part 3-5, might take a different view.

*(f) Reality Check: the (real) resolution*

Tesla has no liability under US public law. Both regulatory investigations<sup>1188</sup> absolved Tesla, finding a crash attributable to human error caused by a truck driver, who entered the highway to turn right- perhaps expecting a speeding driver to slow a little in deference to size. As Tesla’s data showed, Autopilot was on, the braking system did not warn or deploy, and the driver took no avoidance action. The NHTSA (ODI) examined if Tesla systems “may not function as designed, increasing the risk of a crash...”<sup>1189</sup> It concluded that there were no defects in design or performance, finding that Tesla’s system complied with the rear-end collision avoidance technology industry standard in 2016, and was not designed to perform in “all crash modes, including crossing path collisions”.<sup>1190</sup> They benchmarked other manufacturers, concluding that none had cross-vehicle collision avoidance, without inferring Tesla’s leading market position as early-tech-release innovator.<sup>1191</sup> The implicit message is that so long as

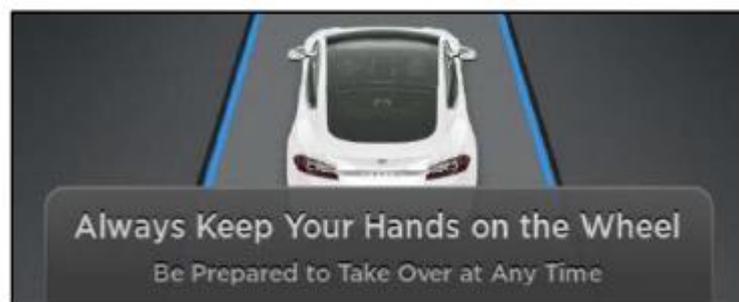
<sup>1188</sup> United States Department of Transport, NHTSA, ‘ODI Resume Investigation PE 16-007 re Tesla Motors Inc.’ (19 Jan 2017 accessed 22 Jan 2017) <<https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.PDF>> (Tesla ODI Report). Note the ODI examined the following issues as to the design and performance of Tesla’s Autopilot system: “1) AEB design and performance in the subject Tesla and peer vehicles; 2) human-machine interface issues related to Autopilot operating mode; 3) data from crash incidents related to Tesla’s Autopilot and AEB systems; and 4) changes Tesla has implemented in the Autopilot and AEB systems”: 2.

<sup>1189</sup> Tesla ODI Report, *ibid*.

<sup>1190</sup> That conclusion relied upon a 2011 report which validated Tesla’s radar/ camera-based system, and voluntary industry agreement to make AEB ‘standard’ by 2022, both of which may be outdated given the rapid pace of current smart car developments such as lidar and the like: Tesla ODI Report; above n 1188: [2.2] Objective Tests for Imminent Crash Automatic Braking Systems Final Report Volume 1 of 2. (2011). DOT HS811 521. National Highway Traffic Safety Administration. Washington, DC.

<sup>1191</sup> At [2.2]: “ODI surveyed a dozen automotive manufacturers and several major suppliers to determine if the AEB capabilities in crossing path collisions had changed since the CAMP CIB project was completed. None of the companies contacted by ODI indicated that AEB systems used in their products through MY 2016 production were designed to brake

vehicles comply with overall industry levels - 'state-of-the-art' - then anyone who aims and markets higher has some performance latitude, so long as the driver remains in control. Secondly, the ODI concluded that as an Advanced Driving System only, it requires full driver attention to monitor and take crash avoidance action. This is consistent with Tesla manuals and in-car information, but arguably less consistent with certain marketing representations and consumer expectations, which are of import to 'safety' expectations under the ACL. The ODI also noted that other jurisdictions dislike the name 'Autopilot' but that was beyond scope,<sup>1192</sup> which ignores an implied systems-capability impression conveyed to consumers.<sup>1193</sup> It is perhaps an implicit ACL question to determine which consumers are more likely to see and remember: marketing and driving impressions, or systems warnings and Manual instructions.



***Figure 4. Dialog Box that Appears Every Time Autosteer is Activated.***

Graphic 4.5 Tesla vehicle dialog box  
Source: ODI Report page 6

Tesla's driver engagement system<sup>1194</sup> was improved by update v 8.0; but the ODI report suggests that it conformed to design and industry practice at the time of the accident. The public policy interest in drawing no adverse inference appears also in the ACL. But again, this does not account for Tesla's market or marketing position: Tesla arguably represented its product as peer-leading which implies (re)setting the

---

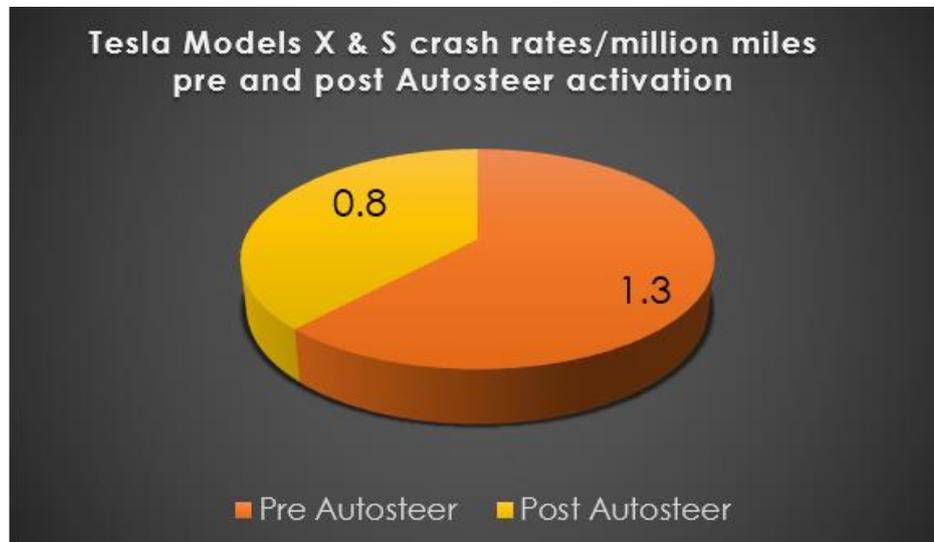
for crossing path collisions: Tesla ODI Report, above n 1188 :3. Note also that the technology exists at Google and Mercedes and other companies: they have just not yet approved it for consumer release.

<sup>1192</sup> Ibid: 3 at footnote 9

<sup>1193</sup> Ibid: 6. These are: 1) the owner's manual; 2) new software release notes, which refer to the owner's manual; 3) Autosteer user agreement required before first time use or post ignition cycles ending with Autosteer off; 4) a dialog box that appears every time Autosteer is activated reminding the driver to "Always keep your hands on the wheel" and "Be prepared to take over at any time" (Figure 4); 5) the user interface information, which appears at all times while driving - the blue shaded circle around the white steering wheel indicates Autosteer is in operation.

<sup>1194</sup> This is described as an "escalating series of warnings" as follows: (1) visual alert indicating that hands on the steering wheel are required; (2) If no response, an audible chime sounds after 15 seconds; then (3) A pronounced chime after 10 seconds; than (4) within five seconds, the vehicle gradually slows in the lane. (5) warnings stop when the driver's hands are detected and Autopilot operation resumes. Note v 8.0 has changed this to 'strike out' the system if the driver fails to respond.

mark. Finally, the accident data suggested uncommon but foreseeable<sup>1195</sup> “extended [driver] distraction” of up to seven seconds, which may constitute a safety defect, but the ODI accepted that design process, evaluation and testing justified finding otherwise.<sup>1196</sup> In conclusion, the ODI noted Tesla crash rates – which (remarkably) after Autosteer, dropped almost 40%:



Graphic 4.6 Tesla improved crash rates MY2014- 2016  
Source: Author using data from ODI Report, page 11.

The ODI concluded that Tesla had informed consumers that driver attention remains required, that Advanced Driving Systems are for rear-end collisions and have limitations... in a variety of ways – “although not as specific as it could be.”<sup>1197</sup> And drivers “should” read and heed warnings. It has closed its investigation, though reserved open findings as to whether a safety-related defect exists.

*(g) Hypothetical: a conclusion*

Joshua Brown was the first fatality in over 130 million miles driven by Tesla customers,<sup>1198</sup> when the US national fatality average is one per 94 million miles.<sup>1199</sup> Musk has argued an ethical duty to make AP available, asserting that Tesla’s autonomous technology saves lives:

---

<sup>1195</sup> In the US, an unreasonable risk arising from reasonably foreseeable owner “abuse” may constitute a safety-related defect: *United States v. Gen. Motors Corp.*, 518 F.2d 420, 427 (D.C. Cir. 1975) It is likely that a similar finding would be made here, as it implies a failure to warn scenario, or at least one where consumer instruction and warnings are inadequate.

<sup>1196</sup> *Ibid*: 10 [5.3].

<sup>1197</sup> *Ibid*: page 11.

<sup>1198</sup> The Tesla team, above n 1137. Note however that Rand Corporation suggest that verification that self-driving cars are “as safe” as human drivers, will require 275 million miles to be driven fatality free: Cummings, above n 394. See also Rand, above n 232.

<sup>1199</sup> While this sounds a safety improvement, it is not determinative. Statistics may occur in clusters – for example were there suddenly two more fatal Tesla accidents in quick succession, the safety calculation would reduce to one in 43 million miles –

*Once we get to the point where Autopilot is approximately 10 times safer than the US vehicle average, the beta label will be removed.*<sup>1200</sup>

There is no industry standard as to the “ten times” figure;<sup>1201</sup> nor is it binding, permanent or meaningful. Implied within the auto industry remit is the duty to take reasonable care, to design and test exhaustively for safety and to release products which “do no (foreseeable) harm”. Arguably, releasing a product disclaimed by impractical or obscure warnings, with permissive alert systems allowing non-recommended behaviors and which (it seems) were so rapidly, readily ‘fixable’, implies a deficiency in judgement, if not duty.<sup>1202</sup> However, car safety is always a matter of degree and hindsight has many benefits.<sup>1203</sup>

As this discussion suggests, the product liability provisions appear simple, but are evidentially difficult to establish and practically, rarely tested. In a ‘smart’ device context, this is exacerbated by complex technology, complicated causation and the human factor. It is impossible to know if there are few cases, or few because manufacturers and their insurers settle strong claims to avoid adverse judgements. Jurisprudentially it is not an optimal situation, as the indistinct ‘consumer expectation’ upon which Part 3-2 relies and the uncertain ‘state of the art’ defence reveal, nor do private settlements clarify the law, expose consumer detriment or signal market (safety) issues. It is yet another justification for a general safety provision to require that all consumer goods must be reasonably safe - to reinforce the safety-by-design culture implicit in section 9(2) and Part 3-5.

---

or half the national average. As such, the statistic alone does not evidence greater Tesla safety, nor does it point to accident responsibility.

<sup>1200</sup> Elon Musk, ‘Master Plan, Part Deux’ *Tesla Blog* (20 July, 2016 accessed 2 Aug 2016) <[https://www.tesla.com/en\\_AU/blog/master-plan-part-deux](https://www.tesla.com/en_AU/blog/master-plan-part-deux)>

<sup>1201</sup> Rand Corporation claim that verification of self-driving cars being as “safe as” human drivers, will require 275 million miles to be driven fatality: Cummings, above n 1182.

<sup>1202</sup> The NHTSA investigation had access to all Tesla’s test data and product design, testing etc. Their sole question was whether a “safety defect”, warranting regulatory intervention, existed.

<sup>1203</sup> Having sat on a recall committee at times, the author is aware though that the thought processes must anticipate everything conceivable that may go wrong and adopt reasonable mitigation strategies. Further, drivers have always died speeding in vehicles which could have had speed limiters installed, and the industry has never adopted, nor been expected to adopt, that type of precautionary design approach for passenger vehicles (c/f trucks). In Australia, the Advertising Code does prohibit depiction of excessive speed in the marketing of cars.

## 4.7 Other ACL CIOT ‘gaps’

### 4.7.1 Strategic acquisition,<sup>1204</sup> redundancy & ‘orphans’

Strategic CIOT corporate acquisition is unlikely to constitute an anti-competitive misuse of market power,<sup>1205</sup> but may adversely impact consumers by targeting data acquisition (Ch 6) and strategic redundancy. In mid-2016, consumers had a bad taste of the latter. Google had acquired Nest and then Revolv,<sup>1206</sup> supporting their USD\$300 smart home hub and app for a time, and then ‘bricking it’ in favour of their own (competing) platform. Users were quietly informed via Revolv’s website<sup>1207</sup> that their smart home would soon remotely, become ‘dumb’:

*“They are not merely ceasing to support...they are advising customers that on May 15th a container of hummus will actually be infinitely more useful than the Revolv hub...”<sup>1208</sup>*

The case illustrates how CIOT mergers and acquisitions may leave devices ‘orphaned’,<sup>1209</sup> consumers ‘app-less’ with obsolescent systems and a dumb device, and even reduce overall market competition. Happily, after online pressure, Google finally posted a website “refund” offer... incidentally linking consumers to Nest.<sup>1210</sup>

While the ACCC would express concern as to ongoing consumer guarantee responsibility, any misleading representations or whether the s. 58 repair obligations are breached, there may be no clear remedy. The law does not oblige consumer IOT devices to stay ‘smart’ for any given time, absent other conduct in breach of the ACL. It is a situation which may warrant attention, as such devices proliferate, may outlast anticipated durability and suppliers may come and go.

---

<sup>1204</sup> The related issue of inter-company data sharing is considered in Ch. 5 as to privacy.

<sup>1205</sup> Competition and Consumer Act 2010 (Cth) This is a structural form of consumer detriment. The ACCC Chair has recently cautioned that Australia’s economy is becoming increasingly concentrated which may adversely affect competition: Rod Sims, ‘ACCC Chairman discusses the increasing concentration in Australia’s economy’ (27 Oct 2016 accessed 28 Oct 2016) < <http://www.accc.gov.au/media-release/accc-chairman-discusses-the-increasing-concentration-in-australia's-economy>>

<sup>1206</sup> Adrian Kingsley-Hughes, ‘Nest to deliberately brick old smart hubs’ *ZDNet* (4 April 2016 accessed 7 Apr 2016) < <http://www.zdnet.com/article/nest-to-deliberately-brick-old-smart-hubs/>>

<sup>1207</sup> According to Arlo Gilbert, owners were not directly notified even though Revolv/ Google have customer email addresses: Arlo Gilbert, ‘The time that Tony Fadell sold me a container of hummus’ *Blog* (3 Apr 2016 accessed 2 Sept 2016) < <https://arlogilbert.com/the-time-that-tony-fadell-sold-me-a-container-of-hummus-cb0941c762c1#3r06trom>; Revolv, ‘A letter from Revolv’s founders’ (n.d. accessed 7 Apr 2016) < <http://revolv.com/>>

<sup>1208</sup> Gilbert, *ibid.* See also Nick Statt, above n 351.

<sup>1209</sup> Google/ Revolv refused to pay consumers compensation, commenting (irrelevantly in Australia at least) that the “one-year warranty against defects in materials or workmanship has expired.” It implies their strategy was to maintain Revolv until the manufacturer warranties had expired, which they viewed discharged their responsibility. In Australia, the consumer guarantees may (usually) outlast the manufacturer’s (contractual) warranty.

<sup>1210</sup> <http://revolv.com/>

## 4.7.2 Penalties

*"Some companies think they have a lot to gain from breaching our competition and consumer law; they should have much to lose as well..." – ACCC<sup>1211</sup>*

ACL remedies available to both the regulator<sup>1212</sup> and successful plaintiffs<sup>1213</sup> are extensive and flexible, but there is an obvious regulatory gap<sup>1214</sup> - pecuniary penalties are considerably lower than international and competition equivalents for "no strong policy reason",<sup>1215</sup> are lower than relative ASIC penalties,<sup>1216</sup> are attracting adverse judicial comment<sup>1217</sup> and are too low to incentivize larger corporations,<sup>1218</sup> such as those which dominate CIOT markets.<sup>1219</sup> Penalties act as a prioritising incentive for compliance and a disincentive to illegality, as well as fund future enforcement actions.<sup>1220</sup> Further, non-compliance – such as misleading practices in data gathering or exploitation of unfair terms - are increasingly prevalent or lucrative for CIOT entities, and "...should not be seen as a cost of doing business..."<sup>1221</sup> Reflecting this, the CAANZ proposes parity with competition law penalties.<sup>1222</sup>

---

<sup>1211</sup> Speech by Rod Sims, ACCC Chairman, 'ACCC's Complaint and Enforcement Policy' *Committee for Economic Development of Australia*, Sydney (19 February 2015).

<sup>1212</sup> ACL Part 5-1 details non-court imposed enforcement powers including undertakings, substantiation notices and public warning notices. CCA section 134A empowers the ACCC to issue infringement notices in lieu of civil penalty proceedings.

<sup>1213</sup> ACL Part 5 powers include injunctive relief, pecuniary penalties and compensation orders.

<sup>1214</sup> While submissions generally divided on predictable partisan lines, submissions to the ACL review from consumer groups, the Australian Labor Party and small business all agreed. These include ACCAN, CHOICE, Consumer Action Law Centre, Consumers Federation Australia, Legal Aid Qld, and many others: CAANZ, above n 840: 177.

<sup>1215</sup> ACCC Chair Sims quoted in Annabel Hepworth, 'ACCC: 'rogues don't care about penalties' The Australian (16 Apr 2016 accessed 2 Aug 2016) <<http://www.theaustralian.com.au/business/accc-rogues-dont-care-about-penalties/news-story/0bbdf40e76bd23c3ae273f54455b0a60>>

<sup>1216</sup> The Corporations Law expresses penalties in penalty units, which are statutorily determined and subject to cpi. As a result, these have risen whereas the ACL penalties have not.

<sup>1217</sup> Gordon, J in the Coles case said that the ACL maximum penalty was "arguably inadequate for a corporation the size of Coles": *Australian Competition and Consumer Commission v Coles Supermarkets Australia Pty Ltd* [2014] FCA 1405 (22 December 2014) The Full Court of the Federal Court suggested that the ACCC \$6M penalty sought in the Nurofen case was "modest" and at the "bottom of the appropriate range": *Australian Competition and Consumer Commission v Reckitt Benckiser (Australia) Pty Ltd* [2016] FCAFC 181 (16 December 2016). Note ACCC penalty submissions are 'advisory' only (unlike some overseas jurisdictions) and courts are free to set higher penalties if justified- but recent court practice is to accept ACCC penalties if within a generally 'permissible range'.

<sup>1218</sup> Sims, above n 1211. He cites the recent *Flightcentre* price fixing \$11M penalty which was criticised in the financial press and Gordon, J's comment in the *Coles* case that a regime of \$1.2 per offence is "arguably inadequate" against a company with an annual \$22B revenue: Federal Court of Australia, 22 December 2014, *Australian Competition and Consumer Commission v Coles Supermarkets Australia Pty Ltd* [2014] FCA 1405 (22 December 2014) <<http://www.austlii.edu.au/au/cases/cth/FCA/2014/1405.html>>

<sup>1219</sup> The maximum competition penalty is ten times the maximum consumer protection penalty. In the EU, GDPR Article 83 contemplates administrative fines of 20 million EUR or 4% total worldwide annual turnover of preceding FY, whichever greater.

<sup>1220</sup> Increasing penalties, using some of the increased revenue from these penalties to increase the Australian Competition and Consumer Commission's (ACCC) litigation budget, and give the ACCC formal powers to conduct market studies in the public interest.

This submission details the implications of that policy suite for enhancing the enforcement a

<sup>1221</sup> Sims, above n 842.

<sup>1222</sup> ACL Review, above n 840: 7. Proposal 18 as to maximum financial penalties proposes an increase to the greater of the maximum penalty (\$10 million) or three times the value of the benefit a company (wrongfully) received or where not determinable, 10% of annual turnover for the previous year. Individuals face a \$500 thousand fine. See also n 825.

## 4.8 Conclusion

This chapter has looked at the ACL to locate potential gaps or uncertainties which may lead to consumer detriment. The proposals to address gaps are summarized below and complement to some extent the privacy considerations highlighted in the next chapter.

CHAPTER 4: GAP SUMMARY	
<b>Proposal 1: Act early</b>	Budget and plan resourced compliance-based consumer and provider education, regulatory stocktake and early enforcement action(s).
<b>Proposal 2: Sweep now</b>	Sweep large CIOT firms to ensure their terms comply with ss. 64 and 67 to underline consumer guarantee operation.
<b>Proposal 3: Clarify 'freemium'</b>	Clarify ACL section 5 so that 'donated' free(mium) goods which collect recipient data accessible to the donee or its affiliates, are treated as a supply of goods or services and receipt, an acquisition.
<b>Proposal 4: Clarify device 'accuracy'</b>	ACCC guidance or industry standards to better clarify and communicate device accuracy performance levels to consumers, especially in smart self (health) categories
<b>Proposal 5: address 'always-on' data collection</b>	Provide guidance that 'always-on' devices require explicit (not bundled) consumer consent and that collectors who transmit data to third parties must contractually ensure those parties comply with the terms of the initial consents
<b>Proposal 6: address safety privacy security &amp; data use practices</b>	Expand section 29 to prohibit false representations as to 'goods' safety, privacy, security or related data collection and use practices.
<b>Proposal 7: increase penalties</b>	Harmonise consumer law penalties with competition penalties plus permit criminal penalties for breaches of section 18.
<b>Proposal 8: prohibit unfair practices</b>	Enhance ACL capacity to promote fairness, overcome unconscionability difficulties and enable examination of 'unfair' CIOT data gathering and use practices
<b>Proposal 9: act on unfair terms</b>	Unfair 'contracts': extend the law to contracts unfair 'overall' Monetary penalties: to incentivize compliance and the increase the risk of infringement. Representative actions should be available to regulators. Capture insurers: delete exclusion of the Insurance Contracts Act 1984 (Cth).

<b>Proposal 10: address Regulation 91 &amp; section 58</b>	Update Reg 91 to remove disclaimer as to repairer liability for data backup to incentivize services backing-up consumer data if required. Update section 58 to include software 'repair' (patch) obligations
<b>Proposal 10: address digital 'goods' definition</b>	Codify Valve by recognising that software-bundled goods providing multiple 'services' are increasingly common 'goods'
<b>Proposal 11: address consumer guarantee disclosure online</b>	Mandate by regulation a model ACL disclosure format by comparative table such as that on Apple's Consumer Law webpage. Adopt CAANZ consumer guarantee proposals
<b>Proposal 12: clarify product safety and liability</b>	Insert an ACL general safety provision Insert goods' security as a 'relevant matter' for device 'safety' in section 9 Clarify 'state of the art' defence Address data handling and software updating practices to manage increasing information asymmetry & to preserve formal regulator notification of recall.
<b>Proposal 13: address device 'orphans'</b>	Amend section 58 to require ongoing device and app support for a reasonable period, commensurate with device cost and purpose.

*Table: 4.2 Summary chapter 4*

*Source: Author*

## Chapter 5 Privacy law & CIOT: an overview

*The smog of personal data is the carbon dioxide of privacy. We've emitted far too much of it over the past decades, refusing to contemplate the consequences... And as computers are integrated into the buildings and vehicles and cities we inhabit, as they penetrate our bodies, the potential harms from breaches will become worse.*<sup>1223</sup>

*Now is the time for setting privacy expectations...*<sup>1224</sup>

In 2016, the Australian Privacy Commissioner (**APC**) hailed a “resurgence” in privacy trust as an “information age concern”.<sup>1225</sup> By mid-2017, he promises Australians IOT privacy guidance and updated big data and anonymization guidance.<sup>1226</sup> It is an ambitious goal for an entity which, faced with budget pressure and threatened disbandment, has struggled in a privacy-adverse environment politically.<sup>1227</sup> As the Commissioner admits, it has all been “...a little challenging, to say the least”<sup>1228</sup> – and now, the consumer IOT has arrived.

---

**In this chapter, references to the Office of the Australian Information Commissioner (OAIC) include the Australian Privacy Commissioner (APC) and vice versa, unless the context suggests otherwise. Timothy Pilgrim is both APC and Australian Information Commissioner as at 2017.**

<sup>1223</sup> Cory Doctorow, ‘Forget Apple’s fight with the FBI – our privacy catastrophe has only just begun’ *The Guardian* (4 Mar 2016 accessed 17 Apr 2016) < <https://www.theguardian.com/technology/2016/mar/04/privacy-apple-fbi-encryption-surveillance>>

<sup>1224</sup> Michelle Dennedy, chief privacy officer for Cisco and founding member of EWF, quoted in Elizabeth Weise, ‘Hey, Siri and Alexa: Let’s talk privacy practices - USA Today’ (2 Mar 2016 accessed 7 May 2017) <https://www.usatoday.com/story/tech/news/2016/03/02/voice-privacy-computers-listening-rsa-echo-siri-hey-google-cortana/81134864/> The EWF devised draft “voice guidance principles” applicable to voice assistants such as Google home or Amazon’s Alexa (see Ch. 7): Alta Associates, ‘Executive Women’s Forum, ‘Voice Privacy Guiding Principles’ (Version 1, Feb 2016 accessed 15 Mar 2016) < [http://c.ymcdn.com/sites/www.ewf-usa.com/resource/collection/CAA076AF-9566-4E1E-9F07-6421154DE0EA/Voice\\_Privacy\\_Guiding\\_Principles\\_Public\\_\(final\).pdf](http://c.ymcdn.com/sites/www.ewf-usa.com/resource/collection/CAA076AF-9566-4E1E-9F07-6421154DE0EA/Voice_Privacy_Guiding_Principles_Public_(final).pdf)>

<sup>1225</sup> Timothy Pilgrim, ‘Privacy Awareness Week Launch 2016 (16 May 2016 accessed 12 Jun 2016) Speech by Timothy Pilgrim to the PAW Business Breakfast, Sydney <<https://www.oaic.gov.au/media-and-speeches/speeches/privacy-awareness-week-launch-2016>> He cited figures that 94% of Australians privilege trust over convenience in purchasing goods and services: Deloitte, above n 461.

<sup>1226</sup> “My priority is protecting Australian’s personal information in the digital age. In the coming year my office will be addressing these modern challenges by releasing guidance on big data, de-identification and the Internet of Things to help businesses and the wider community take privacy in their hands”: Ibid.

<sup>1227</sup> “In the 2014 Budget the Government announced its intention to disband the OAIC, introduce new arrangements for the handling of FOI matters, and re-establish an Office of the Privacy Commissioner. However, as part of the 2016 Budget, the Government announced that it would not proceed... and returned funding to the OAIC to enable it to continue with its regulating role...” Pilgrim, Ibid.

<sup>1228</sup> Ibid. The *Freedom of Information Amendment (New Arrangements) Bill 2014* fell into abeyance in the Senate when a federal election was announced.

## 5.1 Australian Privacy Law: a (brief) overview

*While neither privacy nor FOI are absolute rights; a proactive, pro-disclosure and by-design approach ensures businesses... meet their responsibilities to communities while building trust.*<sup>1229</sup>

*"Privacy isn't dead; it's just going through an identity crisis..."*<sup>1230</sup>

Privacy is an international human right.<sup>1231</sup> For advocates, it is an "asset"<sup>1232</sup> under serious threat; for its critics, an anachronism long "dead", and for privacy regulators, a slippery issue, legislatively 'repackaged'. Australian privacy is a non-absolute, competing right.<sup>1233</sup> There is no statutory or common law<sup>1234</sup> right to privacy,<sup>1235</sup> and despite commitments to international instruments,<sup>1236</sup> declarations<sup>1237</sup> and guidelines, it is questionable whether Australian laws create an internationally- consistent regime in OECD terms.<sup>1238</sup> While data breach disclosure laws finally commence in 2018,<sup>1239</sup> online privacy has declined<sup>1240</sup> through

---

<sup>1229</sup> Timothy Pilgrim, Commissioner's Message, OAIC, Corporate Plan 2016- 17 <<https://www.oaic.gov.au/about-us/corporate-information/key-documents/corporate-plan-2016-17>>

<sup>1230</sup> Colin Wood 'Rethinking Privacy: Though Technology has Outpaced Policy, That's No Reason to Give Up' *Government Technology* (2 June 2014 accessed 30 Mar 2015) <http://www.govtech.com/data/Rethinking-Privacy-Though-Technology-has-Outpaced-Policy-Thats-No-Reason-to-Give-Up.html>

<sup>1231</sup> Article 17 of the International Covenant on Civil and Political Rights, to which Australia is a signatory, states: (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks. Note the Victorian and ACT Human Rights legislation picks up on clause (1) but not (2), which Clarke suggests, makes them virtually inoperative in privacy terms. See also, Article 12 of the Universal Declaration of Human Rights.

<sup>1232</sup> Natasha Maclaren-Jones, Foreword, cited in NSW Legislative Council Standing Committee of Law and Justice, 'Final report: remedies for the serious invasion of privacy in New South Wales' (3 Mar 2016 accessed 10 Mar 2016):9 <<https://www.parliament.nsw.gov.au/committees/DBAssets/InquiryReport/ReportAcrobat/6043/Report%20no%2057%20Remedies%20for%20the%20serious%20invasion%20of%20.pdf>>

<sup>1233</sup> Public policy in Australia clearly recognises competing rights and interests, such as (limited) free speech, (limited) free media, the free flow of information and business' right to efficacy: *Privacy Act 1988* (Cth) s 16A. See also the Minister's Second Reading Speech: Commonwealth, Parliamentary Debates, House of Representatives, 12 April 2000, 15749 (Attorney-General D Williams), 15749–15750. Privacy may conflict with but also complement free speech – for example, in the US, the First Amendment protections as to freedom of speech and association, also protect privacy: Daniel J Solove, Marc Rotenberg and Paul M Schwartz, *Information Privacy Law* (Aspen, 2<sup>nd</sup> ed, 2006) 33.

<sup>1234</sup> The High Court left the possibility open in *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, but subsequent cases have not fundamentally clarified the position. As such legal uncertainty persists.

<sup>1235</sup> The ALRC report indicates this contrasts with the UK, Canada, USA and New Zealand: Australian Law Reform Commission (ALRC), 'Serious Invasions of Privacy in the Digital Era' *Final Report* (June 2014 accessed 3 Apr 2015) 22 [1.24- 1.31] <<https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123>>

<sup>1236</sup> International Covenant on Civil and Political Rights, <<http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>> Art 17 is referenced in *Privacy Act 1988* (Cth) Preamble and s 2(A)(a).

<sup>1237</sup> International Consumer Protection and Enforcement Network (ICPEN), above n 18.

<sup>1238</sup> OECD, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013 accessed 5 Jun 2016) <<https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>>

<sup>1239</sup> The (second) current bill is the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* (Cth), which is still before parliament. One exception is health records, which entail sensitive personal information so the *Personally Controlled Electronic Health Records Act 2012* imposes mandatory data breach requirements upon the System Operator, registered repository and portal operators (as defined). These are subject to civil penalties for failing to comply with section 75 as to mandatory data breach reporting. The *Privacy Act 1998* also simultaneously imposes privacy-related obligations. In 2014, under a voluntary notification system, the Privacy Commissioner commented that "...a number of high profile breaches were not reported to us..." – the figures have improved from 61 (2012-13), 67 (2013-14) to 110 (2013-14), though are still very under-reported.

<sup>1240</sup> The then Communications Minister stated that the bill ensure retention for two years and "...does not expand the range of telecommunications metadata which is currently being accessed by law enforcement agencies in Australia": Minister for

recent mandatory data retention laws.<sup>1241</sup> In this fraught legal environment, the consumer IOT will challenge the Australian privacy regime and its regulator's capacity to respond.

The principal privacy statute is the *Privacy Act 1988* (Cth) (**PA**):<sup>1242</sup> which establishes a remedial<sup>1243</sup> set of technology-neutral (feel-good) principles but as Wigney, J comments:

“...a more labyrinthine, opaque piece of legislation I have yet to discover... legislative porridge... Where almost every word is defined in ways that are counter-intuitive...”<sup>1244</sup>

The 13 Australian Privacy Principles (**APP**)<sup>1245</sup> are designed to, inter alia,<sup>1246</sup> regulate<sup>1247</sup> the collection, use, storage and disclosure (collectively *handling*) of ‘personal information’ (**PI**) and ‘sensitive information’ (**SI**), and to provide consumers with access and correction rights.<sup>1248</sup> The PA applies to any act or practice with an Australian “link”,<sup>1249</sup> including foreign entities which ‘carry on business’ in Australia (see Ch 4)<sup>1250</sup> and collect or hold PI in Australia.<sup>1251</sup> The former is broadly interpreted as Valve suggests, and

---

Communications Malcolm Turnbull, *House of Representatives Hansard*, 30 October 2014, p.12560. Note however that the APC released a privacy business resource advising that metadata is subject to the APPs – so business awaits Telstra's appeal (discussed below) to ascertain the true position.

<sup>1241</sup> The *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015* (Cth) was designed to prevent the “...further degradation of the investigative capabilities of Australia's law enforcement and national security agencies”: Ibid:12562. When passed, it amended the *Telecommunications (Interception and Access) Act 1979* (Cth) s187AA to specify that telecommunications companies are now obliged to store (inter alia) computer and phone metadata including subscriber/ account holder details, and communication data as follows – time, date, location and duration, source destination, service type used (e.g. email, SMS, social media or voice) and delivery services type (e.g. cable, Wi-Fi, ADSL, VoIP). For ‘privacy reasons’ the Act specifically excludes storage of the *content* of phone calls or emails, or web browsing history: Dean Carrigan, John Gallagher and Yvonne Lam ‘Controversial mandatory data retention laws passed’ *Clyde & Co LLP* (30 March 2015 accessed 31 Mar 2015) <<http://www.lexology.com/library/detail.aspx?g=ef4d20da-0bd0-4045-ae8d-07b14992d6d5>>

<sup>1242</sup> Note that State agencies are regulated by state and territory legislation – excluding Western Australia & South Australia: *Information Privacy Act 2014* (ACT), *Information Act 2002* (NT), *Privacy and Personal Information Protection Act 1998* (NSW), *Information Privacy Act 2009* (Qld), *Personal Information Protection Act 2004* (Tas), *Privacy and Data Protection Act 2014* (Vic).

<sup>1243</sup> As such, it “should be construed so as to give the fullest relief which the fair meaning of its language will allow...”: per Warren, J citing *Bull v Attorney-General (NSW)*(1913) 17 CLR 370 [384].

<sup>1244</sup> Wigney, J of the Federal Court cited in Peter Leonard, ‘Australian privacy Law: swimming in the porridge of offshore disclosure’; G+T (6 Nov 2014 accessed 28 May 2015) <<http://www.lexology.com/library/detail.aspx?g=61f5ad3e-95cf-4576-a128-c112278b2790>>

<sup>1245</sup> Schedule 1 of the *Privacy Act 1988* (Cth). The former principles were in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

<sup>1246</sup> Part III applies to the handling of credit-related personal information for inclusion on individuals' credit reports.

<sup>1247</sup> The Australian Information Commissioner (**OAIC**) also has obligations under (largely) sector-specific legislation, including the *Telecommunications Act 1997* and the *Telecommunications (Interception and Access) Act 1979 for consultative, monitoring and compliance functions, information handling under the eHealth records system: Personally Controlled Electronic Health Records Act 2012 etc.* See Mathews-Hunt, above n 151.

<sup>1248</sup> It also regulates sensitive health information for health and medical research purposes and individual tax file numbers under the *Data-matching Program (Assistance and Tax) Act 1990* (Cth).

<sup>1249</sup> PA section 5B(1A).

<sup>1250</sup> The OAIC suggest that judicial guidance may be derived from the ACL cases in this regard.

<sup>1251</sup> PA section 5B(3).

requisite 'collection' occurs if from an individual physically in Australia,<sup>1252</sup> (which usually corresponds to device location). Further, while many CIOT providers may be not in Australia, there is a "link" if it (inter alia) markets to or targets services at Australians and it collects PI from Australians. As such the PA will apply to most CIOT situations; the question considered next, is how well.

## 5.2 Gap analysis

CIOT industry practices which do not 'promote the protection of the privacy of individuals'<sup>1253</sup> will infringe the APP regime,<sup>1254</sup> and regulatory 'gaps' will diminish privacy. Inadequate OAIC enforcement disincentivizes compliance,<sup>1255</sup> and issues detection is unlikely absent a complaint or (rare) regulatory audit<sup>1256</sup> and ill-informed consumers cannot complain or give up faced with weak outcomes little-justifying the effort. This systemic latent detriment diminishes privacy, nor can the system self-correct through consumer behaviour.<sup>1257</sup> Perhaps reflecting this market failure, the Productivity Commission recently recommended a new consumer right to access, correct, transfer, and opt out of consensual data collection.<sup>1258</sup> It recommends that the ACCC – not the OAIC<sup>1259</sup> - administers the legislation.<sup>1260</sup>

Potential PA gaps are as follows:

---

<sup>1252</sup> Hall & Wilcox, 'Lessons from the Ashley Maddison Investigation- Part 2' (28 Sept 2016 accessed 2 Oct 2016) <[http://www.lexology.com/library/detail.aspx?g=6c58d9ea-13f2-4b56-968f-56bf7154949d&utm\\_source=Lexology+Daily+Newsfeed&utm\\_medium=HTML+email+-+Body+-+General+section&utm\\_campaign=Lexology+subscriber+daily+feed&utm\\_content=Lexology+Daily+Newsfeed+2016-10-03&utm\\_term=>](http://www.lexology.com/library/detail.aspx?g=6c58d9ea-13f2-4b56-968f-56bf7154949d&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2016-10-03&utm_term=>)>

<sup>1253</sup> This is an object to the PA, section 2A(a).

<sup>1254</sup> The APPs (Sched. 2) are: 1. Open and transparent management of personal information (PI); 2. Anonymity and pseudonymity; 3. Collection of unsolicited PI; 4. Dealing with unsolicited PI; 5. Notification of the collection of PI; 6. Use or disclosure of PI; 7. Direct marketing; 8. Cross-border disclosure of PI; 9. Adoption, use or disclosure of government-related identifiers; 10. Quality of PI; 11. Security of PI; 12. Access to PI; 13. Correction of PI. The long form is accessible here: <<https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles>>

<sup>1255</sup> OAIC, Privacy Action Regulatory Policy (June 2015 accessed 3 Jan 2016) <<https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/>>

<sup>1256</sup> For example, in 2015, the APC announced "We are just getting ready to conduct an assessment of the online privacy policies of 21 entities against the requirements of Australian Privacy Principle 1. These assessments looked at whether the policies were clearly expressed and up-to-date, covered the content and contact requirements and were available in an appropriate form". Pilgrim, above n 231.

<sup>1257</sup> For example, the author fell victim to the Adobe hack (Aug 2015), and had to change an email address held for over a decade due to spam. A blood-donor friend was victim to the Red Cross data breach, but was told that his name, age, email address was not a 'serious' breach. In both cases, consumers are left feeling vulnerable, inconvenienced and annoyed.

<sup>1258</sup> Productivity Commission, above n 190. This is in the proposed *Data Sharing and Release Act*.

<sup>1259</sup> The draft report also (correctly) suggests that as privacy regulator in a big data context, the OAIC may need additional resources: *Ibid*: 351.

<sup>1260</sup> This supposedly reflects the ACCC competition and consumer policy jurisdiction, but illustrates the converging nature of consumer privacy and consumer protection regulation.

### 5.2.1 Defining PI & SPI

In 2014, international privacy authorities declared CIOT data to be PI:

“Internet of things’ sensor data is high in quantity, quality and sensitivity. This means the inferences that can be drawn are much bigger and more sensitive, and identifiability becomes more likely than not... Considering that the identifiability and protection of big data already is a major challenge, it is clear that big data derived from internet of things devices makes this challenge many times larger. Therefore, such data should be regarded and treated as personal data.”<sup>1261</sup>

In Australia, regulatory uncertainty as to fundamental PA concepts is troubling. The nature of what is “personally identifiable” is changing, as data fusion and de-anonymisation/ re-identification capacities increase exponentially, but Australia law is not evolving apace. Under the PA, PI means “... information or an opinion about an identified individual, *or an individual who is reasonably identifiable*, whether true or not or whether recorded in material form or not” ...<sup>1262</sup> Sensitive PI (SI) attracts greater protection<sup>1263</sup> and concerns an individual’s:

- (a)(i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) ...trade union; or (viii) sexual orientation or practices; or (ix) criminal record; or
- (b) health... or
- (c) non-health genetic information, about an individual; or
- (d) biometric information ... used for... automated biometric verification or identification; or (e) ... templates.<sup>1264</sup>

The 2015 OAIC Guideline confirms that most consumer IOT data is PI: registration/ warranty details, such as name,<sup>1265</sup> address, birth date, telephone number (etc.)<sup>1266</sup> and credit information<sup>1267</sup> are all cited examples. Device-collected data and software may also access or yield PI:

---

<sup>1261</sup> Mauritius, above n 736.

<sup>1262</sup> The definition concludes with whether the information or opinion is true or not, or whether recorded in material form or not. Note section 187LA of the Telecommunications (Interception and Access) Act 1979 extends the meaning of PI to cover information kept under Part 5-1A of that Act.

<sup>1263</sup> See for example APP 3, 6 and 7. The OAIC acknowledges that SI handling breach may result in discrimination, mistreatment, humiliation, embarrassment and undermine personal dignity: OAIC, Guidelines, supra n 1299 :[B140- 141]

<sup>1264</sup> PA section 6.

<sup>1265</sup> Note that surname often reveals ethnic derivation – but often not. As such the Guidelines state that surname alone is not SI, nor is every opinion, belief or value. Clearly the facts of each circumstances are relevant. For example, surnames of refugees on a boat coming to Australia may become SPI if they indicate ethnic derivation or political affiliations,

<sup>1266</sup> Other examples include medical records, bank account details and commentary or opinion about a person.

<sup>1267</sup> This is provided if device or software licensing, subscription or ongoing payments arise. For example, there is a strong suggestion that Tesla may make certain software ‘upgradeable’ via additional or subscription payments. They offer access

“...photographs, IP addresses,<sup>1268</sup> Unique Device Identifiers and other unique identifiers, personal contact lists, which reveal details about a user’s social connections and the contacts themselves, voice print and facial recognition biometrics, because they identify and collect unique characteristics of an individual’s voice or face, location information, because it can reveal user activity patterns and habits and, as a consequence, identity.”<sup>1269</sup>

Mobile devices commonly hold PI, IP addresses<sup>1270</sup> are usually PI<sup>1271</sup> and even dynamic IP addresses - if as the EU Court of Justice recently found, the collector “has the legal means which enable it to identify the data subject with additional data which [it]... has about that person.”<sup>1272</sup> All this is consistent with international precedents,<sup>1273</sup> reports<sup>1274</sup> and regulation<sup>1275</sup> and portends a necessary expansion of PI

---

to vehicle service repair manuals, service documents, wiring diagrams, and part information currently by time-period subscription, but do not have a dedicated link to Australia. See their UK link here: <<https://service.teslamotors.com/>>

<sup>1268</sup> See also the EU Working Party 29 (2008) Opinion: EU, Article 29 Data Protection Working Party, ‘Opinion 1/2008 on data protection issues related to search engines’ (Adopted 4 Apr 2008 accessed 2 Aug 2016) <[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf)> and the English Court of Appeal in *Google Inc. v Judith Vidal-Hall and others* [2015] EWCA Civ 311, 27 March 2015. The Court of Appeal held there is a serious case to answer that third-party cookie-collected online behavioural data is personal data, even though not connected to other information directly identifying an individual

<sup>1269</sup> OAIC, ‘Mobile privacy: a better practice guide for mobile app developers’ (Sept 2014 accessed 21 Jan 2016) <<https://www.oaic.gov.au/agencies-and-organisations/guides/guide-for-mobile-app-developers>>

<sup>1270</sup> IP addresses are a digital “fingerprint” left by a device which accesses the internet – so for example, internet-connected CIOT devices have an IP address. They are strings of numbers which identify a device to the ISP and website owners – usually only one is attached per household or subscriber. Dynamic IP addresses however change which makes them less likely to be PI unless combined with other data (such as date and time) which may identify an individual. In that context, these are likely to be PI: Mason Hayes and Curran, ‘Are Dynamic IP Addresses Personal Data?’ (29 September 2016 accessed 20 Oct 2016) <http://www.mhc.ie/latest/blog/are-dynamic-ip-addresses-personal-data> See also *Israel v Bank Ha’Po’alim*, cited in EU Data Protection Working Party, Opinion 6/2009 on the level of protection of personal data in Israel (2009) <[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp165\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp165_en.pdf)> Note the now-defunct Obama US FCC proposed rulemaking which defines PI as “any information linked or linkable to an individual” with an opt out of IP address use: Federal Communications Commission (FCC), ‘In the Matter of Protecting the Privacy of Customer of broadband and Other Telecommunications Services’ Notice of Proposed Rulemaking (1 Apr 2016 accessed 2 Aug 2016) (WC Docket No. 16-106) <<https://www.fcc.gov/document/fcc-releases-proposed-rules-protect-broadband-consumer-privacy>>

<sup>1271</sup> OAIC, supra n 1306: 20 [paras B.92].

<sup>1272</sup> *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, the CJEU found that “...dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.” The case concerned an internet service provider. Mason, above n 1270.

<sup>1273</sup> See Canada, NZ and US cases respectively: *Gordon v Canada (Health)* (2008) FC 258; *Proceedings Commissioner v Commissioner of Police* [2000] NZAR 277; *American Civil Liberties Union v Clapper et al*, 785 F.3d. 787 (2nd Cir. 2015) In the latter the Second Circuit Court of Appeals dismissed the view that identification of a specific plaintiff was ‘speculative’ by evidence that the NSA searched the files regularly, which included the plaintiffs.

<sup>1274</sup> See for example, Executive Office of the President, above n 41 (Big Data).

<sup>1275</sup> Directive of the European Parliament and Council, Directive 95/46 EC [1995] OJ L 281 refers to a person who can be identified “directly or indirectly” including by reference to identifiers (name, ID number, location data, an online identifier): Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (GDPR) <<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC>>; The UK *Data Protection Act 1988* provides that PI means “...data which relate to a living individual who can be identified—(a) from those

categories to adapt to consumer IOT (and other) technologies. However, a recent much-anticipated decision on the former PI definition<sup>1276</sup> has exposed a ‘gap’ or at best, raises legal uncertainty as to PI scope and “identifiability” under the PA. As Anna Johnston put it:

“Well. That was a curve ball no-one saw coming.”<sup>1277</sup>

In *Grubb v. Telstra*,<sup>1278</sup> the APC determined that mobile phone metadata<sup>1279</sup> (including geolocation) was PI, identifying an individual through matching device identifiers, IP address and Telstra’s customer database,<sup>1280</sup> to which Telstra must provide access under NPP6.1(APP 12). After a successful AAT appeal,<sup>1281</sup> the APC appealed to the Full Federal Court,<sup>1282</sup> which arguably, due to the narrow appeal grounds,<sup>1283</sup> adopted a literal, non-purposive<sup>1284</sup> approach, upholding the AAT decision. The case turned upon whether the metadata was “about”<sup>1285</sup> an individual<sup>1286</sup> (which Telstra had acknowledged)<sup>1287</sup> or the

---

data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller...’(etc.)

<sup>1276</sup> PI was then defined (relevantly) as “information or an opinion... about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion...” The current definition (relevantly) is “... information or an opinion about an identified individual, or an individual who is reasonably identifiable.”

<sup>1277</sup> Anna Johnston, ‘Mobiles, metadata and the meaning of ‘personal information’, *SalingerPrivacy Blog* (19 Jan 2017 accessed 3 Feb 2017) <<https://www.salingerprivacy.com.au/2017/01/19/federalcourtdecision/>>

<sup>1278</sup> *Ben Grubb v Telstra Corporation Limited* [2015] AICmr 35

<sup>1279</sup> ‘Metadata’ is data about data; that is, not what people type on a device or say over the phone, but rather the footprint that’s left behind. It is variously officially defined. See the dataset required to be retained under the mandatory data retention scheme here: <https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/Dataset.pdf>> See also page 46 here: Australian Government, Attorney-General’s Department, ‘Departmental submission Inquiry into the comprehensive revision of the Telecommunications (Interception and Access) Act 1979

Senate Legal and Constitutional Affairs References Committee’ (2016 accessed 5 Mar 2017)

<[http://www.aph.gov.au/Parliamentary\\_Business/Committees/Senate/Legal\\_and\\_Constitutional\\_Affairs/Comprehensive\\_revision\\_of\\_TIA\\_Act](http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act)>

<sup>1280</sup> While not a straightforward exercise, Telstra used the process to assist law enforcement agencies regularly: Eli Fisher, ‘Developments in Data Driven Law: A Discussion with Peter Leonard’ G+T (23 Sept 2016 accessed 30 Sept 2016) <<https://www.gtlaw.com.au/?q=developments-data-driven-law-discussion-peter-leonard>>

<sup>1281</sup> Decision [2015] AATA 991 (18 Dec 2015) per Dep President S A Forgie.

<sup>1282</sup> *Privacy Commissioner v Telstra Corporation Ltd*, No VID 38/2-16, Full Federal Court of Australia (Dowsett, Kenny and Edelman, JJ)

<sup>1283</sup> The court stated: “There was no ground of appeal which alleged that the AAT erred in its conclusion that none of the information was about Mr Grubb. In other words, the Privacy Commissioner did not seek to establish that any of the information was about Mr Grubb”: Johnston, above n 1277.

<sup>1284</sup> The court referred to PA objects of protecting individual privacy as “aspirational” and uninfluential in its determination. It stated: “this appeal concerned only a narrow question of statutory interpretation which was whether the words ‘about an individual’ had any substantive operation’: Ibid: [73]

<sup>1285</sup> This word still appears in the definition, though slightly differently. PI was then defined as “information or an opinion... about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion...” The current definition is “... information or an opinion about an identified individual, or an individual who is reasonably identifiable.”

<sup>1286</sup> The AAT’s finding conflicts with European and US authority. For example, in *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, the independent advisor to the EU’s highest court found that IP addresses are PI where they are handled by a website operator. a dynamic IP address and browsing date and time were under certain circumstances (i.e. where the information provides the ability to identify the individual) personal data under the EU legislation.

<sup>1287</sup> In the AAT, Telstra’s legal counsel said: “I’m dealing here with the question of mobile network data in relation to Mr Grubb’s mobile telephone service. It’s difficult for me to see how that could not be information about him. It’s information about his service”: Johnston, above n 1277.

network itself,<sup>1288</sup> and concluded the latter, even though Telstra could identify Mr Grubb (with effort) by combining multiple databases.<sup>1289</sup> Consistent with its narrow analysis, the court conflated object with subject, confusing the primary collection purpose, with what data is ‘about’,<sup>1290</sup> though acknowledged that information may have multiple subject-matters and that context (including linkage) may render data ‘about’ an individual. The decision is heavily criticised:<sup>1291</sup> it has “gutted” PI,<sup>1292</sup> defies international precedent<sup>1293</sup> and lacks any objective PI-definition methodology.<sup>1294</sup> Consumer IOT data raises the same questions: it may reliably distinguish or analytically infer user identity, even in shared environments, it involves device IP addresses and geolocation data, and commonly involves multiple-subject information - for example, running/ driving data is about the distance/ car but also, the runner/driver.<sup>1295</sup> How the decision impacts upon the present (distinguishable) PI definition is questionable. PI was then (relevantly) “information... *about an individual* whose identity is apparent, or can reasonably be ascertained, from the information...” The current definition (relevantly) refers to “... information ... *about an identified individual*, or an individual who is reasonably identifiable.” While the language differs, it is difficult to see why the court’s interpretation would<sup>1296</sup> if metadata were considered again:

---

<sup>1288</sup> AAT Deputy President Forgie decided that unless an individual is identified in the information intrinsically, then the first question is whether that information is “about an individual”; if not, then the second question as to whether identity can “reasonably be ascertained” is redundant. The author respectfully suggests that were the case about the current PI definition, the question could be split into: is the information about an identified individual, and if not, then is the individual ‘reasonably identifiable’. On the facts, the AAT found that the data was about the service delivery to Mr Grubb, not Mr Grubb himself. Note the definition for PI then was “information about an individual, whose identity is apparent or can reasonably be ascertained from the information or opinion about the individual”:

<sup>1289</sup> Telstra argued that it is possible to link geolocation and URL data to an individual but their systems made it difficult, requiring complicated historical searches within the retention period of 3 to 30 days. In contrast the APC found that Telstra regularly cross-matched metadata in response to law enforcement requests and responded to 85.000 such requests (July 2013- June 2015).

<sup>1290</sup> Johnston, above n 1277.

<sup>1291</sup> See for example, respected practitioner Peter G. Leonard, ‘A review of Australian Privacy Commissioner v Telstra Corporation Limited Full Federal Court of Australia [2017] FCAFC’, G+T (16 Feb 2017) <https://www.gtlaw.com.au/insights/review-australian-privacy-commissioner-v-telstra-corporation-limited> who expresses concern as to the lack of policy consideration or guidance provided; Jake Goldenfein, ‘Australia’s privacy laws gutted in court ruling on what is ‘personal information’ *The Conversation* (19 Jan 2017 accessed 19 Jan 2017) <http://theconversation.com/australias-privacy-laws-gutted-in-court-ruling-on-what-is-personal-information-71486>; c/f Johnston, above n 1277.

<sup>1292</sup> Goldenfein, *ibid*.

<sup>1293</sup> Amicus curiae brief of Australian Privacy Foundation and NSW Council for Civil Liberties in *Privacy Commissioner v Telstra Corporation Limited* (File No. VID 38/2016) (Filed 17 Aug 2016 accessed 2 Sept 2016) < <https://www.privacy.org.au/papers/fca-pcvt-160817.pdf>>

<sup>1294</sup> Leonard, above n 1291.

<sup>1295</sup> Note in the AAT, Deputy President Stephanie Forgie gave an example which was narrow in terms of possible multiple information use: “A link could be made between the service records and the record kept at reception or other records showing my name and the time at which I had taken the care (sic) in for service. The fact that the information can be traced back to me from the service records or the order form does not, however, change the nature of the information. It is information about the car ... or the repairs but not about me”. Johnston, above n 1277.

<sup>1296</sup> This view is also adopted by Cain Sibley and Ken Powell, ‘What about me? The Full Federal Court says personal information must be “about an individual” *Clayton Utz* (2 Feb 2017 accessed 3 Mar 2017) < <https://www.claytonutz.com/knowledge/2017/february/what-about-me-the-full-federal-court-says-personal-information-must-be-about-an-individual>>

In each case, it is necessary to consider whether each item of PI requested, individually or in combination with other items, is about an [identifiable] individual...<sup>1297</sup>

Had the appeal required the court to rule upon the AAT's 'evaluative conclusion', it is possible the it may have found multiple subject matters<sup>1298</sup> – but the judgment implies a rejection of evolving data matching and linking technologies, whereby a mobile phone colour may (in combination) render its owner identifiable. It is a case which raises more questions than it answers.<sup>1299</sup> This uncertainty creates privacy risk, as to the meaning of PI and how data recipients should respond to technology and data holdings, as granularity and analytics increase, and holdings expand. Uncertainty may also embolden pro-risk PI retention practices - especially where expensive and time-consuming cases against well-funded commercial entities like Telstra, fail.<sup>1300</sup>

Clearly if the PA is to have its intended effect, then any capacity by any entity to reasonably identify an individual from information holdings, should be sufficient to activate the Act. Indeed, the new metadata retention regime takes this approach,<sup>1301</sup> deeming all mandatorily-retained data as PI.<sup>1302</sup> However, it remains unclear how the CIOT industry perceives the data its devices and apps collect, though in questionable contractual practices and data ownership attitudes, there may be a clue.

## 5.2.2 The principles

*The APPs require a privacy by design...*<sup>1303</sup> - OAIC

*“... overcollecting... (to sift for possible correlations) is the norm...”*<sup>1304</sup>

---

<sup>1297</sup> *Privacy Commissioner*, above n 1282 [63]. The insertion is mine to illustrate how their evaluation would operate under the new PI definition.

<sup>1298</sup> Johnston, above n 1277.

<sup>1299</sup> Cain, above n 1296.

<sup>1300</sup> Ben Grubb first made complaint to the APC as a journalist testing the law in 2014. The APC made its determination in mid-2015, and the federal Court, in January 2017. Note that the implications for Telstra have been superseded by statute: telecommunications companies' metadata holdings must be retained under new mandatory data retention provisions in the Telecommunications (Interception and Access) Act 1979. Section 187LA deems information retained as PI “about an individual” if the information relates to the individual or a communication to which the individual is a party.

<sup>1301</sup> It applies to internet, carriage service and content service providers, under the Telecommunications Act (Cth).

<sup>1302</sup> Section 187LA Telecommunications (Interception and Access) Act 2015 came into force on 13 October 2015.

<sup>1303</sup> OAIC, above n 1269: 2.

<sup>1304</sup> Peter Leonard, 'Customer data analytics: privacy settings for 'Big data' Business International Data Privacy Law 4 (1) (2014 accessed 10 Apr 2015) 53 – 68 <<http://idpl.oxfordjournals.org/>>

The APPs are in PA Schedule 1 and augmented by non-binding<sup>1305</sup> guidelines,<sup>1306</sup> including as to privacy impact assessments<sup>1307</sup> the Privacy Management Framework,<sup>1308</sup> mobile app developers<sup>1309</sup> data breach<sup>1310</sup> and regulatory action.<sup>1311</sup> This section considers each APP to locate gaps.

- **APP1 imposes the obligation for an entity to implement PA compliance “practices, procedures and systems” and to have a “...clearly expressed and up-to-date” privacy policy available [1.3];**<sup>1312</sup> for example, on a website.<sup>1313</sup> As chapter 6 suggests, many entities have deficient privacy policies<sup>1314</sup> which fail to transparently and accurately explain CIOT collection practices<sup>1315</sup> or reveal CIOT-collected data use purposes and potential data flows. Absent this, then any consent obtained as to data collection and use becomes questionable and terms may potentially, be misleading or unfair.

The OAIC claims that APP1 requires privacy by design (**PBD**) using a Privacy Management Framework which practically, means a risk management-based identification and mitigation of privacy risk:<sup>1316</sup>

*PBD aims at building privacy and data protection up front, into the design specifications and architecture of information and communications systems and technologies, in order to facilitate compliance with privacy and data protection principles.”*<sup>1317</sup>

---

<sup>1305</sup> Legally binding guidelines as to medical research, tax file numbers and so on are found here:

<https://www.oaic.gov.au/agencies-and-organisations/legally-binding-guidelines-and-rules/>

<sup>1306</sup> As to the APPs: OAIC, ‘Australian Privacy Principles Guidelines’ (1 April 2015 accessed 5 April 2015)

[http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP\\_guidelines\\_complete\\_version\\_1\\_April\\_2015.pdf](http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP_guidelines_complete_version_1_April_2015.pdf) > Others include: the Privacy Action Regulatory Policy, the Guide to Privacy Regulatory Action, the Guide to undertaking Privacy Impact Assessments and the OAIC Privacy Management Framework. It is also emphasized in the ‘better practice guide’ for mobile app developers.

<sup>1307</sup> OAIC, ‘Guide to undertaking privacy impact assessments’ (May 2014 accessed 2 Jan 2016) <

<https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments>>

<sup>1308</sup> OAIC, ‘Privacy management framework: enabling compliance and encouraging good practice’ (N.D. accessed 10 May 2016) < <https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework>>

<sup>1309</sup> OAIC, above n 1269.

<sup>1310</sup> OAIC, ‘Guide to developing a data breach response plan’ (April 2016 accessed 8 Apr 2016) <

<https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-developing-a-data-breach-response-plan.pdf>>; OAIC, ‘Guide to securing personal information’ (Jan 2015 accessed 8 Apr 2016) <

<https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>>

<sup>1311</sup> OAIC, ‘Guide to privacy regulatory action’ (June 2015 accessed 3 Feb 2016) < <https://www.oaic.gov.au/resources/about-us/our-regulatory-approach/guide-to-oaic-s-privacy-regulatory-action/oaic-regulatory-action-guide.pdf>>

<sup>1312</sup> APP 1 requires that PI is managed in an open and transparent way (APP 1.1) and that APP entities to take “reasonable steps to implement practices, procedures and systems” that will ensure APP compliance, as well as compliance with any PA-registered code and which also, enable related inquiry or complaints management (APP 1.2).

<sup>1313</sup> Privacy policies must inform consumers as to the kinds of PI collected/ held, how this occurs; the purposes for which it is collected, held, used and disclosed; access and correction processes; complaints process and management; and location of any overseas disclosure.

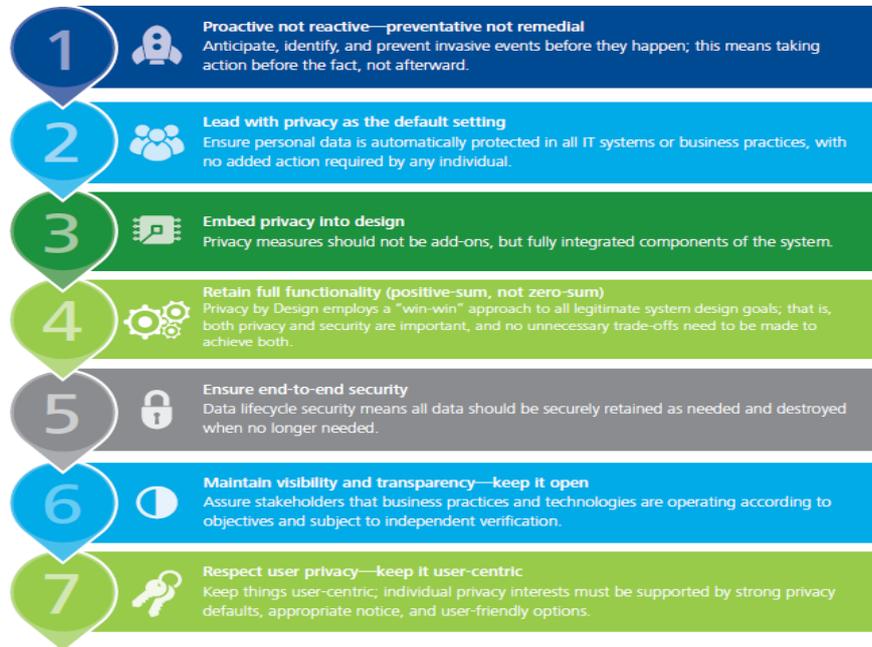
<sup>1314</sup> APP 1.4 details the policy must contain (a) the kinds of PI collected and held; (b) how the entity does this; and (c) for what purpose(s); as well as individual rights such as (d) access and correction; (e) how complaints are made and dealt with; (f) if disclosure occurs to overseas recipients; and (g) the likely overseas countries.

<sup>1315</sup> For example, by device documentation or set-up, software registration and consents.

<sup>1316</sup> OAIC, ‘Guide to Big Data and the Australian Privacy Principles’ *Consultation Draft* (May 2016 accessed 2 May 2016): 6-7 < <https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/>>

<sup>1317</sup> Ibid: 2.

The Framework requires a top-down embedded “culture of privacy”,<sup>1318</sup> through robust practices, procedures and systems, ongoing efficacy evaluation; and continuous privacy monitoring and improvement. PBD is codified, incorporated by reference or by (non-binding) guideline<sup>1319</sup> in Australia,<sup>1320</sup> the UK,<sup>1321</sup> and the EU,<sup>1322</sup> and promoted by the FTC. It has seven foundational principles:



Graphic 5.1 7 Foundational principles for Privacy by Design  
Source: Anna Cavoukian & Deloitte<sup>1323</sup>

These principles manage privacy lifecycle risk, which offers CIOT providers multiple benefits such as reducing privacy litigation or penalties, systematising compliance, reducing liability gaps, boosting consumer confidence, improving breach management, and a defensive ‘best practice’ posture in the

<sup>1318</sup> OAIC, above n 1308: 1.

<sup>1319</sup> It was unanimously adopted by ‘landmark’ resolution of the 2010 International Conference of Data Protection and Privacy Commissioners. Anna Cavoukian as Canadian Privacy Commissioner legitimised the concept within privacy regulation: Anna Cavoukian, ‘Operationalizing Privacy by Design: From Rhetoric to Reality’, Office of the Information and Privacy Commissioner (2012 accessed 4 Mar 2016) <http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1254>. See also Anna Cavoukian, ‘A regulator’s perspective on Privacy by Design’ (n.d. accessed 10 May 2016) < <https://fpf.org/wp-content/uploads/A-Regulators-Perspective-on-Privacy-by-Design.doc>> Australian states have also adopted the principle.

<sup>1320</sup> Australian states have also adopted the principle.

<sup>1321</sup> Article 23 of the European Data Protection Regulation, which is effective in 2018. EU Data Protection Regulation, ‘Data protection by design and default’ (Accessed 26 June 2016) <http://www.eudataprotectionregulation.com/#!data-protection-design-by-default/c20k7>

<sup>1322</sup> Ibid.

<sup>1323</sup> Deloitte, ‘Privacy by Design: setting a new standard for privacy certification’ (2015 accessed 3 Jan 2016): 2 <<https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF>> Used with kind permission of Dr Cavoukian.

event of breach. Compliance with PBD systems also enables trust mark certification,<sup>1324</sup> which checks system robustness, but is also a marketable way to inspire consumer confidence, increase sales and business value, differentiate products, and reduce legal liability upon an actionable breach.

But there is a regulatory gap here. Despite OAIC rhetoric, the APPs are silent as to PBD or avert to it descriptively only, and guidelines have no legal effect. There is no determination stating that APP 1.2 mandates PBD,<sup>1325</sup> nor court ruling to that effect<sup>1326</sup> and the OAIC does not audit PBD compliance and cannot direct industry to conduct a PIA.<sup>1327</sup> The practical outcome is that PBD is 'optional', and for CIOT manufacturers, entails time and costs to design-in privacy and security systems, which raises cost: benefit questions in a highly-competitive, fast-moving marketplace. There is evidence that PBD has not transferred from regulator rhetoric to industry practice: as recently as 2014, Telstra was not PBD-compliant.<sup>1328</sup> This gap, adversely impacts privacy enforcement, as the OAIC does not audit or compel disclosure of PBD practices, nor can the OAIC direct an 'organisation'<sup>1329</sup> to conduct a privacy impact assessment. PBD may thus, be observed more in the breach than in observance – it is cheaper to go to market without PBD, and accept the low risk of getting caught – which with CIOT risks to privacy, raises an unacceptable gap.

---

<sup>1324</sup> For example, with an entity such as TRUSTe. This enables the display of a recognised symbol and may improve business practices, promote consumer, investor and supplier confidence, as well as potentially deflect regulator interest. See <<https://www.truste.com/>>

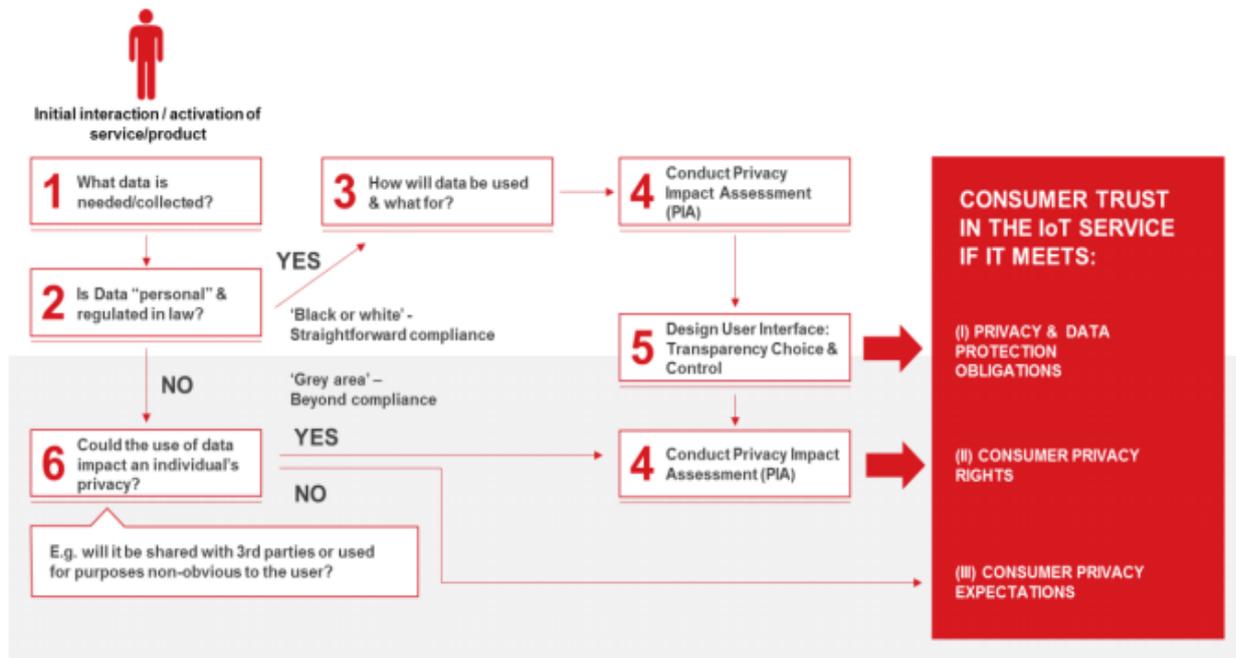
<sup>1325</sup> Section 52 of the Privacy Act 1988 (Cth) enables the OAIC to make determinations on privacy complaints either of its own initiative or where conciliation has failed to resolve a matter. The determinations are subject to appeals to the Administrative Appeals Tribunal (s 96 PA) or by the Federal Circuit Court or Federal Court of Australia under section 5 of the Administrative Decisions (Judicial Review) Act 1977 (Cth). Application to appeal must be made within 28 days (s 29(2) Administrative Appeals Tribunal Act 1975 (Cth) and ADJR Act section 5), fees are payable and the ADJR process provides the Federal Court may refer a matter back to the Information Commissioner should the decision be wrong at law or the IC powers were not exercised properly.

<sup>1326</sup> Note the reports may be somewhat self-selective – one would expect companies to resolve cases before appeal where they are vulnerable to adverse determination. But since its insertion in 2014, there are no cases dealing with complaints relating to APP 1.2 at all. This may be because there is a delay in complaints being made, a delay in breaches being identified or a delay in cases coming before the OAIC. It may also be because (perhaps with the force of the new provisions) complaints are resolved prior to requiring regulatory action.

<sup>1327</sup> Ibid.

<sup>1328</sup> "Telstra will also establish a clear policy for central software management (including information security arrangements), review contracts relating to personal information handling (including by enhancing Telstra's control over third party providers), implement a data loss prevention program, adopt a Privacy by Design strategy, and exit its contract with the third party provider.": Telstra Corporation Limited: Own motion investigation report [2014] AICmrCN 1 (1 March 2014) <<http://www.austlii.edu.au/au/cases/cth/AICmrCN/2014/1.html>>

<sup>1329</sup> As distinct from a government agency.



Graphic 5.2 IOT 'Privacy by Design' Decision Tree  
 Source: GSMA<sup>1330</sup>

A related PBD concept is privacy (and security) by default. The APPs do not refer to this, which means the automatic application of the strictest privacy (and security) settings of a device or app, and informed, opt-in consumer actions to modify those settings. In the meantime, device data stays in the highest protection mode. It also implies data minimisation consistent with APP 11, as well as promotes the designed-in use of privacy-enhancing technologies, as recommended by EPIC,<sup>1331</sup> and aligns with Article 25 of the incoming EU *General Data Protection Regulation (GDPR)*<sup>1332</sup> which stipulates 'data protection by design and by default'.<sup>1333</sup> Given the complexity of CIOT device and app set-ups, this is a consumer protection 'gap' in Australia. If this were mandated in Australia, it would overcome evidenced lax CIOT security practices such as default passwords or inadequate encryption, which imperil CIOT network security and inevitably, enable DDoS attacks (discussed supra) and adversely impact upon consumer privacy, trust and confidence.

<sup>1330</sup> GSMA, 'IoT Privacy by Design Decision Tree' (8 May 2015 accessed 8 Mar 2016) <<http://www.gsma.com/iot/iot-knowledgebase/iot-privacy-design-decision-tree/>>

<sup>1331</sup> EPIC, "Comments of the Electronic Privacy Information Center to the National Telecommunications and Information Administration, US Department of Commerce On the Benefits, Challenges and Potential Roles for the Government in Fostering the Advancement of the Internet of Things" (2 June 2016 accessed 26 Jun 2016): 11 <<https://www.ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things>>

<sup>1332</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

<sup>1333</sup> Ibid: Articles 24 and 25.

- **APP 1.3** also seeks to ensure open and transparent data management, to “build consumer trust and confidence”.<sup>1334</sup> But in a CIOT context, that regulatory object is clearly failing. In 2015, the APC found over half of 21 online privacy policies audited “inadequate”.<sup>1335</sup> In 2016, a global IOT sweep found that 71% of reviewed Australian CIOT device terms did not adequately explain how PI is managed.<sup>1336</sup> Internationally, most of 314 smart devices were found to “interfere with privacy”<sup>1337</sup> in breach of privacy laws (**Sched. 2**). The sweep identified three main concerns: firstly, many fitness device policies did not adequately explain PI collection, use and disclosure practices. Few were device-specific, privacy promises did not match user experience and most did not disclose third party information recipients. Secondly, many failed to explain PI storage and protection practices, and thirdly, data deletion information was non-existent or difficult to find.<sup>1338</sup> The outcome confirms the OAIC’s 47 website sweep (2013),<sup>1339</sup> and its 2015 ‘follow up’, showing that 55% were still APP1 non-compliant.<sup>1340</sup> Persistently poor compliance outcomes suggest an APP1 regulatory failure - and notice and consent failing at both ends.

---

<sup>1334</sup> OAIC, above n 1316: 6.

<sup>1335</sup> Paris Cowan, ‘Pilgrim to audit 21 Australian privacy policies’ *itnews* (20 Feb 2015 accessed 2 Feb 2016) <https://www.itnews.com.au/news/pilgrim-to-audit-21-australian-privacy-policies-400708> Pilgrim stated: “These assessments will look at whether the policies are clearly expressed and up-to-date, cover the content and contact requirements and are available in an appropriate form”.

<sup>1336</sup> The devices were fitness and health monitors, smart travel locks and thermostats though explicit data was not released. The author contacted the OAIC for details, but it did not respond. OAIC, ‘Privacy shortcomings of Internet of Things businesses revealed’ (23 Sept 2016 accessed 28 Sept 2016) < <https://www.oaic.gov.au/media-and-speeches/news/privacy-shortcomings-of-internet-of-things-businesses-revealed>>

<sup>1337</sup> PA section 13(1). The AIC can investigate with based upon a complaint (which usually leads to conciliations under section 40A, or under its own motion (PA Part V).

<sup>1338</sup> *Ibid.*

<sup>1339</sup> Of 47 websites checked, almost 50% of policies exhibited ‘readability’ issues, i.e. “they were considered to be too long and difficult to read”, Using the Flesch-Kinkaid Reading Ease test, the average age was 16 with none meeting the OAIC14 years as their preferred benchmark. Relevance was a problem for 65% of the sites: OAIC, ‘Privacy Commissioner: Website privacy policies are too long and complex’ (14 Aug 2013 accessed 2 Nov 2016) < <https://www.oaic.gov.au/media-and-speeches/media-releases/privacy-commissioner-website-privacy-policies-are-too-long-and-complex>>

<sup>1340</sup> Entities included the ANZ Bank, Dept of Human Services, Microsoft and Instagram. The “follow up” resweep still found that 25% (5) privacy policies did not outline how to request access or correction of PI; another 25% did not adequately describe how they protect PI; 40% (8) did not outline how privacy complaints are dealt with; 20% did not outline overseas disclosure or likely countries for that disclosure. OAIC, ‘Privacy policies still have room for improvement’ (4 May 2015 accessed 2 Nov 2016) < <https://www.oaic.gov.au/media-and-speeches/media-releases/privacy-policies-still-have-room-for-improvement>>

- **APP3** provides that an entity must not solicit<sup>1341</sup> and collect<sup>1342</sup> PI unless it is “reasonably necessary<sup>1343</sup> for one or more of the entity’s [lawful]<sup>1344</sup> functions or activities” [3.2] and then, only by “lawful and fair means” [3.5] and only from the individual [3.6] - unless it is impracticable or unreasonable to do so. “Sensitive information” (SI)<sup>1345</sup> requires consent for collection, which may be implied.<sup>1346</sup>

This raises CIOT issues: firstly, CIOT devices both actively solicit and collect PI which by data minimisation, should be limited to that “reasonably necessary” for the functions or activities of the entity.<sup>1347</sup> The OAIC imposes an objective test: “would a reasonable person, properly informed, agree collection is necessary”.<sup>1348</sup> The OAIC cites collecting more PI than necessary<sup>1349</sup> or collecting for future use or for a related body corporate, as examples of unnecessary collection, and clearly, data optimisation for sales purposes exceeds the consumer device remit.<sup>1350</sup> To be effective, then CIOT data minimisation must be enforced – but as the Milo example below suggests, this is often not the case and not always for nefarious reasons. Secondly, fair, lawful<sup>1351</sup> collection must not be deceptive or unreasonably

---

<sup>1341</sup> ‘Solicited’ PI includes an individual’s PI “.... provided by another entity in response to a request, direction, order or arrangement for sharing or transferring information between both entities...”: *OAIC Guideline* above n 1306: 4 [para 3.7] Note that “unsolicited” PI must be destroyed or de-identified soon as practicable if it is lawful and reasonable to do so: APP 4

<sup>1342</sup> ‘Collect’ means to collect PI for “inclusion in a record...”: s 6(1) PA. ‘Record’ includes in a document, electronic or other device’, so includes PI stored on a device or in a database such as that which CIOT device systems use to store and analyse data. Note also in a smart home context, “collection” includes obtaining (etc.) PI from “surveillance cameras where an individual is identifiable or reasonably identifiable” as well as “biometric technology such as voice or facial recognition”: OAIC, Guidelines: above n 1306: 7- 8.

<sup>1343</sup> This is an objective test as to whether a reasonable person, properly informed would agree collection is necessary: OAIC Guidelines, above n 1306: 6. Note that PI collection may not be reasonably necessary where more information than is required for a function is collected or where it is being collected for entry into a database for future use: Guideline, above n 1306: 194: 7 [para 2.32].

<sup>1344</sup> ‘Lawful’ means not unlawful, that is not illegal, criminal, prohibited or proscribed by law and includes collection via hacking for example but excludes a breach of contract: *OAIC Guidelines*, above n 1306:14 [para 3.6- 3.61].

<sup>1345</sup> “Sensitive information” means (a) information or an opinion about an individual’s:(i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b)health information about an individual; or (c) non-health genetic information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.

<sup>1346</sup> “Consent” means “express consent or implied consent”: PA section 6.

<sup>1347</sup> APP 3.2. OAIC Guidelines point to website description, annual reports, advertising etc., to identify these, or any “directly related” functions or activity.

<sup>1348</sup> OAIC, Guidelines: above n 1306: 7. Relevant factors will include the primary purpose of collection, how the PI is used and whether the entity could fulfil its functions absent that information?

<sup>1349</sup> Examples include *Own Motion Investigation v Australian Government Agency* [2007] PrivCmrA 4; *D v Banking Institution* [2006] PrivCmrA 4; *M v Health Service Provider* [2007] PrivCmrA 15.

<sup>1350</sup> It is unlikely that a CIOT entity would highlight ‘data trading’ clearly, although a privacy statement may enable it (often obliquely or euphemistically) within a broad ambit of data transfers. The question here, is whether CIOT data sales lack the clear or direct connection to a function/ activity as required.

<sup>1351</sup> APP 3.5. Not lawful includes hacking: Criminal Code Act 1995 Part 10.7, using a listening device of telephone interception without a warrant: Telecommunications (Interception and Access) Act 1979 (Cth) section 7 and Surveillance Devices Act 2004 (Cth) section 14; requesting information for or in connection with a discriminatory act: e.g. Disability Discrimination Act 1992 section 30; Sex Discrimination Act 1984 section 27.

intrusive;<sup>1352</sup> but numerous CIOT security systems, baby monitors,<sup>1353</sup> smart TVs,<sup>1354</sup> and digital voice assistants<sup>1355</sup> have already been implicated in this.<sup>1356</sup> The OAIC cites misrepresenting the purpose or effect of collection, or any consequence of not providing the information, as possibly “unfair” means – and CIOT privacy statements or terms commonly assert that “device functionality” may diminish if information is not provided – without clearly specifying the extent (if any) and how.<sup>1357</sup> Further any assessment of “fair” again raises “consent” issues (**Ch 6**), but the obligation is conveniently avoided, if obtaining consent is generally “unreasonable or impractical” – as may be the case for shared devices or those operating in shared environments. Even if individual privacy consents are valid, questions persist as to implying consent of unwitting smart home or car occupants, third party visitors or persons who share or borrow CIOT devices – or even a person who buys a smart home or car, without changing settings or understanding how it all works. Thirdly, APP3 allows collection of PI “reasonably necessary” to pursue a collector’s “legitimate functions or activities”, assessed “objectively and practically”.<sup>1358</sup> But “legitimate” is a loaded term. While most entities justify obtaining PI to provide wanted consumer analytics (e.g. fitness trackers use height and weight), or for functionality reasons (e.g. to operate the smart home or car), the privacy sweeps have shown excess information collection with no objective justification. Finally, the ‘lawful and fair means’ criteria is contentious in many CIOT situations, where the purpose or consequence of collection is questionably represented<sup>1359</sup> and/ or without express or implied ‘consent’ (if required).

- **APP 4** concerns unsolicited PI/ SI collected by an entity, which if collectable under APP3, falls under APPs 5-13, but if not, must be destroyed or de-identified as soon as practicable.

---

<sup>1352</sup> Guidelines, above n 1306: 14. See also the Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012: 77.

<sup>1353</sup> Arguably collection may deceive consumers where security is not as represented or enables other unlawful collections via hacking: Stanislav, above n 617.

<sup>1354</sup> Samuel Gibbs, ‘Samsung’s voice-recording smart TVs breach privacy law, campaigners claim’ (28 Feb 2015 accessed 10 May 2016) <<https://www.theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim>>

<sup>1355</sup> For example, as to future, Samsung plans Viv to integrate with smartphones, tablets, wearables and home appliances, based upon its “sophisticated natural language understanding, machine learning capabilities and strategic partnerships that will enrich a broader service ecosystem”. The idea is a voice-powered interface for all of its devices - phones, home hubs, fitness trackers to refrigerators.: Carly Page, ‘Samsung buys Viv AI tool to build its own assistant to rival Siri and Cortana’ (6 Oct 2016 accessed 10 Oct 2016) <<http://www.computing.co.uk/ctg/news/2473325/samsung-buys-viv-ai-tool-to-build-its-own-assistant-to-rival-siri-and-cortana>>

<sup>1356</sup> Rory Carroll, ‘Goodbye privacy, hello ‘Alexa’: Amazon Echo, the home robot who hears it all’ *The Guardian* (21 Nov 2015 accessed 4 Mar 2016) <<https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud>> Amazon says Alexa streams audio a fraction of a second before ‘woken’ and continues until a request is processed” so conversation fragments will be captured.

<sup>1357</sup> Again, the Nestle app collected a range of PI as to its child user, and only at the end (once data was collected) did it indicate that data was not required to use the fitness band, and this was neither prominent nor was it clear how to remove data entered and take that option.

<sup>1358</sup> OAIC, above n 1316: 9.

<sup>1359</sup> OAIC Guideline above n 1306: 14 [para 3.63].

The CIOT uncertainty here is whether data collected via devices (as distinct from solicited inputs like sign-up data) or SI incidentally collected from non-consenting third parties, is ‘solicited’ or collected via “no active steps”?<sup>1360</sup> This is potentially unclear, but it seems sensible that a device setup to monitor and transmit data is an active collection step to solicit whatever data that device detects, and that consent to third party SI collection is likely ‘implied’, or alternatively, that its severance for destruction or de-identification may not be ‘reasonable’ due to impracticality,<sup>1361</sup> so APP5- 13 apply.<sup>1362</sup>

- **APP 5** details privacy notice contents,<sup>1363</sup> which (where practicable) must be disclosed at or before collection, clearly and prominently displayed on device or by (e.g.) link or where by third party supply, that party is contractually bound to notify the individual.

Impracticability may arise, if, for example, devices lack screens, requiring referral to website terms. Individuals must also be informed of collection methods; for example, if through “hidden ... RFID” or software or biometric technology.<sup>1364</sup> Ideally, just-in-time on-device or smartphone notification with links or opt-in ‘accept’ boxes is preferable notice to long, unheralded privacy statements, but the latter proliferates. Despite voluminous guidance,<sup>1365</sup> codes<sup>1366</sup> and the APP law, genuine ‘notice’ as a precursor to genuine ‘consent’ in a CIOT context is limited,<sup>1367</sup> as is realistic ongoing (contractual) protection of data once transferred or sold (**Ch. 6**).

---

<sup>1360</sup> ‘Solicit’ means a request to provide PI or information within which PI is included, but a ‘request’ merely means an “active step” taken to collect the information which may not involve ‘direct communications between the entity and the individual’: OAIC Guideline above n 1306: 14 [para 4.5- 4.8].

<sup>1361</sup> The Guidelines cite that destruction or de-identification of unsolicited PI may not be practical if “commingled with solicited personal information” – see [4.26 for an example]: OAIC Guidelines, above n 1306: [4.25]

<sup>1362</sup> If not, then the consequence at the extreme, is that all CIOT data (other than that directly inputted or perhaps that emanating from the owner) should be de-identified pre-use or destroyed as soon as practicable.

<sup>1363</sup> APP 5 provides that at or before (or asap after) collection of PI, the entity must take reasonable steps to ensure that the individual is informed of: its identity and contact details; if PI is not collected from the individual or that individual may not be aware of the collection, the fact and circumstances of the collection; if PI was collected mandatorily by law; the purposes of collection; consequences if all or any PI is not collected; any disclosures or type thereof; that its privacy policy contains access/ correction/ complaints and complaints management information; and finally, details of the location of any overseas disclosure intended.

<sup>1364</sup> OAIC Guideline, above n 1306: 6 [para 5.11].

<sup>1365</sup> For example, see OAIC, above n 1303 or the guidelines explaining the APPs: OAIC, above 1307.

<sup>1366</sup> A ‘gold standard’ example is ICO, ‘Privacy notices, transparency and control’ (7 Oct 2016 accessed 20 Oct 2016) <<https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/>>

<sup>1367</sup> Mark Briedis, Jane Webb & Michael Fraser, ‘Improving the Communication of Privacy Information for Consumers’ ACCAN & UTS (Feb 2016 accessed 2 Oct 2016) <http://accan.org.au/files/Grants/Improving%20Comm%20Privacy%20Info-full-accessible.pdf>

- **APP 6:** PI held<sup>1368</sup> for a “primary purpose” must not be used for a “secondary purpose” without consent unless such use or disclosure is “reasonably expected”<sup>1369</sup> and the secondary purpose is (if SI) “directly related”<sup>1370</sup> or where PI only, “related”<sup>1371</sup> to that primary purpose.<sup>1372</sup>

Reasonable expectation is an objective question of fact, as to what a properly informed reasonable person would expect; an interesting CIOT data-use question usually avoided via the consent exception. A simple drafting exercise will satisfy APP6 through broad purpose categories – e.g. “data analytics, marketing and affiliated third party uses...” It is however difficult to discern how the collection purpose can be maintained when data is commonly shared and on- sold, combined and recombined, exposing it to re-identification or to new unanticipated correlations and uses. Future “collection creep”<sup>1373</sup> is implicit in changeable terms and “function creep” is almost implicit in broad conceptual purposes (e.g. marketing), such that absent *enforced* legal or contractual restraints, data use may go ‘rogue’.<sup>1374</sup> Nothing in the PA addresses this gap, absent regulatory oversight.

APP 6.2(e) allows use or disclosure for secondary purposes in seven permitted ‘general situations’<sup>1375-</sup> which include preventing a serious threat to life, health or safety,<sup>1376</sup> locating missing persons<sup>1377</sup> and where PI is (objectively)<sup>1378</sup> reasonably necessary for any ‘enforcement related activities’<sup>1379</sup> of police, immigration, ASIC and others, without warrant.<sup>1380</sup> CIOT data as to smart self, home and car may

---

<sup>1368</sup> OAIC Guideline, above n 1306: 4 [para 6.7] indicates that ‘hold’ refers to information in the possession and control of the entity either physically or by right or power to deal with it.

<sup>1369</sup>OAIC Guideline, above n 1306: [6.20] The ‘reasonably expects’ test is an objective question of fact in each case and has regard to what a reasonable properly informed person would expect in the circumstances.

<sup>1370</sup> OAIC Guideline, above n 1306: [6.26] This is one “closely associated with the primary purpose, even if it is not strictly necessary to achieve that primary purpose”.

<sup>1371</sup> OAIC Guideline, above n 1306: [6.26]: This is one “connected to or associated with the primary purpose”. It must be more than tenuously linked: *B v Hotel* [2008] PrivCmrA 2, *E v Insurance Company* [2011] PrivCmrA 5.

<sup>1372</sup> APP 6.2 (b) – (e) and 6.3 contain exclusions related to for example, court and enforcement mandated situations.

<sup>1373</sup> Uber was recently accused of this: after being penalised for poor geolocation data protection, it took an incremental approach to extending location data collection again, initially amending its privacy statement, then months later rolling out a software update with notice and consents, (see <https://help.uber.com/h/ba9dd342-158d-421f-a9ea-0e6c7aaad726>) for tracking to extend after passengers leave the vehicle: Kate Conger, ‘Uber begins background collection of rider location data’ *TechCrunch* (29 Nov 2016 accessed 29 Nov 2016) <https://techcrunch.com/2016/11/28/uber-background-location-data-collection/> updated its privacy policy in 2015 to allow for background location data collection,

<sup>1374</sup> In 2011, the world’s largest satnav device maker TomTom sold anonymised vehicle speed and location data to the Netherlands government which was used (to Tom Tom’s embarrassment) for setting speed traps.

<sup>1375</sup> These are listed in PA section 16A. Of possible CIOT relevance include: Lessening or preventing a serious threat to life, health or safety (where consent is unreasonable or impracticable)

<sup>1376</sup> PA section 16A (1) Item 1.

<sup>1377</sup> PA section 16A (1) Item 3.

<sup>1378</sup> The test is whether a reasonable person properly informed would agree the use or disclosure is reasonable in the circumstances.

<sup>1379</sup> PA section 6(1): this includes prevention, detection, investigation and prosecution or punishment of criminal offences and intelligence gathering activities.

<sup>1380</sup> OAIC, APP Guidelines, above n 1306: 14 [para 6.56- 6.64] Note “enforcement activity” is defined very broadly in section 6(1) to include intelligence-gathering, prevention, detection, investigation, prosecution or punishment of criminal offences.

evidence a serious threat (for example, in-home violence or dangerous driving) and would assist law enforcement, but is also potentially prejudicial, inaccurate and privacy-intrusive. While public policy<sup>1381</sup> may justify such disclosures, always-on surveillance-style data derived from ubiquitous consumer IOT devices, justifies a careful rethink.<sup>1382</sup>

APP 6.3 allows PI use and disclosure by any related body corporate for the same “primary purpose”;<sup>1383</sup> which again, encourages wide statements, data fusion and potentially, uses in unexpected contexts.<sup>1384</sup> Data-rich CIOT companies are also highly attractive targets:<sup>1385</sup> for data, but also for technology-acquisition and/ or anti-competitive reasons.<sup>1386</sup>

- **APP 7**<sup>1387</sup> prohibits non-consensual direct marketing<sup>1388</sup> using SI, but allows PI use in limited circumstances. Most privacy statements include advertising communications use, and device or

---

<sup>1381</sup> Policy includes protection of safety, national security and the like. Practically police can already physically search homes and cars for a wide range of reasons. See for example, the extensive warrantless search rights in Queensland which include to prevent domestic violence, to take a breath test and to preserve evidence: <http://www.legalaid.qld.gov.au/Find-legal-information/Criminal-justice/Police-and-your-rights/Police-searches-without-a-warrant>

<sup>1382</sup> The Parliamentary Inquiry found that the police sought warrantless authorisations to access mobile phone and internet metadata 310,000 times in five years, before mandatory data retention laws were enacted. Suelette Dreyfus, of the University of Melbourne, warns “If we don’t stop this creep into our private worlds that government is using technology for, it only becomes a matter of time before these other lines are crossed as well. It’s important that we draw that line right here and now.”: David Wroe and Nino Bucci, ‘Police access phone and internet data 1300 times a week’ (14 Jan 2015 accessed 2 Feb 2017) *The Syd Morning Herald* <<http://www.smh.com.au/federal-politics/political-news/police-access-phone-and-internet-data-1200-times-a-week-20150113-12nga3.html>>

<sup>1383</sup> Privacy Act 1988 (Cth) section 13B provides that collection of “personal information” (PI) (but not ‘sensitive information’ as defined) between related bodies corporate is not generally an interference with the privacy of an individual. APP 6.6 provides that PI shared between RBCs has the same “primary purpose” for both as at collection. PA Guideline page 18 [para 6.77] ‘Related bodies corporate’ has the meaning defined in the Corporations Law.

<sup>1384</sup> The Guidelines provide an ambiguous example here; suggesting that a contractor applying to work for a company may have that application shared between RBCs. It is unclear if this is the same context as the parent is overseeing their contracting engagement or whether they are assessing suitability for the contractor to work for them too (presumably the former as ‘purpose’ must stay the same): OAIC Guideline, above n 1306: 3 [para 7.9] Internationally, there are numerous examples of large entities buying other companies to access their data as a treasure trove; especially, entities which have collected PI with very broad use consents – such as social media companies.

<sup>1385</sup> For example, Walmart purchased the Social Calendar app which had 15 million registered users, 110 million personal notifications (such as date of birth, anniversary date and the like) and 10 million monthly reminders were suddenly able to be combined with Walmart’s already extensive customer databases, as well as any others to which they had access. This data was used in targeted advertising recommending Walmart gift purchases based upon user’s friends’ Facebook page content. Similarly, Google purchased DoubleClick in 2008 to feed data into its AdSense advertising network which by 2011, made Google some \$36.5 billion. The purchase price was US\$3.1 billion. Data taken from *Google v Vidal-Hall, Hann and Bradshaw* [2015] EWHC Civ 311 [para 6.1]

<sup>1386</sup> The Economist, ‘The Rise of the Corporate Colossus threatens both competition and the legitimacy of business’. *Leader section* (17 Sept 2016 accessed 20 Nov 2016) <<http://www.economist.com/news/leaders/21707210-rise-corporate-colossus-threatens-both-competition-and-legitimacy-business>> page 9 cited by Rod Sims, ‘ACCC Chairman discusses the increasing concentration in Australia’s economy’ Speech (27 Oct 2016 accessed 28 Oct 2016) <<http://www.accc.gov.au/media-release/accc-chairman-discusses-the-increasing-concentration-in-australia-s-economy>>

<sup>1387</sup> This is subject to the application of the *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth). The former covers email, instant messaging, SMS (text messages) and MMS (image-based mobile phone messaging) messages of a commercial nature. It does not cover faxes, internet pop-ups or voice telemarketing, which is subject to the Do Not Call Register.

<sup>1388</sup> OAIC Guideline, above n 1306: 3 [para 7.9] ‘Direct marketing’ means the use or disclosure of PI to communicate directly with an individual to promote goods and services, including by email, online or by mail.

app sign-ups often (by default) include an opt-in<sup>1389</sup> to such advertising. Google Home recently voiced a smart audio advertisement (aka 'helpful' information), and sparked a social media backlash.<sup>1390</sup> Direct (profiled) advertising is coming to further monetize the consumer IOT, and pre-checked app opt-ins likely will too. In the case of marketing covered under the *Spam Act 2003 (Cth)*, consent must be express 'opt-in' or reasonably inferable.<sup>1391</sup>

- **APP 8** is relevant to CIOT data flows, cloud storage and analytics. Prior to cross border "disclosure" to (for example) a contractor, an entity must take reasonable (usually contractual) steps<sup>1392</sup> to ensure that the recipient does not breach the APPs (or it may be accountable), unless laws or an enforceable code impose "substantially similar" recipient obligations, and with enforcement powers accessible to the individual. If an entity stores CIOT data overseas (as most apps do), but retains effective handling control<sup>1393</sup> then this is 'use', not 'disclosure' caught by APP8. Further, if a foreign law compels disclosure then the APP entity is absolved. Consumers are unlikely to understand foreign laws but the PA does not oblige the entity to explain this or to modify its disclosure choices to ensure more privacy- protective outcomes. Further, the entire chain-of-liability approach is overturned if an 'express general situation' arises,<sup>1394</sup> or upon obtaining express informed consent, provided specific matters are addressed, which CIOT providers usually manage online by disclaimer in their standard privacy terms.<sup>1395</sup>
- **APP 10 Accuracy:** requires 'reasonable steps' to ensure that PI collected is "accurate, up to date and complete". Inaccuracy has consequences in the consumer IOT (**Chs 3 and 4**). PI is

---

<sup>1389</sup> APP 7.2 allows DM use where the information is collected from the individual who would reasonably expect the use for that purpose and a simple opt-out mechanism (such as a checkbox) is provided. Where there is no such reasonable expectation or where information is collected by a third party (such as a data vendor or app provider), where practicable the individual must have consented to use, and an opt-out (reminder) statement must be provided in every piece of DM

<sup>1390</sup> Al Roberts, 'Has advertising arrived on Google Home?' *ClickZ* (9 May 2017 accessed 10 May 2017) <<https://www.clickz.com/has-advertising-arrived-on-google-home/110247/>>

<sup>1391</sup> Spam Act 2004 (Cth): Sched 2 clause 2(b) consent can reasonably be inferred from: (i) the conduct; and (ii) the business and other relationships; of the individual or organisation concerned. Non-automated voice calls are covered by the Do Not Call Register Act 2006 (Cth).

<sup>1392</sup> Contracts may include clauses as to auditing compliance, protocols imposed on the service provider, indemnities, warranties, reporting and the like.

<sup>1393</sup> Relevant factors as to effective control might include retaining (sole) rights as to access, changing or retrieving PI, who accesses it, security measures and whether it remains retrievable or deletable: OAIC Guidelines, above n 1306: [8.14] Note some contracts may retain 'control' sufficiently to make storage a 'use', such that the APP entity may breach the APPs as it "holds" the information, as it retains the right and power to deal with it (or can access it physically). Guidelines, above n 1306: [B.79- 81]

<sup>1394</sup> PA section 16A as discussed above.

<sup>1395</sup> APP 8.2(b) allows an entity to obtain consent for cross border disclosure which must explain that the entity would no longer be accountable for the data under the PA, the recipient will not comply nor will redress be available. This is effectively a disclaimer by express notice and consent. Guidelines, above n 1306: [8.39]

'inaccurate' if it contains a defect or error,<sup>1396</sup> and may create an 'incomplete'<sup>1397</sup> and misleading consumer picture, which is self-perpetuatingly, 'out-of-date':<sup>1398</sup> for example a bad driver can improve with experience. That data may evolve through many hands, under diminishing contractual obligations, while re-identification risk increases over time. And of course, consumers may never know who is holding or analysing/ using their data, or for how long.

- **APP 11 Security:** PI must be protected against loss, misuse or interference and "...unauthorised use, modification or disclosure". If any PI is no longer needed, then 'reasonable steps' must be taken to destroy or de-identify it.

**Ch. 3** illustrated serious CIOT security issues, but if 'reasonable' security steps are taken,<sup>1399</sup> the OAIC assert that hacking or data breach is not a privacy breach, but rather a police issue. This ignores consumer privacy harm, does not incentivize best practice security, nor imposes compliance-based regulatory action. In 2016, there were four determinations involving APP 11,<sup>1400</sup> (of 6 since 2010) which awarded \$3- 10,000 for non-economic loss.<sup>1401</sup> While an increase, the OAIC is not 'go-to' for breach: indeed, in the US, the FTC has prosecuted over 60 ('unfair') security cases,<sup>1402</sup> US shareholder derivative actions are ongoing for security-related breach of fiduciary duty,<sup>1403</sup> and substantial UK fines have been imposed.<sup>1404</sup>

---

<sup>1396</sup> Inaccurate means the information contains an error or defect: Guidelines, above n 1306: [10.12] – even opinions must not be "misleading"; and must not present a "partial or misleading picture": [10.17]

<sup>1397</sup> OAIC, Guidelines, above n 1306: [10.17] 'Incomplete' PI presents a partial or misleading picture, not 'a true or full picture'.

<sup>1398</sup> OAIC, Guidelines, above n 1306: [10.15] 'Out-of-date' PI contains non-current facts, opinions or other information.

<sup>1399</sup> The ICO fined TalkTalk £400,000 for its "failure to implement the most basic security systems measures." The hacker is facing criminal charges: ICO, TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack ' (5 Oct 2016 accessed 20 Oct 2016) < <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/>> Note however, the ICO cannot order consumer compensation.

<sup>1400</sup> Since 1 Nov 2010, the determinations are: 'JO' and Comcare [2016] AICmr 64 (21 September 2016); 'IY' and Business Services Brokers Pty Ltd t/a TeleChoice [2016] AICmr 44 (30 June 2016); 'IX' and Business Services Brokers Pty Ltd t/a TeleChoice [2016] AICmr 42 (30 June 2016); 'IR' and NRMA Insurance, Insurance Australia Limited [2016] AICmr 37 (27 June 2016); 'EQ' and Great Barrier Reef Marine Park Authority [2015] AICmr 11 (2 February 2015); 'DO' and Department of Veterans' Affairs [2014] AICmr 124 (13 November 2014); 'CP' and Department of Defence [2014] AICmr 88 (2 September 2014).

<sup>1401</sup> Ibid.

<sup>1402</sup> The FTC have prosecuted over 60 data breach cases over recent years. See *FTC v Wyndham Worldwide Corp. et al.*, Civil No. 13-1887 (Dist. Court New Jersey, 7 Apr 2014) <<http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation> [Dist Ct].

<sup>1403</sup> Joseph W Swanson & John E Clabby, 'A Firewall for the Boardroom: Best Practices to Insulate Directors and Officers from Derivative Lawsuits and related Regulatory Actions regarding Data Breaches' *Corporate Accountability Report* (14 Aug 2015 accessed 12 Apr 2016) 13 CARE 1810

<sup>1404</sup> Phil Muncaster, 'UK's ICO doubled number of data breach fines in 2016' *InfoSecurity* (5 Jun 2017 accessed 7 Jun 2017) <<https://www.infosecurity-magazine.com/news/uks-ico-doubled-number-of-data/>>

Finally, as to destruction or de-identification, there is no evidence that this practice is complied with,<sup>1405</sup> either internationally<sup>1406</sup> or in Australia; nor is there a mechanism for consumers to enforce destruction.<sup>1407</sup> Data value and cloud computing promote retention 'just-in-case', but the OAIC has never 'swept' this issue. Given experts view large data sets as a security "honey-pot"<sup>1408</sup> and CIOT data's granular, voluminous nature, the OAIC could readily shape industry privacy practices by own-motion<sup>1409</sup> audits of data retention practices. Given it "expects" entities to conduct information security risk assessments under its PIA process,<sup>1410</sup> a simple regulator audit could start by examining those documents, if they exist at all.

- **APP 12 Access and APP 13 Correction Rights**<sup>1411</sup> These provide an entity must give individuals access<sup>1412</sup> to PI held<sup>1413</sup> about them, on request, subject to specified refusal grounds,<sup>1414</sup> and set minimal procedural requirements as to reasonable steps to correct PI held

---

<sup>1405</sup> The OAIC's joint Ashley Maddison investigation has no relevance to the CIOT other than evidencing indicative data management practices. It resulted in enforceable undertakings which included: to "...cease its practice of retaining indefinitely personal information of users whose accounts are deactivated or inactive; determine an appropriate period following account deactivation, or following an extended period of inactivity, upon which to delete personal information, based on ordinary usage patterns and its business needs; and inform users of these policies...": Enforceable Undertaking Under s 33E of the Privacy Act 1988 (Cth), Australian Information Commissioner - Avid Life Media Inc. (ALM) (trading as Ruby Corp.) (21 Aug 2015) <<https://www.oaic.gov.au/privacy-law/enforceable-undertakings/avid-life-media-enforceable-undertaking>>

<sup>1406</sup> Australian de-identification failure examples include Australia Post and an almost instant de-identification breach of the 10% Medicare data set, and the similar breach of the ABS internal workforce data 'Open government' (formerly SPI) data sets as to the PBS and Medicare were withdrawn from publicly available databases when University of Melbourne researchers promptly re-identified the data: <http://www.huffingtonpost.com.au/2016/09/28/privacy-commissioner-to-investigate-medicare-data-breach/>; See the OAIC view here: Timothy Pilgrim, 'Privacy, Data & De-identification' *Speech by Timothy Pilgrim to CeBIT, Sydney* (2 May 2016 accessed 30 May 2016) <<https://www.oaic.gov.au/media-and-speeches/speeches/privacy-data-de-identification>>

<sup>1407</sup> Productivity Commission, above n 190: 309- 310.

<sup>1408</sup> OAIC, Big Data, above n 1316: 22.

<sup>1409</sup> PA s 40(2) of the Privacy Act, the Commissioner may, on the Commissioner's own initiative, investigate an act or practice that may be an interference with the privacy of an individual or a breach of APP 1 if the Commissioner thinks it desirable that the act or practice be investigated.

<sup>1410</sup> OAIC, Big Data, above n 1316: 23.

<sup>1411</sup> APP 9 prohibits the use of "government related identifiers" subject to some exclusions. APP 12 deals with access rights (as in the Grubb case discussed above) and APP13 deals with correction of information which is inaccurate, out-of-date, incomplete, irrelevant or misleading for the purpose for which it is held: Guidelines, above n 1306 [13.30-13.41].

<sup>1412</sup> APP 12 stipulates minimum requirements as to response times [12.66–12.67], how access is given [12.68–12.75], any charges [12.76–12.81], and written notice, including refusal reasons [12.82–12.87]. The Guidelines suggest "prompt, uncomplicated and inexpensive" access is desirable: OAIC Guidelines, above n 1306: [12.19].

<sup>1413</sup> 'Hold' means in its possession or control of any record containing PI: section 6(1) and extends beyond physical possession to any PI the entity has a right or power to deal with: OAIC Guidelines, above n 1306 [12.7].

<sup>1414</sup> APP 12.3 refusal grounds are: access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety (APP 12.3(a)); access would unreasonably impact other's privacy (APP 12.3(b)); the request is frivolous or vexatious (APP 12.3(c)); the PI relates to existing or anticipated legal proceedings not accessible by discovery in those proceedings (APP 12.3(d)); access would reveal the prejudicial intentions of the organisation in relation to negotiations with the individual (APP 12.3(e)); access would be unlawful (APP 12.3(f)); denying access is required under an Australian law or court/tribunal order (APP 12.3(g)); the provider has reason to suspect that unlawful activity, or serious misconduct, relating to its functions or activities has been, is being or may be engaged in such that access would prejudice appropriate actions in that regard (APP 12.3(h)); access would prejudice enforcement related activities of an enforcement

to ensure that it is accurate, relevant, complete, up-to-date, and not misleading.<sup>1415</sup> While data control is a laudable objective and one which both the GDPR and Productivity Commission are seeking to (re)enshrine,<sup>1416</sup> at present, consumers often cannot identify or locate a CIOT entity - or any chain of data-handling entities - much less seek access and data correction rights. Nor do the APPs entitle consumers to request information deletion (despite APP 11) which is a significant gap given the sheer volume of data collected by CIOT devices. If the *Grubb case* is any example,<sup>1417</sup> then troublesome access across corporate databases and setting access precedents, much less mandatory deletion rights, may be strongly resisted.

As this discussion suggests, the APPs have significant regulatory uncertainties or gaps when it comes to CIOT privacy. Others are considered next.

### 5.3 Other consumer privacy ‘gaps’

As the APP analysis above suggests, the law may fail to address new harms, or be uncertain, under-inclusive or even obsolete in many CIOT contexts.<sup>1418</sup> Some other CIOT-relevant PA ‘gaps’ include issues as to application, data anonymity, geolocation and law reform.

#### 5.3.1 Application

Subject to minor exceptions,<sup>1419</sup> the PA does not apply to small businesses<sup>1420</sup> with an annual turnover of \$3 million or less.<sup>1421</sup> This is a gap in the privacy regime given that many smaller players may be

---

body (APP 12.3(i)) ; or “reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process” (APP 12.3(j)).

<sup>1415</sup> APP 9 prohibits the use of “government related identifiers” subject to some exclusions. APP 12 deals with access rights (as in the *Grubb case* discussed above) and APP13 deals with correction of information which is inaccurate, out-of-date, incomplete, irrelevant or misleading for the purpose for which it is held: Guidelines, above n 1306 [13.30-13.41].

<sup>1416</sup> Productivity Commission, above n 1316: 183.

<sup>1417</sup> Telstra argued that releasing Mr Grubb’s metadata would unreasonably impact upon the privacy of other individuals: Privacy Commissioner v Telstra, above n 1282: [31].

<sup>1418</sup> Bennet Moses (2007) classifies regulatory failures in a technological change context in these four categories as cited in Manwaring, above n 836: 6.

<sup>1419</sup> These include private sector health providers (including private schools, childcare centres, GPs etc.), businesses that sell and purchase PI, credit reporting bodies, employees’ associations and contracted service providers for Commonwealth contracts.

<sup>1420</sup> Or not for profits. Note ‘small businesses’ does not include those with a related body corporate with a turnover exceeding the \$3M threshold: <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/information-sheet-private-sector-12-2001-coverage-of-and-exemptions-from-the-private-sector-provisions>

<sup>1421</sup> PA section 6EA provides that they may ‘opt-in’. If this link is accurate, there appears to be no entity which has decided to ‘opt in’ to date: <<http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/information-sheet-private-sector-12-2001-coverage-of-and-exemptions-from-the-private-sector-provisions>>

involved in consumer IOT data collection and is inconsistent with most international frameworks.<sup>1422</sup> Exceptions apply if a related body corporate is subject to the Act or the entity (inter alia)<sup>1423</sup> trades in a consumer's personal information<sup>1424</sup> without consent.<sup>1425</sup> This may catch some small data brokers and (the rare) CIOT data collector/ discloser who fails to insert consents in their terms. It should however be noted that the CIOT data market is latent and diverse, so absent consumers detecting an adverse downstream outcome (targeted advertising or notified data breach, for example) - from a linkable disclosure – the PA has little impact.

### 5.3.2 *Data Anonymity, De-identification – no one will know!*

“...businesses and consumer groups could benefit from “something more concrete against which to measure claims of de-identification and anonymity...”<sup>1426</sup>

Anonymised<sup>1427</sup> or de-identified<sup>1428</sup> data use is largely unregulated in Australia. Information is de-identified when “no longer” defined “PI”,<sup>1429</sup> through removal of personal identifiers<sup>1430</sup> and removal/ alteration of individually or collectively rare or unique attributes.<sup>1431</sup> OAIC Guidance<sup>1432</sup> permits de-identified data release,<sup>1433</sup> but warns re-identification risk warrants active assessment and management,

---

<sup>1422</sup> PC, ‘Big Data Report’ above n 41: 498-9. See for example, the New Zealand *Privacy Act 1993*; UK *Data Protection Act 1998*; GDPR; OECD Privacy Guidelines (revised 2013); APEC Privacy Framework 2005.

<sup>1423</sup> It also includes a health service provider as defined.

<sup>1424</sup> This means to disclose or collect an individual's PI by receiving or providing a “benefit, service or advantage...” to another. It is open as to the point at which CIOT device or software companies will be deemed ‘data brokers’ if their relative income earned from product sales versus data sales, is disproportional. However, given the proliferation of privacy policies with consents as to data sales, those companies will likely comply with the PA.

<sup>1425</sup> Or if mandated by law.

<sup>1426</sup> FTC, citing EPIC in Letter to Commenter (EPIC) RE In the Matter of Compete, Inc., Matter/File Number: 102 3155 (2013) <<https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competeepicletter.pdf>>

<sup>1427</sup> ‘Anonymisation’ means processing personal data to irreversibly prevent identification. Methods include randomisation, generalisation, pseudonymisation, noise addition, permutation, differential privacy, aggregation, k-anonymity, l-diversity and t-closeness. : EU, ‘Opinion 05/2014 on Anonymisation techniques’ *Article 29 Data Protection Working Party* (adopted 10 Apr 2014 accessed 15 Apr 2015) [3] <[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)>

<sup>1428</sup> ‘De-identification’ means that the information is no longer about an identified individual or one who is reasonably identifiable: *Privacy Act 1988* (Cth). section 6(1). It usually includes two aspects: firstly, removing personal identifiers (name, address, dob etc.) and secondly, removal/ alteration of other information which may allow identification (e.g. rare characteristics or a combination thereof): OAIC, ‘De-identification of Data and Information’ *Privacy Business Resource 4* (April 2014 accessed 20 Apr 2015) <[http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-business-resources/privacy\\_business\\_resource\\_4.pdf](http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-business-resources/privacy_business_resource_4.pdf)>

<sup>1429</sup> PA section 6 defines “deidentification” as where PI is no longer about an identifiable individual or one reasonably identifiable.

<sup>1430</sup> The Guidelines cite for example, name, address, dob, (etc).

<sup>1431</sup> OAIC, above n 1306: [B59 – 62]: 13

<sup>1432</sup> OAIC, ‘Privacy Business resource 4: De-identification of Data and Information’ (April 2014 accessed 9 Oct 2016) <<https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-4-de-identification-of-data-and-information>>

<sup>1433</sup> The OAIC allow ‘information asset’ release of de-identified data, provided that indirect identification risks are assessed and managed via a ‘motivated intruder’ test, an assessment is done ‘in the round’ and factors such as the cost, practicality, difficulty and likelihood of re-identification occurring are considered. ‘De-identification’ may occur through many methods which must be assessed in context: the OAIC list examples such as removing quasi-identifiers (eg. profession, income),

having regard to “cost, difficulty, practicality and likelihood”.<sup>1434</sup> The difficult question is the reasonable threshold beyond which re-identification risk becomes low or remote.<sup>1435</sup> To illustrate, Fitbit’s privacy terms allow them to sell or use aggregated, de-identified data, protected by “legal and technical measures”.<sup>1436</sup> But in 2013, CIA analysts could identify a person’s identity, height, weight and gender – using anonymised Fitbit data, or just “gait data alone.”<sup>1437</sup> Researchers explain that consumer IOT datasets are “sparse”, so only a few data points are often identifying: an MIT study re-identified 95% of the 1.5 million anonymised people, using only four annual smartphone location points.<sup>1438</sup> The problem is that big data, technological advance and consumer IOT granularity, allow individual or combined database points which “...will almost certainly” enable *re-identification*.<sup>1439</sup> In other words, as the Art 29 WP Opinions,<sup>1440</sup> data commissioner’s guidance,<sup>1441</sup> and the ICO *Code of Practice*<sup>1442</sup> acknowledge, current or future re-identification is a likely risk which increases with time.<sup>1443</sup>

---

combining identifying information into categories (e.g. ages into 25- 35); using ‘tolerable errors’; swapping information between data subjects to retain the same overall outcomes; using synthetic data and data suppression: OAIC, above n 181: 3- 4. ‘Motivated intruder’ test means whether a reasonably competent non-specialist but motivated person would be able to identify the data via resources such as the internet, public documents and reasonable enquiries. ‘In the round’ means an assessment of whether any entity or member of the public could identify an individual from the data, including in combination with other available information/ data.

<sup>1434</sup> OAIC, above n 1432.

<sup>1435</sup> Section 6 of the Privacy Act defines “deidentification” as where PI is no longer about an identifiable individual or one reasonably identifiable.

<sup>1436</sup> *Ibid.*

<sup>1437</sup> Peppet, above n 283: 129 citing Ira Hunt, Chief Technology Officer, ‘The CIA’s grand challenges with data’ (20 Mar 2013) <<http://gigaom.com/2013/03/20/even-the-cia-is-struggling-to-deal-with-the-volume-of-real-time-social-data/2> archived at <http://perma.cc/Q8DG-S2PL>>

<sup>1438</sup> Larry Hardesty, ‘How Hard is it to ‘De-Anonymise’ Cellphone Data?’ *MIT News* (27 Mar 2013 accessed 3 Mar 2016) <<http://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data>>. The four points involved locating a single phone user within a few hundred yards of a transmitter some time during an hour within a 12-month period. The cellphone location was inferred from the cell tower it was connected to, and the time of the connection fell within a one-hour interval. Each cellphone had a unique, randomly generated identifying number, so that its movement could be traced over time. But there was no information connecting that number to the phone’s owner. These are described as “fairly low spatial and temporal resolution” data sets.

<sup>1439</sup> Re-identification is not defined in the Privacy Act 1988 (Cth) but means turning de-identified data back into PI through reasonably reliable inference or data matching or similar techniques, either by reference to the dataset alone or through aggregation with other data. This may mean that *Privacy Act* consents have to be obtained post data collection (at the time of re-identification) which is so administratively difficult that businesses may either ‘lock up’ their data or ignore the Act: Reyhaneh Saadati and Alec Christie, ‘Big Data, Big issues? Is Australian Privacy Law keeping Up?’ *DLA Piper* (26 July 2013 accessed 25 Mar 2015) <[https://www.dlapiper.com/en/australia/insights/publications/2013/07/big-data-big-issues-is-australian-privacy-law-ke\\_/](https://www.dlapiper.com/en/australia/insights/publications/2013/07/big-data-big-issues-is-australian-privacy-law-ke_/)>

<sup>1440</sup> EU, Article 29, above n 1427; Opinion 03/2013 on Purpose Limitation (2013)

[http://ec.europa.eu/justice/data=protection/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](http://ec.europa.eu/justice/data=protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf)

<sup>1441</sup> (Ireland) DPC, ‘Anonymisation and pseudonymisation’ (2016 accessed 2 Oct 2016)

<<https://dataprotection.ie/viewdoc.asp?DocID=1594&ad=1>>

<sup>1442</sup> ICO, ‘Anonymisation Code of Practice’ (accessed 8 Aug 2016) <<https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>>

<sup>1443</sup> See the numerous examples cited in Bruce Schneier, ‘Why ‘Anonymous’ Data Sometimes Isn’t’ *WIRED* (13 Dec 2007 accessed 15 Apr 2015) <

[http://archive.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters\\_1213](http://archive.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213)>

Anonymisation failures abound.<sup>1444</sup> As the Irish DPC suggests, no technique is 100% effective to irreversibly anonymise data,<sup>1445</sup> which repeated public<sup>1446</sup> and private<sup>1447</sup> sector failures evidence. Practices such as data collection optimisation, “data fusion,”<sup>1448</sup> “matching,”<sup>1449</sup> “linking”<sup>1450</sup> and the “mosaic effect,”<sup>1451</sup> make de-identification a “limited proposition”<sup>1452</sup> and “...an illusion,”<sup>1453</sup> entailing “residual” privacy risk.<sup>1454</sup> There is no reason to expect that consumer IOT companies will de-identify data with any greater success. Indeed, faced with multiple failures, the Australian government has chosen hard law over technology. It is legislating to criminalise any attempt to re-identify de-identified government

---

<sup>1444</sup> For example, AOL released 19 million web searches of 700,000 anonymised consumers, only to find many of them re-identified publicly: Numeric IDs were attached to each of the 658,000 subscribers whose searches contained identifying personal information; e.g. name, location and social security data: Anick Jesdanun, ‘AOL: Breach of Privacy Was a Mistake’ *The Washington Post* (7 Aug 2006 accessed 15 Apr 2015) < [http://www.washingtonpost.com/wp-dyn/content/article/2006/08/07/AR2006080700790\\_2.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/08/07/AR2006080700790_2.html)> A researcher identified a US state governor from supposedly de-identified public health data. The Massachusetts Group Insurance Commission (GIC) released anonymised data as to state employee hospital visits for researcher use – which the Governor assured everyone were private as identifiers had been removed. Latanya Sweeney decided to test that proposition; she knew the governor’s city, purchased the voting roll and combined the voter information – name, address, postcode and dob - with the GIC records. Her study revealed 6 people with his dob, 3 were male and only he had the right postcode. She thus located the Governor’s data, which she sent to his office: Nate Anderson, “‘Anonymized’ data really isn’t—and here’s why not’ *Ars Technica* (8 Sept 2009 accessed 15 Apr 2015) <http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/>> In 2009, Netflix was sued by class action for allegedly voluntarily disclosing the personal information of 480,000 subscribers when it provided contest participants with data sets containing over 100 million subscriber movie ratings and preferences, to improve its recommendation system data. The damage alleged included that movie watching history would “...identify or permit inference of her sexual orientation...” which would adversely affect her livelihood and family life in their community: *Valdez-Marquez, Sinopli, Navarro et al v Netflix, Inc.* U.S. District Court for the Northern District of California, San Jose Division, Civil Action No. c09 05903) <<http://privacylaw.proskauer.com/uploads/file/doe-v-netflix.pdf>> (17 Dec 2009) The case settled.

<sup>1445</sup> (Irish) DPC, above n 1441.

<sup>1446</sup> In 2016 anonymised Australian Government health data was promptly re-identified, and within one week, anonymised employee census data of 100,000 employees was withdrawn, for fear of re-identification: C. Culnane, Benjamin Rubenstein and Vanessa Teague, ‘Understanding the maths crucial for protecting privacy’ *Pursuit, Dept of Engineering and Technology* (29 Sept 2016 accessed 5 Oct 2016) <<https://pursuit.unimelb.edu.au/articles/understanding-the-maths-is-crucial-for-protecting-privacy>> The latter dataset was downloaded at least 58 times before the error was realised: Noel Towell, ‘96,000 public servants in new data breach’ *The Canberra Times* (5 October 2016 accessed 10 Oct 2016) < <http://www.canberratimes.com.au/national/public-service/96000-public-servants-in-new-data-breach-20161004-grul2p.html>>

<sup>1447</sup> One study found that 25% of websites shared personal login details with third parties, including sexual orientation and drug use habits: Valentino-DeVries, above n 752. OkCupid for example sent user names to one company, gender, age and postcode data to seven companies, drug use to six companies and sexual orientation to two companies – but claims that as sent, it is all ‘anonymized’, but this may not prevent re-identification especially in combination.

<sup>1448</sup> Executive Office of the President, above n 41 (Big Data). For example, data brokers are known to reattach individual personal data obtained from retailers to anonymised browsing history, to provide a whole new analysed data set for retailer’s marketing use: Jennifer Valentino-DeVries, above n 752.

<sup>1449</sup> Data matching means comparing multiple systems of records to aggregate data about an already identified subject.

<sup>1450</sup> Data linking means linking identified and anonymous databases to de-anonymise or re-identify anonymous data by identifying data fingerprints, which may often then be linked to other data sets.

<sup>1451</sup> Ibid: this means the integration of big data whereby personally identifiable information can be derived or inferred from supposedly de-identified datasets.

<sup>1452</sup> PCAST Report, ‘Big Data and Privacy’ Harvard Law Petrie-Flom Center, *Online Symposium on the Law, Ethics and Science of Re-identification Demonstrations* (2013) 8.

<sup>1453</sup> Data from just four ‘anonymous’ credit card purchases can identify 90% of people: Jamie Condliffe, ‘Anonymised Credit Card Data Really Isn’t Very Anonymous’ *Gizmodo* (31 Jan 2015 accessed 15 Apr 2015) <<http://www.gizmodo.com.au/2015/01/anonymized-credit-card-data-really-isnt-very-anonymous/>>

<sup>1454</sup> The EU opinion concluded that unless engineered properly and constantly revised to reflect latest technology developments, anonymization presents “residual risks” to consumers: EU, above n 182.

data, or to publish or communicate any re-identified dataset<sup>1455</sup>- but consumer PI will not attract the same protection. In the meantime, the OAIC is rewriting its guidance, warning that privacy impact assessments must always be undertaken when assessing de-identification in a big data world.<sup>1456</sup>

### 5.3.3 Geolocation

Smart device and app geolocation is ubiquitous, useful<sup>1457</sup> and uniquely privacy intrusive.<sup>1458</sup> Location data is created when electronic devices are trackable via GPS or Wi Fi, and is revelatory of vast tracts of SI/PI, including home and workplace, “social graph”,<sup>1459</sup> behavioural patterns, “business connections, political affiliations or medical conditions”<sup>1460</sup> or other correlations of inferable purpose.<sup>1461</sup> Of all anonymised data, it is readily re-identified and where public, tracking creates “...new risks ranging from data theft to burglary, to even physical aggression and stalking.”<sup>1462</sup> The recent Telstra case suggests that geolocation metadata is not PI, insofar as it may not be “about” an (identified) individual. In contrast, Uber were prosecuted for privacy-intrusive geolocation practices<sup>1463</sup> and the Irish DPC regards location-revealing home-router data<sup>1464</sup> and smart car geolocation data, as PI.<sup>1465</sup> If location metadata is not PI in Australia, then legislative resolution is required; cases are too few and slow, and the federal government

---

<sup>1455</sup> Senator George Brandis, ‘Amendment to the Privacy Act to Further Protect De-Identified Data’ *Media release* (28 Sept 2016 accessed 29 Sept 2016) <<https://www.attorneygeneral.gov.au/Mediareleases/Pages/2016/ThirdQuarter/Amendment-to-the-Privacy-Act-to-further-protect-de-identified-data.aspx>>

<sup>1456</sup> The OAIC advises in its latest draft guide, that privacy impact assessments should always be used when assessing de-identification and using big data. That assessment should consider the range of information, algorithms and how data will be used or disclosed: OAIC, above n 1316: 5. The final has not been released as at submission date.

<sup>1457</sup> Geolocation permits geographically-relevant services such as the maps, navigation, weather, restaurants and so on. Other examples also include augmented reality, geotagging internet content, tracking people (friends, children etc.), and (sometimes useful) location based advertising.

<sup>1458</sup> The Art 29 WG suggest it can be secret (through app updates) or ‘semi-secret’ – people may forget the setting, not be properly informed location services are ‘on, or when settings change from ‘private’ to ‘public’.

<sup>1459</sup> Philippe Golle and Kurt Partridge, ‘On the anonymity of Home/ Work Location pairs’ *Stanford University* (n.d. accessed 3 Aug 2016) <<http://crypto.stanford.edu/~pgolle/papers/commute.pdf>>; Philippe Golle and Kurt Partridge ‘Your Morning Commute Is Unique: On The Anonymity Of Home/Work Location Pairs’ (13 May 2009 accessed 3 Aug 2016) <<https://33bits.org/2009/05/13/your-morning-commute-is-unique-on-the-anonymity-of-homework-location-pairs/>>

<sup>1460</sup> Golle, *ibid*.

<sup>1461</sup> Data Protection Commissioner (Ireland), above n 346.

<sup>1462</sup> *Ibid*.

<sup>1463</sup> New York Attorney-General, ‘A.G. Schneiderman Announces Settlement with Uber to Enhance Rider Privacy’ *Media release* (Jan 2016 accessed 2 Nov 2016) <<http://www.ag.ny.gov/press-release/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy>> These included to encrypt passenger geo-location information, adopt multi-factor authentication pre-employee PI access, etc. Uber also had to pay \$20,000 with respect to an un-notified data breach. After the AG opened an investigation into Uber’s collection, maintenance and disclosure of rider personal information amid reports that Uber executives had access to riders’ locations and that Uber displayed this information in an aerial view, known internally as “God View.” Note their Jan 2015 New York Attorney General’s Office settlement which mandated Uber encrypt its user data: <<http://www.ag.ny.gov/press-release/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy>>

<sup>1464</sup> Irish DPC, above n 346.

<sup>1465</sup> Irish DPC, above n 346. For smart cars, the Irish DPC distinguishes between data as to a private or company vehicle (the location of which is linked to a living person) versus an autonomous taxi carrying unidentifiable persons, but it seems unlikely that any smart car would ever not collect occupant-identifying PI whether via camera, booking or payments systems.

has already, in its data retention regime, accepted that such information is best privacy-protected as “personal”.

#### 5.3.4 Law reform.... again

One Australian desktop IOT privacy study<sup>1466</sup> found legal ‘gaps’ as to ubiquitous, international collection and security,<sup>1467</sup> and concluded that the PA “cannot keep up with, or properly protect security,<sup>1468</sup> privacy rights management and personal information control”.<sup>1469</sup> Another analysed CIOT privacy harms utilising Solove’s taxonomy;<sup>1470</sup> and upon author revision, every identified harm as to information collection;<sup>1471</sup> processing,<sup>1472</sup> dissemination;<sup>1473</sup> and private affairs invasion<sup>1474</sup>, is “relevant” in a CIOT context. While Thierer asserts that data breach alone is not a “harm”,<sup>1475</sup> EU and (some) US authority disagrees, and Australia’s new mandatory data breach scheme hinges upon finding “serious [individual] harm” in breach.

Successive Australian enquiries have recommended a statutory privacy tort to redress privacy harms,<sup>1476</sup> to prohibit intrusions into a person’s “seclusion or private affairs (including by unlawful surveillance)”; and the misuse or disclosure of PI. A tort, distinct from the OAIC approach in privately and impartially<sup>1477</sup> conciliating most consumer privacy complaints,<sup>1478</sup> would strengthen consumer options to enforce privacy

---

<sup>1466</sup> This was assessed through four themes derived from a literature review: unauthorised surveillance, uncontrolled data generation and use, inadequate authentication and information security risk. Xavier Caron, Pachellos Bosua, Sean B. Maynard and Atif Ahmad, ‘The Internet of things (IoT) and its impact on individual privacy: An Australian perspective’ *Computer Law and Security Review* 32 (2016) 4- 14

<sup>1467</sup> Ibid. The only other Australian desktop review found (without real legal analysis) that privacy law would be sufficient. This accorded with NTC findings as C-ITS and autonomous vehicles; again, based upon submissions rather than rigorous legal analysis.

<sup>1468</sup> Ibid.

<sup>1469</sup> Ibid: 13.

<sup>1470</sup> Daniel Solove, ‘A Taxonomy of Privacy’ *University of Pennsylvania Law Review* 154: 3 (Jan 2006 accessed 21 Apr 2016): 477- 564 <<http://www.jstor.org/stable/40041279>>. this exercise was first undertaken by Vulkanovski, above n 110, but in a different manner.

<sup>1471</sup> Subcategories are: surveillance, interrogation

<sup>1472</sup> Subcategories are: aggregation, identification, insecurity, secondary use, exclusion

<sup>1473</sup> Subcategories are: breach of confidentiality, disclosure, exposure, increased accessibility, blackmail or extortion, appropriation, distortion.

<sup>1474</sup> intrusion and decisional interference.

<sup>1475</sup> Section 40A requires the OAIC make a reasonable attempt to conciliate a complaint. It states that “Most complaints are resolved in this way”: OAIC, above n 1255: 6 [28].

<sup>1476</sup> Both the UK and NZ recognise a tort of misuse of private information and a tort of intrusion upon seclusion. See for UK: *Vidal-Hall v Google* [2014] EWHC 13 (QB); and NZ: *Hosking v Runting* (2004) 7 HRNZ 301; (2005) 1 NZLR 1; *C v Holland* [2012] NZHC 2155. The USA has recognised a common law right of privacy for almost a century: Ruth McColl, “Privacy, Business and the Digital Era” [2014] *NSWJSchol* 15 <<http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/NSWJSchol/2014/15.html?stem=0&synonyms=0&query=APP1.3>>

<sup>1477</sup> Chapter 1 [1.15] The APC does not advocate and the process is “free, informal and accessible” without requirement for legal representation but each bears their own costs. OAIC, above n 1311.

<sup>1478</sup> OAIC, above n 1255 and OAIC, above n 1311.

rights publicly in a CIOT context. As the possibility was left open by the High Court<sup>1479</sup> and its nature, operation and necessity has been repeatedly recommended by authoritative Australian enquiries 2008-2015,<sup>1480</sup> this reform is not explored further here.

Given the multiple gaps identified as to the APPs and that open data regime proposals are premised (largely) upon access,<sup>1481</sup> it seems clear that Australian consumer privacy protections and industry compliance would be strengthened by proactive public consumer litigation, in addition to the private PA complaints-managed regime.

#### 5.4 (Un) smart privacy cases

*“... universal notions of privacy and security don’t necessarily translate to the Internet of Things...”*<sup>1482</sup>

There are no Australian CIOT-related privacy cases. But international cases are factually illustrative and invite questions as to the PA’s capacity to respond. Recent examples concern smartTVs,<sup>1483</sup> Amazon’s ‘Alexa’, Google Nest Cam,<sup>1484</sup> and computer<sup>1485</sup> and Xbox<sup>1486</sup> ‘spy’ software. In 2013, LG’s smart TV was ‘caught’ collecting consumer data without any opt out<sup>1487</sup> and in 2016, EPIC filed a FTC complaint alleging<sup>1488</sup> that Samsung smart TV voice-recognition involves deceptive and unfair practices, by

---

<sup>1479</sup> *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199. Two lower court decisions recognised a tort of invasion of privacy as well, though both settled before an appellate decision could be given. See *Grosse v Purvis* [2003] QDC 151 (16 June 2003); *Doe v Australian Broadcasting Corporation* [2007] VCC 281.

<sup>1480</sup> ALRC, above n 1235; Australian Law Reform Commission, ‘For your Information: Privacy Law and Practice’ Report No. 108 (May 2008 accessed 5 Jan 2016) <[https://www.alrc.gov.au/sites/default/files/pdfs/108\\_vol1.pdf](https://www.alrc.gov.au/sites/default/files/pdfs/108_vol1.pdf)>; NSW Law Reform Commission, ‘Invasion of Privacy’ Report No. 120 (3 Mar 2016 accessed 5 Jun 2016) <>; ALRC, above n 1235; Victorian Law Reform Commission, ‘Surveillance in Public Places’ Report 18 (12 Aug 2010 accessed 3 Apr 2016) <<http://www.lawreform.vic.gov.au/projects/surveillance-public-places/surveillance-public-places-final-report>> Privacy torts exist in both the US and the UK.

<sup>1481</sup> Productivity Commission, above n 190 Ch. 9.

<sup>1482</sup> Ben Warlick, attorney with Morris, Manning and Martin in Atlanta, cited in AP, ‘Hello Barbie and Security Not the Perfect Couple, Claims Lawsuit’ *Investor’s Business Daily* (n.d. 2015 accessed 15 Jan 2017) <<http://www.investors.com/news/technology/hello-barbie-security-not-the-perfect-couple-claims-lawsuit/>>

<sup>1483</sup> EPIC, above n 356.

<sup>1484</sup> EPIC, ‘Request for Workshop and Investigation of ‘Always On’ Consumer Devices’, *Letter to US Department of Justice and the FTC* (10 Jul 2015 accessed 4 Feb 2016) <<https://epic.org/2015/07/epic-urges-investigation-of-al.html>>

<sup>1485</sup> Google’s Chromium browser: EPIC assert that Chromium browser software turns on computer microphones, to listen for the “OK Google” prompt which results in “constant voice recording” in private homes: *Ibid*: 2.

<sup>1486</sup> Microsoft’s ‘Kinect’ in Xbox consoles, monitors voices until it hears a command, even when it is ‘off’: T C Sottek, ‘The Xbox One will always be listening to you, in your own home’ *The Verge* (21 May 2013 accessed 4 Feb 2016) <<http://www.theverge.com/2013/5/21/4352596/the-xbox-one-is-always-listening>> cited in EPIC, *Ibid*: footnote 16.

<sup>1487</sup> The TV reported to LG every channel change, scanning all shared files on the home network and its opt-out mechanism did not work: Justin Brookman, ‘Eroding Trust: How New Smart TV Lacks privacy by design and Transparency’ (27 Nov 2013 accessed 26 Apr 2016) <<https://iapp.org/news/a/eroding-trust-how-new-smart-tv-lacks-privacy-by-design-and-transparency/>>

<sup>1488</sup> Samsung, above n 356.

recording users and by internet-transmission for third party processing, together with device data and IP address.<sup>1489</sup> Samsung's Privacy Policy disclosed this, but (EPIC say unfairly) disclaimed responsibility for third party privacy and security standards,<sup>1490</sup> arguing that consumers could not reasonably anticipate their TV transmitting private conversations to another company. The FTC has since warned 'always-on' app developers not to spy on viewing habits,<sup>1491</sup> and pursued the Vizio case,<sup>1492</sup> which highlighted default tracking. Vizio did not notify consumers or obtain consent; but covertly linked registration PI with viewing history which it on-sold to third parties, including cross-device advertisers. Clearly, this deceptive 'omission' violates the ACL (**Ch. 4**), and breaches APPs 3, 5 and 6 (and others) as to non-disclosure of non-related purposes, nor would (express) consent be inferable, given data is likely PI if not SI. Samsung has also been accused,<sup>1493</sup> but notified their tracking in a bundled consent with a one click "opt in", so even if a once-off, buried mid sign-up process, this would comply with APP requirements.<sup>1494</sup> Of course the consent fallacy is that the person who clicks 'accept' for all device viewers, may lack legal authority or capacity. In its specificity, the FTC settlement illustrates Australia's 'so-so' privacy regime: it requires affirmative express consent and "prominent disclosure", separate from other terms, as to collected/shared data type, the identity or specific categories of third party recipients and "all [sharing] purposes". "Prominent" disclosure must be noticeable, unavoidable and understandable by ordinary consumers<sup>1495</sup> without inconsistency or contradiction.<sup>1496</sup> While the PA mandates disclosure, there is regulatory

---

<sup>1489</sup> EPIC, above n 356. The complaint alleges breach of section 5, as well as the Electronic communications Privacy Act (which prohibits interception of oral communications", and COPPA as to children.

<sup>1490</sup> The policy stated "You should exercise caution and review the privacy statements applicable to the third-party websites and services you use".

<sup>1491</sup> Email from Claire Gartland, EPIC Consumer Protection Counsel to author, 11 Aug 2016.

<sup>1492</sup> *Federal Trade Commission, Attorney General of the State of New Jersey, and NJ Division of Consumer Affairs v. VIZIO INC. and VIZIO Inscape Services, LLC*, Case 2:17-cv-00758, Filed 6 Feb 2017 <<https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc>>

INCL 'Complaint for Permanent Injunction and Other Equitable and Monetary Relief'

<[https://www.ftc.gov/system/files/documents/cases/170206\\_vizio\\_2017.02.06\\_complaint.pdf](https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf)> and 'Stipulated Order for Permanent Injunction and Monetary Judgment'

[https://www.ftc.gov/system/files/documents/cases/170206\\_vizio\\_stipulated\\_proposed\\_order.pdf](https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf) and 'Concurring Statement of Acting Chairman Maureen K. Ohlhausen In the Matter of Vizio, Inc.'

<[https://www.ftc.gov/system/files/documents/public\\_statements/1070773/vizio\\_concurring\\_statement\\_of\\_chairman\\_ohlhaus\\_en\\_2-6-17.pdf](https://www.ftc.gov/system/files/documents/public_statements/1070773/vizio_concurring_statement_of_chairman_ohlhaus_en_2-6-17.pdf)>

<sup>1493</sup> EPIC, above n 356.

<sup>1494</sup> EPIC alleged that: "When the voice recognition feature is enabled, everything a user says in front of the Samsung SmartTV is recorded and transmitted over the internet to a third party regardless of whether it is related to the provision of the service": EPIC, *Ibid*. California has enacted laws to address smart TV voice recognition privacy and disclosures:

Assembly Bill No. 1116, 2015-16, <[https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\\_id=201520160AB1116](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1116)> c/f Samsung deny the accusation: Samsung, above n 356.

<sup>1495</sup> If targeted to children, elderly, terminally ill etc. then they include reasonable members of those groups. Disclosure must by both syntax and diction understandable to ordinary consumers and appear in each language in which the 'triggering representation' appears.

<sup>1496</sup> *FTC v Vizio*, above n 1492: Order II as to Notice and Affirmative Express Consent. Prominent disclosure requires: Visual disclosure: by size, location, contrast, length of time it appears and other characteristics, to stand out contextually so it is "easily noticed read and understood"; Audible disclosure: delivered at volume, speed and cadence sufficient to hear and understand; and where delivered by any interactive electronic medium communication: (e.g. firmware update), it must be "unavoidable".

uncertainty as neither the PA or Guidelines specify substantive compliance, such that the standards required become a question for judicial interpretation rather than industry knowledge and regulatory control.

In 2016, a class action<sup>1497</sup> alleging that We-Vibe 4+ smart vibrators “secretly collect and transmit highly sensitive personally identifiable [user] information”, settled.<sup>1498</sup> Remotely app-controllable, the device enabled “connected lover” sessions, and without notice or consent, recorded use date and time, and settings<sup>1499</sup> which it transmitted with the user’s email address to cross-border servers. The settlement (without admission) involved a USD\$3.7 million, with up to \$10,000 to each customer.<sup>1500</sup> While mildly-amusing and privacy-offensive in turn, the case illustrates that lawful data disclosure,<sup>1501</sup> breach or extortion has a darker side, when device ‘use’ is illegal in several US states<sup>1502</sup> and countries.<sup>1503</sup> No less dark are “creepy, eavesdropping” smart toys. ‘CloudPet’ is a smart stuffed-animal marketed as “a message you can hug”, but has allegedly exposed over 800,000 customer credentials and 2 million children’s voice recordings – which were stored in an insecure internet-accessible database.<sup>1504</sup> Security experts describe the breach as “sinister” and “unforgiveable”.<sup>1505</sup> Mattel’s ‘Hello Barbie’,<sup>1506</sup> sparked an

---

<sup>1497</sup> Prompted by a DefCon security exposé. A software flaw also enabled a hacker to control the device remotely: Ry Crist, ‘Screwed by sex toy spying? You may get \$10k’ CNET (15 Mar 2017 accessed 20 Mar 2017) <<https://www.cnet.com/au/news/app-enabled-sex-toy-users-get-10000-each-after-privacy-breach/>>

<sup>1498</sup> *N.P. & Ors v Standard innovation (US) Corp bda We-Vibe*, Case No 1:16-cv-8655, United States District Court of Illinois (Filed 2 Sept 2016) <<https://www.cnet.com/news/internet-connected-vibrator-we-vibe-lawsuit-privacy-data/>>

<sup>1499</sup> These included device temperature, vibration level and mode.

<sup>1500</sup> Customers who used only the vibrator (not the app) receive up to \$199.

<sup>1501</sup> The app Terms of Use included usual clauses allowing the manufacturer to divulge device use data upon court order.

<sup>1502</sup> In *1568 Montgomery Highway v. City of Hoover (2009)*, the Alabama Supreme Court upheld as constitutional a statute prohibiting the sale of “any device designed ... primarily for the stimulation of human genital organs” - which targeted dildos and vibrators. The court concluded the rationale was “public morality” and as there is no recognised constitutional right to sexual freedom, the law should be upheld.

<sup>1503</sup> For example, penalties include public lashings (Saudi Arabia) and 32 months jail (Indonesia).

<sup>1504</sup> Alex Hern, ‘CloudPets stuffed toys leak details of half a million users’ *The Guardian* (1 Mar 2017 accessed 14 Mar 2017) <https://www.theguardian.com/technology/2017/feb/28/cloudpets-data-breach-leaks-details-of-500000-children-and-adults> Details included email addresses and passwords, profile pictures, and voice recordings; while the company denied the latter, experts report that the recordings were accessible via the url, which is in turn accessible via the app. Password requirements were also described as “lax” so “trivial” to hack. The records are being traded online according to ‘Have I Been Pwned’ data breach website. CloudPets did not notify users of the hack.

<sup>1505</sup> John Madelin, CEO of RelianceACSN quoted Ibid.

<sup>1506</sup> Samuel Gibbs, ‘Hackers can hijack Wi-Fi Hello Barbie to spy on your children’ *The Guardian* (26 Nov 2015 accessed 10 May 2016) < <https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children>>; Samuel Gibbs, above n 618; NBC, ‘New Wi-Fi Enabled Barbie Can be Hacked, researchers Say’ NBC 5 Reports (17 Dec 2015 accessed 10 May 2016) [http://www.nbcchicago.com/investigations/WEB-10p-pkg-Surveillance-Toy\\_Leitner\\_Chicago-353434911.html](http://www.nbcchicago.com/investigations/WEB-10p-pkg-Surveillance-Toy_Leitner_Chicago-353434911.html)> See Toy Talk, ‘Hello Barbie Companion Application Terms of Use’ (14 Oct 2015 accessed 10 May 2016) <https://toytalk.com/hellobarbie/terms/>; Toy Talk, ‘Privacy Policy’ and ‘Children’s Privacy Policy’ (Last revised 11 Jan 2016 accessed 10 May 2016) < <https://www.toytalk.com/legal/privacy/>>; Toy Talk, ‘Hello Barbie Privacy Policy’ (Last Revised 5 Jan 2016 accessed 10 May 2016) < <https://www.toytalk.com/hellobarbie/privacy/>>; Manta, Irina D & David S. Olson, ‘Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly.’ 67 *Alabama Law Review* 135 (2015) <[https://law.depaul.edu/about/centers-and-institutes/center-for-intellectual-property-law-and-information-technology/programs/ip-scholars-conference/Documents/ipsc\\_2015/abstracts-papers-presentation/OlsonD\\_abstract.pdf](https://law.depaul.edu/about/centers-and-institutes/center-for-intellectual-property-law-and-information-technology/programs/ip-scholars-conference/Documents/ipsc_2015/abstracts-papers-presentation/OlsonD_abstract.pdf)>

EU state investigation and a class action seeking injunctions and damages for an “inherently dangerous product” involving “...unlawful and negligent collection, use and distribution of minor’s personal information”.<sup>1507</sup> In 2016 both the FTC and EU<sup>1508</sup> initiated actions against ‘My Friend Cayla’ and ‘i-Que robot’ smart toys, which like Hello Barbie, use speech recognition software via a smartphone-pairable app, doll microphone and speakers, to “talk” to children.<sup>1509</sup> The toys record interactions, and are allegedly, readily hackable.<sup>1510</sup> The FTC complaint alleges privacy consent and consumer protection legislation breaches,<sup>1511</sup> while EU complaints allege the toys violate Directives,<sup>1512</sup> and breach ‘unfair terms’, data minimisation principles,<sup>1513</sup> and enable (partly-unidentified) third party data sharing subject to their ‘unfair’ terms.<sup>1514</sup> The terms may also enable profiling and targeted advertising to children<sup>1515</sup> and

---

<sup>1507</sup> *Archer-Hayes & C.H. and Johnson & AP. & Ors v. ToyTalk Inc, Mattel Inc., Samet Privacy LLC dba Kidsafe Seal Program & Ors*, Class Action Complaint, Case No. BC 603467 Superior Court of California (Filed 7 Dec 2015) <http://www.coppanow.com/wp-content/uploads/HelloBarbieComplaint.pdf> The case pleads Violation of the Unfair Competition Law, Negligence, Unjust Enrichment (they made money on the doll where they shouldn’t have) and Invasion of Privacy and COPPA. The latter Act provides it is unlawful an online service directed to children to collect personal information from a child without (1) providing notice of what information is collected, how it is used, and its disclosure practices; and (2) obtaining verifiable parental consent. Moreover, the operator must provide parents with (1) a description of the information collected; (2) the opportunity to refuse to permit further use, maintenance, or future collection of personal information from the child; and (3) reasonable means to obtain any personal information collected from the child. The operator is further required “to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children [which includes identifying and contact information, geolocation and voice in audio file etc.]: 15 USC 6501 (8)

<sup>1508</sup> They filed with EU Commission, the International Consumer Protection and Enforcement Network, and national DPAs in Norway, Greece, Belgium, France, the Netherlands and Ireland

<sup>1509</sup> The software locates answers to questions either from a list of pre-programmed answers, or from limited internet sources (e.g. Wikipedia, Google and Weather Underground).

<sup>1510</sup> Any smartphone can connect to Cayla via Bluetooth, even without physical access, due to an “inadequate quality” Bluetooth chip and no mechanical barriers. See the complaint-supporting research from Norway: FORBRUKERRÅDET, ‘Report: Investigation of privacy and security issues with smart toys’ (2 Nov 2016 accessed 15 Jan 2017) <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf>; FORBRUKERRÅDET, ‘#Toyfail’ (Dec 2016 accessed 15 Jan 2017) <<https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf>>

<sup>1511</sup> *In the Matter of Genesis Toys and Nuance Communications*, ‘Complaint and Request for Investigation, injunction, and other relief’, Submitted by The Electronic Privacy Information Center, The Campaign for a Commercial Free Childhood, The Center for Digital Democracy and the Consumers Union (6 Dec 2016 accessed 12 Dec 2016) <<https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf>> The privacy/ consent-related breach was of the COPPA legislation as to their failure to obtain parental consent for information collection for children under 13. Note the GDPR consent age is 15, although member states can reduce it to 13 or 14.

<sup>1512</sup> Data Protection Directive and Unfair Contract Terms Directive. See for example, the complaint to the Norwegian Data protection Authority and The Consumer ombudsman, FORBRUKERRÅDET, ‘Complaint regarding user agreements and privacy policies for internet-connected toys –the Cayla doll and i-Que robot’ (6 Dec 2016 accessed 15 Jan 2017) <<https://fil.forbrukerradet.no/wp-content/uploads/2016/12/complaint-dpa-co.pdf>>

<sup>1513</sup> The terms required smartphone contact access, without justification.

<sup>1514</sup> Unfair terms included a failure to notify consumers before terms changes, data collection exceeding the collection purpose and breaching data minimisation, plus amending privacy policy without notice, the right to use and transfer voice data to third parties, and non-transparent data deletion policies: *Ibid*: 4.

<sup>1515</sup> They allegedly link anonymised and personal information, with publicly available user data for this purpose. Note that the US ‘Instructions’ claim that there “will be no data mining”: <[https://media.wix.com/ugd/a340e5\\_ee88af1dba447a2a1a344d7d872b700.pdf](https://media.wix.com/ugd/a340e5_ee88af1dba447a2a1a344d7d872b700.pdf)>

that certain toy 'answers' constitute marketing. The dolls are banned in Germany as surveillance devices,<sup>1516</sup> but are still sold in Australia.<sup>1517</sup>

Australian regulators may be waiting upon outcomes; but relying upon Norwegian investigation findings, there are potential breaches of APP1 (low privacy policy accessibility); APP3 (collection beyond that required- the apps access parent contacts); APP6 (non-consensual SI use);<sup>1518</sup> APP7 (cross-border data flows); APP 11 (excess data retention).<sup>1519</sup> APP12 as to lax data security; APP 13 (data cannot readily be deleted).<sup>1520</sup> That such privacy-adverse terms proliferate reflects the low likelihood of OAIC action; indeed, the ACCC has its eye on smart toys<sup>1521</sup> and seems far more likely to take them on.

## 5.5 OAIC privacy enforcement performance

*My priority is protecting Australian's personal information in the digital age... [and] to help businesses and the wider community take privacy in their hands.'* – Timothy Pilgrim<sup>1522</sup>

*"We are uniquely placed to bring government, business and technical expertise together to address the privacy dimensions of these technologies to protect both individual privacy, and organisational reputation."*<sup>1523</sup>

The FTC's "current privacy enforcement priorities" include the internet of things, and data security.<sup>1524</sup> FTC CIOT cases are discussed in Ch. 4,<sup>1525</sup> and it continues to successfully assert its jurisdiction.<sup>1526</sup> The EU has an even greater privacy and security case inventory, backed by significant penalties and the

---

<sup>1516</sup> Germany's Federal Network Agency (Bundesnetzagentur) says the toy is banned as "unauthorised wireless transmitting equipment" as it transmits signals and records sound without detection

<sup>1517</sup> See <https://www.myfriendcayla.com/shop-australia>.

<sup>1518</sup> Ibid: 24.

<sup>1519</sup> "...it is not always possible to completely remove all of your information from our databases... because of backups, or other reasons...": Ibid: 25

<sup>1520</sup> Ibid: 25

<sup>1521</sup> Discussion between Delia Rickard and author.

<sup>1522</sup> Pilgrim, above n 1225.

<sup>1523</sup> Timothy Pilgrim cited in OAIC, above n 1229.

<sup>1524</sup> FTC, 'Prepared Statement on Oversight of the Federal Trade Commission' United States Senate (27 Sept 2016 accessed 2 Oct 2016): 8

<[https://www.ftc.gov/system/files/documents/public\\_statements/986433/commission\\_testimony\\_oversight\\_senate\\_09272016.pdf](https://www.ftc.gov/system/files/documents/public_statements/986433/commission_testimony_oversight_senate_09272016.pdf)>

<sup>1525</sup> Ibid: 10. To put this activity in context, the FTC filed over 160 consumer protection complaints, obtained over 300 permanent injunctions/ orders requiring payment of over \$1.6 billion in consumer redress or disgorgement of funds.

Referrals to the Dept of Justice led to 40 judgments and penalties around \$43 million: FTC, Ibid: 3.

<sup>1526</sup> Its application of principles similar in effect to APP 11 is currently under appeal in *LabMD Inc. v FTC*, above n 650.

incoming GDPR;<sup>1527</sup> indeed, the UK's ICO has imposed over £7.8 million in civil penalties.<sup>1528</sup> In contrast, the OAIC is criticised as a "toothless tiger",<sup>1529</sup> and despite enhanced enforcement powers and positive rhetoric,<sup>1530</sup> there is little case-based evidence of improved strategy, policy or approach.<sup>1531</sup> The OAIC's privacy performance is modest, to say the least: in 2015-6 it made seven determinations,<sup>1532</sup> oversaw 123 data breach notifications (none prosecuted), accepted two enforceable undertakings,<sup>1533</sup> conducted 17 self-initiated investigations (s 40(2)), and 21 privacy assessments,<sup>1534</sup> and one court case as the sum

---

<sup>1527</sup> Laraine Laudati, 'Summaries of EU Court Decisions Relating to Data Protection 2000- 2015' Data protection Office & European Anti-Fraud Office (OLAF) (28 Jan 2016 accessed 5 Mar 2016) <[https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw\\_2001\\_2015\\_en.pdf](https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf)> The GDPR applies EU-wide from May 2018. It increases compliance requirements, and imposes significant financial penalties of (whichever greater) up to €20m or 4% of annual worldwide turnover for company groups. These apply to infringements of principles as to processing, including consent conditions, data subject rights, international data transfers, national law obligations allowable under the GDPR, and data protection authority orders including data flow suspension. Commentators suggest that the fines are so significant that firms will take them very seriously leading to behavioural changes. Infringements for entities such as Google, Microsoft, Apple and Facebook could result in fines worth billions.

<sup>1528</sup> ICO, 'Actions we've taken' (accessed 20 Nov 2016) <https://ico.org.uk/action-weve-taken/> This includes 80 undertakings, 52 monetary penalties, 33 enforcement notices, and 25 prosecutions – in 2016 alone. It has also undertaken 157 Audits, advisory visits and overview reports: see <[https://ico.org.uk/action-weve-taken/enforcement/?facet\\_type=Prosecutions&facet\\_sector=&facet\\_date=&date\\_from=&date\\_to=>](https://ico.org.uk/action-weve-taken/enforcement/?facet_type=Prosecutions&facet_sector=&facet_date=&date_from=&date_to=>)

<sup>1529</sup> "The ALRC often heard concerns that the *Privacy Act* is a 'toothless tiger', lacking adequate enforcement mechanisms and sufficient sanctions to ensure compliance...": ALRC, 'Executive Summary' *ALRC Report 108* (2008 accessed 20 Apr 2015) <<http://www.alrc.gov.au/publications/Executive%20Summary/extensive-public-engagement#>>; Matt Goodwin, 'Toothless Tiger...Now With Teeth' *Pigott Stinson* (3 Sept 2013 accessed 20 Apr 2015) <<http://pigott.com.au/publications/toothless-tigernow-with-teeth/>> See for example, the outcome of the first case of privacy breach when the new powers applied: OAIC, 'Optus Enforceable undertaking' (n.d. 2015) <<http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/enforceable-undertakings/enforceable-undertaking-optus.pdf>> See also critique of the OAIC's own motions investigations: Jennifer Siganto, Jodie Lomoff and Mark Burdon, 'The privacy commissioner and own-motion investigations into serious data breaches: a case of going through the motions?' *University of New South Wales Law Journal* (2015) 38 3: 1145-1185 <http://espace.library.uq.edu.au/view/UQ:367575> and the author's conclusions as to OAIC enforcement as to behavioural advertising: Mathews-Hunt, above n 185.

<sup>1530</sup> Pilgrim, above n 1225.

<sup>1531</sup> The first large scale breach case post the amendments involved *Singtel Optus Pty Ltd* which voluntarily notified three privacy breaches caused by their own systems' security flaws, each affecting over 100,000 customers: Michael Pattinson, 'First enforceable undertaking under new privacy laws' *Allens Linklaters* (31 Mar 2015 accessed 20 Apr 2015) <<http://www.allens.com.au/pubs/priv/fopriv31mar15.htm>> The APC did not pursue civil penalties and accepted a section 33E enforceable undertaking, partly due to its cooperation and the (expensive) systems, audit and related corporate reviews included as a part of the settlement: see the text here: <<http://www.oaic.gov.au/privacy/applying-privacy-law/enforceable-undertakings/singtel-optus-enforceable-undertaking>>. Consistent with growing US practice, it is surprising though that the APC did not act under APP 11 as to a failure to take reasonable steps to protect information – in one case, 122,000 customers had personal information published in the White Pages and online – without their consent. This is a serious breach with significant consumer harm to justify civil penalties. In contrast, the ACCC prosecuted Optus for advertising misrepresentations which resulted in \$3.61M in penalties. The Full Federal Court found that Optus was not a 'first offender' and had lax compliance systems: Gilbert & Tobin, 'Singtel Optus Pty Ltd v ACCC' (27 Apr 2012 accessed 20 Apr 2015) <<http://www.lexology.com/library/detail.aspx?g=46cac7c5-c732-4001-b553-98f620b75935>>

<sup>1532</sup> OAIC, 'Annual Report' 2015-6 <https://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201516/part-2-performance> Of these all were individual complaints which had failed at conciliation. None involved 'consumer' issues but rather were "low-tech" individual scenarios. As such they little advance the privacy cause and are more small claims in effect.

<sup>1533</sup> One included the infamous Ashley Madison data breach case which was investigated in conjunction with the Canadian Privacy Commissioner: Enforceable Undertaking Under s 33E of the Privacy Act 1988 (Cth), to the Australian Information Commissioner - Avid Life Media Inc. (ALM) (trading as Ruby Corp.), 21 Aug 2015.

<sup>1534</sup> These were across education, government, identity verification, retail, telecommunications.

of its enforcement activity for 2015-6.<sup>1535</sup> Put simply, the OAIC is small,<sup>1536</sup> poorly funded,<sup>1537</sup> has too much to do and unsurprisingly, has limited regulatory impact.

But the OAIC has G-PEN sweep evidence of existing Australian CIOT privacy problems, and has regulatory powers to influence CIOT pre- widespread consumer adoption: it could publicly educate and warn Australians of CIOT privacy concerns, issue best practice guidance or encourage stakeholders to register a privacy code,<sup>1538</sup> it could investigate a CIOT privacy policy as a test case or seek to prosecute data breach due to inadequate security compliance<sup>1539</sup> or undertake a self-initiated Part V enquiry.<sup>1540</sup> Further it could address its weak evidence-base for CIOT privacy policy-making as to the economic and technical dimensions of privacy, as well as approaches to preventative measures. The comprehends improving its capacity to understand and interpret complaints data, breach statistics, and how sanctions, fines etc. influence CIOT industry behaviour - all potentially rich insights for policy makers<sup>1541</sup> – and none of which publicly exist.<sup>1542</sup> Indeed, the OAIC is less engaged in research and less transparent in its disclosure practices than many of its peers, which may impede its capacity to monitor PA compliance and to detect consumer detriment.<sup>1543</sup> While these approaches might be ‘unusually’ pre-emptive in Australia, there is sufficient international concern<sup>1544</sup> to justify signalling that future success and consumer trust resides in up-front privacy-compliance.<sup>1545</sup>

---

<sup>1535</sup> It managed 19,000 privacy questions, 2,128 privacy complaints – of which only 120 were online, and 97% overall resolved, conducted 21 privacy practice assessments, and 123 data breach notifications in 2015-6: OAIC, ‘Performance’ (accessed 5 May 2017) <<https://www.oaic.gov.au/performance/#!year-2015-16-section-what-we-do-promote-uphold-and-shape-australian-information-privacy-rights>>

<sup>1536</sup> As at 2015-6, the OAIC has 75 staff, of whom 58 are full time.

<sup>1537</sup> In 2015-6 the legal budget was \$253,777.15 external (\$132,719.05 internal), and paid only \$253,777.15 for external legal services – and briefed external counsel only four times: OAIC, ‘Legal Services Expenditure Report 2015-6’ <<https://www.oaic.gov.au/about-us/corporate-information/legal-services/legal-services-expenditure-report-2015-16>> Unless there are significant internal legal resources, it is little wonder they so rarely pursue proceedings or even an amicus status.

<sup>1538</sup> PA Part IIIB.

<sup>1539</sup> Unless APP 11 is breached, the APC will not act on hacking if there is no “disclosure” as required under APP 6. That is no consolation to affected consumers, or incentive for the hacked organisation to institute better security – to “take such steps as are reasonable in the circumstances” [APP 11] to protect its data from unwanted intrusion. ‘Hacking’ or unauthorised data access is of course an issue for the police and criminal law enforcement - but again, this does not redress the individual privacy harm or enable the privacy regulator to take compliance- based action.

<sup>1540</sup> PA section 33C. See the reports here: <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/>

<sup>1541</sup> OECD, above n 505 :34.

<sup>1542</sup> The OECD criticises international regulators for poor data formats unsuited for international comparisons, which impedes analysis.

<sup>1543</sup> The OECD finds gaps across privacy regulators as to the economic and technical dimensions of privacy, and preventative measures. International privacy enforcement authorities gather and release public data, but Australia is not prominent. Improving its capacity to understand and interpret complaints data, statistics as to breach, and how sanctions, fines etc. influence CIOT industry behaviour would offer potentially rich insights for policy makers, justify budget increases and improve consumer information.

<sup>1544</sup> Above n 18.

<sup>1545</sup> Timothy Pilgrim ‘Defining the sensor society’ Presentation by the Privacy Commissioner, to the ‘Defining the Sensor Society Conference’ at University of Queensland, Brisbane (8 May 2014 accessed 30 May 2016 )

## 5.6 Conclusion: chapter five

*My priority is protecting Australian's personal information in the digital age... [and] to help businesses and the wider community take privacy in their hands.'* – Timothy Pilgrim<sup>1546</sup>

As evidenced, the APPs are too weak to meet CIOT challenges and based upon current OAIC strategy and government under-resourcing, are unlikely to exert a positive influence over the promotion of privacy into the future. Privacy law compliance offers potential long term benefits in any industry context,<sup>1547</sup> but given the significant consumer threats posed by the IOT, principles-based, self-fashioned laws with largely 'soft' enforcement will rarely initiate the momentum for substantial corporate investment in any area of legal compliance. In other words, unless it walks the talk, and talks a lot louder, then the OAIC will not be on the radar of many CIOT developers, to the detriment of Australian consumer privacy. Further, while compliance is a laudable long-term regulatory aim, 'soft' enforcement alone rarely initiates the momentum required for aggressive corporate investment in any area of legal compliance. Absent some significant court cases,<sup>1548</sup> financial penalties or evidenced consumer trust backlash, this chapter suggests that limited consent-based privacy administered by the OAIC is unlikely to be effective against the significant consumer IOT privacy challenges.<sup>1549</sup>

To resolve these potential 'gaps', certain recommendations and draft principles appear in **Part IV**. The next chapter considers the consumer contracting and notice and choice consent model in landscape; using various studies, cases and behavioural economics approaches, to expose the greatest legal gap of all - that CIOT consents, data collection and privacy are premised upon a consumer protection contracting fallacy.

---

<https://www.oaic.gov.au/media-and-speeches/speeches/defining-the-sensor-society>; More recently, the CIOT was referenced in a submission to the Canadian Commissioner:

<sup>1546</sup> Pilgrim, above n 1225.

<sup>1547</sup> Interestingly the 2015 IAPP survey found that increasing consumer trust is a "much higher priority" in Europe (48%) than in the US (30%) in terms of the top two reasons for having a privacy programme. In contrast, data protection was US (46%) and EU (38%): IAPP-EY, 'Annual Privacy Governance Report 2015' (2015 accessed 6 Apr 2016): 97 <[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00029-97820.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00029-97820.pdf)>

<sup>1548</sup> The APC's enforcement regime has improved if it were so inclined: it can conduct audits, make a determination (PA Part VI), accept court-enforceable written undertakings (PA ss 33E and 33F) and apply for civil penalty orders (PA Part VIB: penalties range from \$340,000 for individuals and up to \$1.7 million for companies.) The *Optus Case* exemplifies the enforcement policy where an infringing entity 'cooperates': the OAIC accepted an enforceable undertaking in lieu of the educative and publicity benefits of a court case and potential civil penalty. It signals that upon (voluntary) breach notification, organisations which cooperate and agree substantial compliance undertakings and auditing, will not necessarily face enforcement action. The approach may be resource-related but it ignores even egregious breach, which sends a weak message.

<sup>1549</sup> Mathews-Hunt, above n 151,185 and 841. The author's views are derived from personal experience as a corporate lawyer in terms of what motivates investment in compliance within large companies. Note also that consumer trust may be addressed advertising/ branding as well – so a resources choice might be made between investment in marketing versus compliance activities. The better approach is to do both.

Potential problem or “gap”	Consumer detriments (identified & potential)
Legislated reliance upon “informed” or “implied” consent to justify the collection, storage and use of PI or SPI	<ul style="list-style-type: none"> <li>- information asymmetry</li> <li>- behavioural economics suggests ...</li> <li>- impractical in a CIOT device context</li> <li>- market failure evidence (e.g. sweep 2016; evidence of unfair contract terms)</li> </ul>
Lack of mandated privacy-by-design and security-by-design and both by default	<ul style="list-style-type: none"> <li>- information asymmetry</li> <li>- expose consumers to substandard privacy and security protections and anti-privacy and/ or security default settings</li> <li>- requires tech expertise beyond ‘plug n play’ so disadvantages many consumers especially those who are young, elderly, disabled or intellectually disabled or disadvantaged</li> <li>- evidence of unsafe or defective product sales (e.g. 2016 sweep evidences informational defects)</li> <li>- evidence is numerous data breach incidents</li> <li>- market failure</li> </ul>
Limited mandated mandatory data breach reporting to consumers (2018) <sup>1550</sup>	<ul style="list-style-type: none"> <li>- information asymmetry</li> <li>- product and informational complexity prevents consumers making informed decisions as to their CIOT device security and privacy settings</li> <li>- clear evidence that most data breaches are unreported</li> <li>- market failure outcomes</li> </ul>
Lack of mandated requirements as to data protection and retention requirements	<ul style="list-style-type: none"> <li>- information asymmetry</li> <li>- obliges consumers to assess CIOT data flows and security which many lack the information, time or knowledge to do</li> <li>- clear evidence of data breach internationally and in Australia</li> <li>- evidence of unsafe or defective product sales</li> <li>- market failure outcomes</li> </ul>
Lack of ongoing privacy controls over upstream data handlers	<ul style="list-style-type: none"> <li>- information asymmetry</li> <li>- anonymization failures</li> <li>- privacy policies often fail to clearly specify where data goes, who uses it, for what (specific) purpose and for how long</li> <li>- consumers cannot control or monitor privacy compliance of data</li> <li>- collecting entities may not set in place ongoing controls</li> <li>- (undisclosed) commission payments upstream for data</li> <li>- market failure outcomes</li> </ul>
Lack of audits or research to check industry compliance	<ul style="list-style-type: none"> <li>- market failure: system fails to self-monitor</li> <li>- regulatory failure: OAIC fails to monitor comprehensively or to commission research (c/f Office of the Canadian Privacy Commissioner CPC)</li> <li>- evidence of unsafe or defective product sales</li> <li>- evidence of unfair terms in privacy statements and product terms and conditions</li> <li>- goods new to market so consumers purchase rates infrequent</li> </ul>

<sup>1550</sup> On 13 February 2017, the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) was enacted, to insert mandatory data breach notification requirements into the PA.

Weak or nil codes of practice which govern privacy-related concerns <sup>1551</sup>	<ul style="list-style-type: none"> <li>- market failure</li> <li>- e.g. Automotive manufacturer's global privacy undertakings are described by CPC research as "substandard" and non-compliant</li> </ul>
Lack of prosecutions to incentivize industry standards or set regulatory warnings to govern future industry practices and/ or guide possible codes of practice	<ul style="list-style-type: none"> <li>-? regulatory failure as to information asymmetry</li> <li>-? regulatory failure as to generating industry signals</li> <li>- Nil CIOT privacy-related prosecutions or court cases in Australia</li> <li>- Nil data as to CIOT privacy complaints available</li> <li>- evidence of data collection practices in breach of APPs</li> <li>- international complaints evidence</li> </ul>
Systemic weakness in weak prosecution and enforcement practices	<ul style="list-style-type: none"> <li>- political failure</li> <li>- regulatory failure</li> <li>- market failure</li> <li>- APC Guidelines not legally binding</li> <li>- inadequate consumer redress</li> </ul>
No general privacy tort to enable individual privacy right of action	<ul style="list-style-type: none"> <li>- regulatory failure where legal 'gaps' are not addressed<sup>1552</sup></li> <li>- inadequate consumer redress</li> </ul>

Table 5.1 Summary chapter 5

Source: author

<sup>1551</sup> The Australian IOT Alliance is working on a guideline as to privacy and data, due for release in 2017.

<sup>1552</sup> Four substantive public enquiries in 8 years have recommended that a privacy tort be enacted: Australian Law Reform Commission, above n 1480; NSW Law Reform Commission, 'Invasion of Privacy' Report No. 120 ( accessed 5 Jan 2016) < ; ALRC, above n 1235; Victorian law Reform Commission, above n 1473; and NSW Legislative Council Standing Committee of Law and Justice, 'Final report: remedies for the serious invasion of privacy in New South Wales' (3 Mar 2016 accessed 10 Mar 2016)

<<https://www.parliament.nsw.gov.au/committees/DBAssets/InquiryReport/ReportAcrobat/6043/Report%20no%2057%20Remedies%20for%20the%20serious%20invasion%20of%20.pdf>>

## Chapter 6 Contracting & imperfectly rational consumers @ CIOT

*Gaining consumer consent by mystifying them with long-winded legal statements and 20-page policy disclaimers is not a sustainable strategy...*<sup>1553</sup>

*“A “notice and choice” or consent-based approach to privacy protections simply does not work in the Internet of Things.”*<sup>1554</sup>

Digital contracting shapes the consumer IOT ecosystem<sup>1555</sup> - from device purchase, to app download, to data-collection, cloud and data analytics – in a ubiquitous but legally problematic process. Characterised by voluminous, non-negotiable, small print, standard form contracts, online contracting struggles with legal technicalities such as capacity, voluntariness and informed consent. At its best, it confers competition, convenience and efficiency; at its worst, it is a behaviourally-manipulative environment,<sup>1556</sup> where absent consumer agreement, choice narrows unworkably.<sup>1557</sup> Premised upon classical contract theory,<sup>1558</sup> such contracts require offer and acceptance, intention to create legal relations, consideration and capacity, subject to vitiating factors such as misrepresentation, unconscionability, mistake and undue influence.<sup>1559</sup> Devices (rarely) come with hard-copy terms, so consumers must seek out websites and app stores with links to terms and conditions, and expressly-incorporated, privacy, data and cookie (tracking) policies and pop-up boxes (**terms**). Consumer

---

<sup>1553</sup> KPMG, ‘Creepy or cool? Staying on the right side of the consumer privacy line’ (Nov 2016 accessed 9 Nov 2016): 26 <<https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2016/advisory/creepy-or-cool.pdf>>

<sup>1554</sup> EPIC, ‘Comments of the EPIC to the NTIA On the Benefits, Challenges and Potential Roles for the Government in Fostering the Advancement of the Internet of Things’ (2 June 2016 accessed 26 Jun 2016): 12 <<https://www.ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things>>

<sup>1555</sup> E-commerce is the sale of goods and/or services “ordered via the Internet or any other computer-mediated network... regardless of whether the payment and/or the ultimate delivery of the goods and/or services is conducted online or offline” (OECD). The ABS include: “all retail trade activity where the commitment to purchase is made online may be considered to be online retail trade activity...”: Australian Bureau of Statistics, ‘8501.0.55.007 - Information Paper: Measurement of Online Retail Trade in Macroeconomic Statistics, 2013’ (19/08/2013 accessed 17 July 2014) <<http://www.abs.gov.au/AUSSTATS/abs@.nsf/Latestproducts/8501.0.55.007>

Main%20Features12013?opendocument&tabname=Summary&prodno=8501.0.55.007&issue=2013&num=&view=>

<sup>1556</sup> While it may seem odd to assert that a private online consumer purchase or other transaction might be pressured, web marketers employ various tactics such as dark patterns, drip pricing and the like, which may manipulate consumers in a contracting context. The ACCC has finally persuaded Virgin and Jetstar Airlines to cease an opt-in by default for insurance, for online flight bookings. This is after they succeeded (largely) in an action based upon drip-pricing.

<sup>1557</sup> Facebook is perhaps the best example of this. Many workplaces, schools, groups, sporting clubs etc. maintain a page which consumers may have to join to receive news from their ‘social network’.

<sup>1558</sup> Jeannie Marie Paterson, ‘The Australian Unfair Contract Terms Law: The Rise of Substantive Unfairness as a Ground for Review of Standard Form Consumer Contracts’ [2009] *UMelbLRS* 20: 20 <<http://www.austlii.edu.au/au/journals/UMelbLRS/2009/20.html#fn37>>

<sup>1559</sup> These have both statutory and common law bases.

acceptance occurs through mandatory notice,<sup>1560</sup> ‘take it or leave it’,<sup>1561</sup> opt-in or opt-out,<sup>1562</sup> tick a box<sup>1563</sup> or most often, ‘deemed/ implied consent’ inferred from continued site, device or software use.<sup>1564</sup> As **Sched. 1** suggests, many CIOT contracts exhibit troubling features: including length and complexity, standard form non-negotiability; acceptance by use or affirmative consent, and low transparency. Consumers must ‘take or leave’ disadvantageous terms which impose “privacy-trading behaviours”,<sup>1565</sup> and reallocate risk, in an artificial environment. Several US decisions criticise that artificiality: in *Berkson*, Weinstein, J described the “wraps”<sup>1566</sup> as a “questionable [contracting] form”, and in *Meyer*, the court refused to uphold Uber’s (clickwrap) arbitration terms as a “legal fiction”:<sup>1567</sup>

... [online users] “supposedly agreeing to lengthy ‘terms and conditions’ that they had no realistic power to negotiate or contest and often were not even aware of”.<sup>1568</sup>

Obar argues that flawed ‘notice and choice’ regulatory regimes perpetuate a “self-governance fallacy”.<sup>1569</sup> Consumer informational asymmetry, unfair terms and power imbalance underscore serious consumer

---

<sup>1560</sup> This is the stipulated regime under the *Privacy Act 1988* (Cth) for personal information which is not ‘sensitive’ as defined.

<sup>1561</sup> See for example the Samsung Privacy Policy here, which advises that updates ‘may’ be notified to consumers; otherwise the burden to stay informed rests with the consumer to return to the policy page and check for changes: <http://www.samsung.com/au/info/privacy.html>. Note also that additional ‘new’ terms or even, policies may be announced as immediately effective, regardless of consumer awareness and consent is deemed from continued use - see for example, in response to the SmartTV furore here: Samsung, ‘Samsung Global Privacy Policy - SmartTV Supplement’ <<https://www.samsung.com/uk/info/privacy-SmartTV.html>>

<sup>1562</sup> Consider for example, the Jetstar terms used an opt-out for insurance: *Australian Competition and Consumer Commission v Jetstar Airways Pty Limited* (No 2) [2017] FCA 205

<sup>1563</sup> Directive 95/46/EC specifies that ‘Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including by ticking a box when visiting an Internet website’. <<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>> In Australia, the OAIC discourages “opt outs” as intention may be ambiguous where an individual fails to opt out: OAIC, Guidelines, above n 1306: [B.40] A pre-checked box is not effective consent under the *Spam Act* according to the regulator, ACMA: Justin Cudmore and James True, ‘Before you hit send: Complying with the Spam Act – the unsubscribe and identification requirements’ *Marque Lawyers* (9 November 2014 accessed 25 Mar 2015) <[http://www.marquelawyers.com.au/assets/marque-update\\_before-you-hit-send-complying-with-the-spam-act-has-the-recipient-consented-161014.pdf?utm\\_source=Mondaq&utm\\_medium=syndication&utm\\_campaign=inter-article-link](http://www.marquelawyers.com.au/assets/marque-update_before-you-hit-send-complying-with-the-spam-act-has-the-recipient-consented-161014.pdf?utm_source=Mondaq&utm_medium=syndication&utm_campaign=inter-article-link)>

<sup>1564</sup> Nest, ‘Terms of Service’ (UK) (updated 10 Mar 2016 accessed 2 Apr 2016) <<https://nest.com/uk/legal/terms-of-service/>> Clause 1(a) provides: “(a) Overview and Relation to Other Agreements. These Terms govern your use of the Services... All additional guidelines, terms or rules and the Website Privacy Policy ... and the Privacy Statement ... are incorporated by reference into these Terms and you are agreeing to accept and abide by them by using the Services.”

<sup>1565</sup> Bailey, above n 51.

<sup>1566</sup> On websites, these are ‘browsewrap’ and ‘clickwrap’: the former creates contracts purportedly formed through inferred consent via continued website or device use, and the latter, creates contracts through a positive assent - such as clicking “I agree”. In the US and EU, browsewrap contracts are generally not enforceable against a consumer: *Fyeta v Facebook Inc* 841 F Supp 2d 829, 836 (SDNY 2012); whereas ‘clickwrap’ contracts usually are. Rackoff, J also mentioned ‘scrollwrap’ (where consumers must scroll through Terms and click assent beneath) which is a variant of clickwrap, but ended up proposing ‘sign in wrap’, to cover cases where consumers sign into a website or mobile application

<sup>1567</sup> Rackoff, J cited in Paul, Weiss, Rifkind, Wharton & Garrison LLP, ‘Southern District of New York Decision Suggests Increasing Scrutiny of Electronic Agreements’ Client Memorandum (8 Aug 2016 accessed 2 Sept 2016) <<https://www.paulweiss.com/media/3662711/8aug16uber.pdf>>

<sup>1568</sup> *Meyer v Kalanick*, No 15 Civ 9796, 2016 WL 4073012 (SDNY July 29, 2016)

<sup>1569</sup> Jonathan Obar, ‘Big Data and the Phantom Public: Walter Lippman and the fallacy of data privacy self-management’ *Big Data and Society* (July-Dec 2015 accessed 5 Jul 2016) 1-15 <[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00076-98127.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00076-98127.pdf)>

detriment, legitimise commercialised data collection and use, through a virtual appropriation of consumer identity.

This chapter identifies a regulatory failure. Unfair terms regimes have been in force in Australia since 2010 and in Europe longer – yet many CIOT-product providers are not responding to the law – until caught.<sup>1570</sup> While the GDPR may effect broader change, international companies are incentivized to tailor their contracts to the lowest bar in each jurisdiction. If past is precedent, consumers cannot trust CIOT industry members to voluntarily regulate their own contracting behaviour even under the shadow of the law, and neither should regulators.

## 6.1 CIOT contracting ABCs...

*“Manufacturers...sensibly disclaim warranties, limit liabilities, and curb disputes in their standard terms. But courts will flout such measures... unless valid contracts were formed.”<sup>1571</sup>*

*Anyone who has ever installed software after “consenting” to the terms... understands that the disgruntled user has exactly two choices when it comes to mass market license agreements: take it or leave it.<sup>1572</sup>*

Online contracts are legally enforceable in Australia<sup>1573</sup> and internationally.<sup>1574</sup> Even if a consumer does not read the contract but clicks ‘agree’,<sup>1575</sup> – they are usually bound – provided the terms are physically obvious, reasonable steps are taken to attract attention to them pre-contract formulation, and there is no ‘alert’ as to incapacity or vitiating factors.<sup>1576</sup> It is however important to distinguish between contractual

---

<sup>1570</sup> Recent examples include the airlines, which despite consumer angst (evidenced by petitions and the like), failed to redress online drip-pricing and other contracting practices of concern, until the NZ Commerce Dept. and the ACCC took formal action.

<sup>1571</sup> Barbara Melby & A. Benjamin Klaber, ‘Contract Corner: Standard Terms in the IoT Age’ *Morgan Lewis & Brockius LLP* (13 Apr 2017 accessed 14 Apr 2017) <<http://www.lexology.com/library/detail.aspx?g=69f405ae-ead6-442c-a961-bb266bac135b>>

<sup>1572</sup> Jane Chong, ‘We Need Strict Laws If We Want More Secure Software’ (31 Oct 2013 accessed 2 Feb 2016) <<https://newrepublic.com/article/115402/sad-state-software-liability-law-bad-code-part-4>>

<sup>1573</sup> The *Electronic Transactions Act 1999* (Cth) led to uniform state legislation including the *Electronic Transactions Act 2001* (ACT), *Electronic Transactions Act 2000* (NSW), *Electronic Transactions (Victoria) Act 2000* (Vic), *Transactions (Queensland) Act 2001* (Qld), *Electronic Transactions Act 2000* (SA), *Electronic Transactions Act 2003* (WA), *Electronic Transactions Act 2000* (Tas), and *Electronic Transactions (Northern Territory) Act 2000* (NT).

<sup>1574</sup> Forder above n 148: 34- 35. Note the UN Commission on Electronic Trade Law (UNICTRAL) *Model Law on Electronic Commerce*. On 1 July 2016 the EU eIDAS regulation commenced in all EU member states. Aimed to promote user confidence, trust and convenience in digital transactions, the regulation introduces an EU Trust Mark system for qualified trust services and is designed to promote cross border e-commerce, including e-signatures: Digital Single Market, ‘Trust Services and EID’ <<https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>>

<sup>1575</sup> See Forder, above n 148: chapter 4.

<sup>1576</sup> These include ACL unfair terms, unconscionability, misleading or deceptive conduct or false representations, which may vitiate agreement.

and privacy ‘consents’ online – which conceptually blend nuances of technical<sup>1577</sup> and true<sup>1578</sup> consent. The former is satisfied by accepting the policy (use or the ‘click’) whereas the latter, presupposes “informed, free intention”<sup>1579</sup> to accept something read and understood. While the PA does not refine this, OAIC Guidance does: PA consent requirements are limited,<sup>1580</sup> may be ‘express’<sup>1581</sup> or ‘implied’ by reasonable inference,<sup>1582</sup> and require four elements: <sup>1583</sup> adequate advance information,<sup>1584</sup> then consent must be voluntary,<sup>1585</sup> current and specific,<sup>1586</sup> by a person with capacity,<sup>1587</sup> who communicates their consent.<sup>1588</sup> Some academics call this consent duality a “vexed question, with no clear academic or legal consensus”.<sup>1589</sup> Practically, privacy consents are based upon disclosure; that is, provided suppliers disclose information uses and consumers assent or impliedly do so, then the courts will (absent vitiating factors) not interfere. Any alternative view opens millions of online contracts to review based upon participant’s understandings - which is obviously impracticable. It is not however, impossible that a court may find the contract or the express incorporation term flawed such that the privacy policy loses its contractual gloss,<sup>1590</sup> or that a policy communicated after an individual has purchased a device or

---

<sup>1577</sup> ‘Technical’ consent means that the consumers adopt the mechanism required by the supplier to agree to the actions contained within the privacy policy. While that is identifiable in a “clickwrap” situation, it is less clear if ‘continued use of a site or product is ‘consent’. See the discussion in Briedis et al, above n 1367: 42- 43.

<sup>1578</sup> Briedis, above n 1367: 42

<sup>1579</sup> Briedis, above n 1367: 42.

<sup>1580</sup> ‘Consent’ is only relevant in APP3 (collection of SI), use and disclosure (APP 6) direct marketing and cross-border disclosure (APP 8). It provides an exception to a general prohibition against PI being handled in a prohibited manner (e.g. APPs 3.3(a); 6.1(a)), or confers authority to handle PI in a specific manner, in APPs 7.3, 7.4 and 8.2(b): OAIC Guidelines, above n 1306 [B.34]

<sup>1581</sup> Non-legally binding OAIC Guidelines indicate that consent is to be ‘given explicitly, either orally or in writing’. Examples in an online context might include clicking ‘agree’: OAIC, ‘Australian Privacy Principles Guidelines’ (1 April 2015 accessed 5 April 2015) [9 para B. 36] <[http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP\\_guidelines\\_complete\\_version\\_1\\_April\\_2015.pdf](http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP_guidelines_complete_version_1_April_2015.pdf)>

<sup>1582</sup> Section 6(1) contains this definition. Re implied consent, see *Ibid* [para B.37].

<sup>1583</sup> OAIC, above n 1306.

<sup>1584</sup> The Guidelines state that this means clearly and properly informed in plain English and without jargon; and also includes an understanding as to the implications of withholding consent - such as that access to a website may be denied: OAIC, above n 1306: 11 para B.47.

<sup>1585</sup> The OAIC Guidelines say ‘Voluntariness’ is met if the individual has a ‘genuine opportunity’ to provide or withhold consent and excludes duress, coercion or pressure such as to overpower the individual’s will: OAIC, above n 1306: 10, para B 43. Relevant factors include any alternatives open to the individual if they choose not to consent, the seriousness of any consequences if an individual refuses to consent, and any adverse consequences for family members or associates of the individual if the individual refuses to consent.

<sup>1586</sup> The OAIC Guidelines provide that this should be sought upon collection or at the time of use/ disclosure, does not last indefinitely, should be no broader than required for uses and may be withdrawn at any time: OAIC, above n 1306: 11 para B.48 – 51.

<sup>1587</sup> The OAIC Guidelines provide that capacity means that the individual is capable of understanding the consent decision and may be presumed to have capacity unless there is anything to alert the recipient otherwise. Note however that the Guidelines make no mention of capacity online; yet it is clearly a circumstance where persons without the requisite capacity could attempt to provide consent and the recipient is unlikely to be alerted otherwise: OAIC, above 1306: 11 [para B. 52 – 55].

<sup>1588</sup> Above n 1306: at <[https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#\\_Toc380575605](https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#_Toc380575605)

<sup>1589</sup> *Ibid*: 49.

<sup>1590</sup> In *Rana v Australian Human Rights Commission* [2014] FCA 1902, email communications between the parties were held not to form a part of the contract as there was no intent to enter contractual relations; with the result that the ACL unfair

software online is not contractual.<sup>1591</sup> Further, an otherwise valid contract incorporation term may be ineffective if incorporated documents are unavailable or illegible, or where Terms are ‘unfair’ and severed under the ACL (Ch. 4).<sup>1592</sup> A recent US case rigorously reviewed Uber’s online contract process against requirements for reasonably conspicuous notice and unambiguous consent,<sup>1593</sup> and found against enforceability, citing six factors, mostly as to notice and accessibility.<sup>1594</sup> Further the judge observed:

*“electronic agreements fall along a spectrum ... and it is difficult to draw bright-line rules because each user interface differs from others in distinctive ways”.*<sup>1595</sup>

It may be difficult, but bright line rules are clearly required to reset online contracting methodologies and approaches. While the spectrum of online agreements ranges from good to bad, the bad CIOT contract may be uniquely so, in terms of consumer privacy, security, liability and enablement of S/PI data collection, use and commercialisation. It is important to understand why consumers accept such contracts, and why there is prima facie ‘unfairness’ to consumers – such that online contracting as a concept, requires regulatory realignment.

## 6.2 Reading, reading, reading ... the contract

*Privacy Statements are not disclaimers...*<sup>1596</sup>

*Just putting a sticker on it saying ‘customer is responsible’ is a nightmare...*<sup>1597</sup>

---

contract terms did not apply. See also *Rowe v Emmanuel College* [2013] FCCA 231 where a consumer had not ‘accepted’ a ‘separated parent policy’ and so was not able to argue that it contained unfair terms.

<sup>1591</sup> *Ebay International AG v Creative Festival Entertainment Pty Ltd* (2006) 170 FCR 450

<sup>1592</sup> Gordon Hughes, above n 1121: 38- 40; Hughes, Gordon and Lisa Di Marco, ‘Online privacy policies – it’s not just about the Privacy Act’ *Internet Law Bulletin* (April 2015 accessed 2 May 2015) 38- 40; Gordon Hughes and Andrew Sutherland, ‘Enforcement problems with online contacts: an Uber case study’ *Davies Collison Cave* (5 Oct 2016 accessed 10 Oct 2016) <[http://www.lexology.com/library/detail.aspx?g=9eacde91-e023-4334-a1e3-381492e3a212&utm\\_source=Lexology+Daily+Newsfeed&utm\\_medium=HTML+email+-+Body+-+General+section&utm\\_campaign=Lexology+subscriber+daily+feed&utm\\_content=Lexology+Daily+Newsfeed+2016-10-10&utm\\_term=>](http://www.lexology.com/library/detail.aspx?g=9eacde91-e023-4334-a1e3-381492e3a212&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2016-10-10&utm_term=>)>

<sup>1593</sup> The test is derived from *Specht v Netscape Communications Corp.*, 306 F 3d 17 (ed. Cir 2002)

<sup>1594</sup> These were: absence of a check box meant there was no required ‘manifestation’; the user did not have to review any terms before registering; references to the terms and consent were smaller and less conspicuous; “Terms of Use” might imply what services were being provided as opposed to contractual terms relevant to the user; the hyperlink did not go directly to the TOS, and even if the user did access the TOS, the arbitration clause was located three pages into the agreement; Paul, Weiss, Rifkind, Wharton & Garrison LLP, ‘Southern District of New York Decision Suggests Increasing Scrutiny of Electronic Agreements’ *Client Memorandum* (8 Aug 2016 accessed 2 Sept 2016) <<https://www.paulweiss.com/media/3662711/8aug16uber.pdf>>

<sup>1595</sup> See also the ongoing battle in *McLellan et al., v Fitbit, Inc.* (2016) where the plaintiffs allege (inter alia) that Fitbit sell their device and then “unconscionably” exclude court action “through an unconscionable post purchase agreement, which class members were required to accept in order to render their purchase “operational.” See also *In re Ashley Madison Customer data security breach*, Case No 4”15-md-02669 filed 9 Dec 2015.

<sup>1596</sup> Lawson, above n 36.

<sup>1597</sup> Solon, above n 1146 citing Ferdinand Dudenhöffer, auto industry analyst.

Consumers do not read online Terms,<sup>1598</sup> and do not understand them when they do. IDG report that 93% do not read website terms and conditions,<sup>1599</sup> while the OAIC found 56% of Australians do not read website privacy policies.<sup>1600</sup> That 88% of gamers granted Gamestation granted an “eternal option” on their “immortal soul” (rather than opting out for a £5 reward)<sup>1601</sup> comically illustrates an unfunny point<sup>1602</sup> for consumer and privacy regulatory models built upon consumer education/ protection, and disclosure/consent<sup>1603</sup> respectively. Even less funny is that regulators and legislators consistently defend these models,<sup>1604</sup> when research and evidence-based approaches inform them otherwise.

Studies suggest that Terms do not support rational consumer decision-making,<sup>1605</sup> and many are legally “unfair” and unconscionable.<sup>1606</sup> Factors such as length, accessibility/ visibility, complexity, legalese or technicality, positive framing and comprehension impugn consumer online contracting, but consumer law is only gradually responding. The ACL requires an openly evaluative<sup>1607</sup> judicial approach:

The legislative concept of “unfairness” in s 24, with elaboration through the three elements of unfairness, might be described as a guided form of open-ended legislation.<sup>1608</sup>

---

<sup>1598</sup> CAANZ, above n 95.

<sup>1599</sup> Dan Swinhoe, ‘Infoshot: Happy Reading with Terms and Conditions’, IDG Connect (3 Jul 2014 accessed 28 Jul 2014) <<http://www.idgconnect.com/abstract/8491/infoshot-happy-reading-with-terms-conditions>>.

<sup>1600</sup> Consumer Affairs Victoria found a quarter of consumers fail to read contracts, and 21% give only “ cursory consideration”: OAIC, above n 458: 39[2].

<sup>1601</sup> Consumers received a £5 GB coupon for noticing the link. The clause continued: “we reserve the right to serve such notice in 6 (six) foot high letters of fire, however we can accept no liability for any loss or damage caused by such an act. If you a) do not believe you have an immortal soul, b) have already given it to another party, or c) do not wish to grant Us such a license, please click the link below to nullify this sub-clause and proceed with your transaction.”

<sup>1602</sup> Mathews-Hunt, above n 152. In one day, 7,500 consumers granted Gamestation an eternal option to claim their “immortal soul” without liability for loss or damage thereby caused and upon notice served “in 6 (six) foot high letters of fire.” Only 12% of consumers selected “click here to nullify your soul transfer”; the rest (presumably) did not read the terms and conditions.

<sup>1603</sup> As identified in chapter 5, consent is not an APP nor is it required under the Privacy Act: it is only relevant to APP3 (collection of sensitive information), APP 6 (use or disclosure of PI other than for the primary purpose) and APP7 (direct marketing disclosures) and APP 8 (overseas disclosure without retaining APP compliance).

<sup>1604</sup> Obar, above n 1569: 7. Former FTC Chair Ramirez was a staunch CIOT consumer advocate, but still asserted that notice and choice is an appropriate model: Ramirez, above n 446. c/f Stacy A Elvy, ‘Contracting In The Age Of the Internet of Things: Article 2 Of the UCC and Beyond’ [2016] *Hofstra Law Review* 44: 839.

<sup>1605</sup> A. M. McDonald and L.F. Cranor, ‘The Cost of Reading Privacy Policies’, *I/S: A Journal of Law and Policy for the Information Society* (2008) <<http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>>

<sup>1606</sup> Consumer Affairs Victoria, ‘Unfair Contract terms in Victoria: Research into their extent, Nature, Cost and Implications’ *Research Paper No. 12* (October 2007 accessed 5 Aug 2014) [15] <http://www.consumer.vic.gov.au/resources-and-education/research> See the longer discussion in Mathews Hunt, above 152.

<sup>1607</sup> *Paciocco v Australia and New Zealand Banking Group Limited* [2015] FCAFC 50 [363] – [364], Allsop CJ (Besanko and Middleton JJ agreeing)

<sup>1608</sup> *Australian Competition and Consumer Commission v Chrisco Hampers Australia Limited* [2015] FCA 1204 (10 November 2015) <<http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/cth/FCA/2015/1204.html?stem=0&synonyms=0&query=Chrisco>> per Edelman, J at [40].

The ACL does not define fairness, nor transparency within fairness; rather, the court must consider its 'extent',<sup>1609</sup> defined (relevantly) as “reasonably plain language” and possibly, “presented clearly”.<sup>1610</sup> The Explanatory Memorandum states:

...if a term is not transparent it does not mean that it is unfair and if a term is transparent it does not mean that it is not unfair...<sup>1611</sup>

Privacy law is equally unresponsive. APP1.3 refers only to “clear” expression, and although the (non-binding) Guidelines<sup>1612</sup> go further, there is no binding authority using either prism. This discussion therefore justifies its conclusions based upon studies, **Sched. 1** analysis, and examples, in considering common CIOT features which may cause consumer detriment:

**Length:** CIOT contract length is increasing.<sup>1613</sup> Samsung's *SmartHome*<sup>1614</sup> and Fitbit<sup>1615</sup> contracts each exceed 7000 words and take 29.5 minutes to read.<sup>1616</sup> Linked terms increase disclosure but exacerbate length: Garmin<sup>1617</sup> has terms exceeding 10,000 words<sup>1618</sup> across five(+) documents and under one clause, third party links tally to around 32,000 words<sup>1619</sup>

---

<sup>1609</sup> That consideration is only in relation to the impugned term, and only as to ss 24(1)(a) -(c) matters: Ibid: [43].

<sup>1610</sup> ACL s. 24(2)(a). 'Transparency' is defined in s 24(3) to mean expressed in reasonably plain language, legible, presented clearly, and accessible.

<sup>1611</sup> Commonwealth of Australia, House of Representatives, Explanatory Memorandum, Trade Practices Amendment (Australian Consumer Law) Bill (No 2) 2010 (Cth) [5.39] <http://www.austlii.edu.au/au/legis/cth/bill/tpaclb22010505/>> Note the Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ 1993, L 095/29 (EU Directive) Art 5. requires contract terms to be drafted in “plain, intelligible language” without further definition, though a contra proferentem interpretation rule applies. In *Kásler and Káslerné Rábai/OTP Jelzálogbank Zrt*, CJEU 30 April 2014, case C-26/13, ECLI:EU:C:2014:282 points 73–74, the CJEU clarified that where a term is non-transparent, a national court needs to consider this when it assesses 'unfairness'; that is whether non- transparency is contrary to good faith and creates a significant imbalance between the parties' rights and obligations to the detriment of the consumer. See Marco Loos and Joasia Luzak, 'Wanted: a Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers' *Journal of Consumer Policy*, (March 2016) 39(1): 63–90 <<http://link.springer.com/article/10.1007/s10603-015-9303-7#Sec7>>

<sup>1612</sup> OAIC Guidelines stipulate that privacy policies should be honest, accurate, specific, easy to understand, prominently positioned, accessible (etc.)

<sup>1613</sup> In 2008, the average privacy policy was 2,518 words: McDonald, above 1605, whereas a recent Australian study of 16 policies, found an average of 3232 words: Briedis, above n 1367. Note however the contract lengths in Sched. 1 which are similar to Apple iTunes at 19,972 words long – longer than Macbeth (18,000 words): Swinhoe, above n 1599.

<sup>1614</sup> 7,391 words

<sup>1615</sup> 7,397, words

<sup>1616</sup> The method uses the standard reading rate for academic literature of 250 words per minute: McDonald, above n 1605.

<sup>1617</sup> The author purchased an attractive Garmin Vivomove smart self device for personal use, and hence this is the example chosen. It does not suggest (as Sched. 1 confirms) that Garmin is better or worse than other suppliers. Their website is clear in many respects; their terms are likewise – but (in my opinion) negative features which illustrate the criteria still exist.

<sup>1618</sup> Garmin Australia for example, has website terms (3050 words) an app privacy statement (3,911 words), Garmin Connect/ device privacy statement (4747 words), a Connect mobile phone permissions explanation document (614 words), and a security policy (393 words) - with multiple links throughout each.

<sup>1619</sup> These links are to Google, Microsoft (Azure apps insights), and Splunk which tally to 555 words, 2564 (short form) to 23126 long form and 2280 respectively. Note other providers were linked also, until Google purchased them. See the Australian terms <<http://www.garmin.com/en-AU/legal/privacy-statement>> which link to the smart phone app 'Connect' terms here <<https://connect.garmin.com/en-US/privacy>>

- which Garmin recommends “you carefully review”.<sup>1620</sup> Consumer groups<sup>1621</sup> decry such length as “absurd”; CHOICE recently publicly proved that by reading Amazon’s terms out loud – for almost nine hours.<sup>1622</sup>

One recommended solution - layered contract simplification<sup>1623</sup>- is inherently exploitable.<sup>1624</sup> Short form policies inevitably omit or misrepresent detail and may mislead or deter consumers from reading further. Microsoft clearly omits much of its 23,126-word policy in its 2,564-word condensed version; and Nestle’s smart self device short-form<sup>1625</sup> assurance that ‘no children’s data is retained’ is overtaken by devilish detail in its long-form policy, where children’s data *provided by parents* may be retained.<sup>1626</sup> It is a ‘half’-inconsistency hinging upon data “from” versus “about”; a distinction which few who read on, would detect.

---

<sup>1620</sup> See ‘Links, Third Party Apps, and Third Parties’ Privacy Practices’ here: <<http://www.garmin.com/en-AU/legal/privacy-statement>>

<sup>1621</sup> For example, the Norwegian Consumer Council spent 32 hours reading an average app users terms and conditions, based upon the average of 33 apps per smartphone: FORBRUKERRÅDET, ‘#Appfail’ (Nov 2016 accessed 2 Dec 2016) <<https://www.forbrukerradet.no/undersokelse/2015/appfail-threats-to-consumers-in-mobile-apps/>>

<sup>1622</sup> CHOICE, ‘Nine hours of ‘conditions apply’ *Media Release* (15 Mar 2017 accessed 15 Mar 2017) <<https://www.choice.com.au/about-us/media-releases/2017/march/nine-hours-of-conditions-apply>>

<sup>1623</sup> OAIC recommend this approach: OAIC, APP Guidelines, above n 1306: 5 [1.12]. Sensis recently agreed to summarize ‘key terms’ on each product page”: ACCC, ‘Undertaking to the ACCC given for the purposes of section 87B by Sensis Pty Ltd, (11 May 2017 accessed 11 May 2017); Centre for Information Policy Leadership, ‘Ten steps to develop a multilayered privacy notice’, Centre for Information Policy Leadership website <[www.informationpolicycentre.com](http://www.informationpolicycentre.com)>.

<sup>1624</sup> The OAIC recommends condensed privacy policies in its guide, OAIC, ‘Guide to developing an APP privacy policy’ (May 2014) <<https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-developing-an-app-privacy-policy>>; See Helen Nissenbaum, ‘A contextual approach to privacy online’ (2011 accessed 2 Jan 2016) 140 *Daedulus, Journal of the American Academy of Arts and Sciences*, 32- 48; and D. Solove, ‘Privacy Self-Management and the Consents Dilemma’ (2013 accessed 2 Jan 2016) 126 *Harv. Law Rev.* 1880. Nissenbaum refers to a loss of meaning.

<sup>1625</sup> The FAQs state: “How will you protect the personal information of me and my child? Our Privacy Policy sets out how Nestlé collects, stores and uses your personal information and how you can access and update your personal information or make a complaint. You can access the full Privacy Policy here.” As to app-collected data, the short-form states: “...Nestlé does not knowingly collect personal information from children under 15, even with parental consent”: Nestlé Australia, ‘Condensed Privacy Policy’ (updated Sept 2015 accessed 10 Jun 2016) <<http://www.nestle.com.au/info/privacypolicy>>

<sup>1626</sup> After 860 words, the full policy states: “Children under 15 – Nestlé does not knowingly collect personal information **from** children below the age of fifteen. If we discover that we have accidentally collected information from a child, we will remove that child’s information from our records as soon as feasibly possible. However, we may collect personal information **about** children below the age of 15 from the parent or custodian directly.” [author emphasis]: Nestlé Australia, Privacy Policy’ (updated Sept 2015 accessed 10 Jun 2016) <<http://www.nestle.com.au/info/full-privacy-policy>>



Graphic 6.1 Milo Champions™ webpage<sup>1627</sup>  
 Source: ©Nestlé Australia Pty Limited

Length is thus inherently consumer-unfriendly, imposes cognitive overload and reduces provider accountability. Recent UK authority suggests it may render a contract unfair,<sup>1628</sup> while US authority refused to enforce a significant term buried three pages into fine print.<sup>1629</sup> There is no Australian case in which length has justified finding an ‘unfair’ term, though appearance/ location have been referenced.<sup>1630</sup>

**Accessibility/ visibility** relates to accessing the contract, and to locating contractual terms and perhaps, *important* terms within the overall. As product packaging and device screens (if any) shrink, consumers must find multiple documents online, often requiring multiple clicks, cross-referencing, broken links, dense text and uncertain product application. On mobile phones, terms may be physically unreadable. Garmin’s site for example has multiple webpages comprising and linked to its terms, and poorly differentiates which apply to certain products and/ or in Australia.<sup>1631</sup> For the vulnerable or time poor, these are genuine barriers.<sup>1632</sup>

**Complexity** is common and adversely impacts both consumption and comprehension. Length, layout, layering or multiple terms across multiple links creates confusion. Australian consumers complain that online terms cannot be understood (43%), are “boring” and 58% would rather read

<sup>1627</sup> Nestlé, Milo Champions™ (accessed 12 Mar 2017) <<https://shop.milo.com.au/>> © MILO Nestlé

<sup>1628</sup> *Spreadex v Cochrane* [2012] EWHC 1290

<sup>1629</sup> *Meyer v Kalanick*, No 15 Civ 9796, 2016 WL 4073012 (SDNY July 29, 2016)

<sup>1630</sup> *ACCC v Chrisco Hampers Australia Ltd* [2015] FCA 1204, per Edelman, J.

<sup>1631</sup> For example, while the app linked directly to Australian terms, the privacy policy went to a broken link. The website contained numerous policies and it was genuinely confusing to identify which applied to my product and which did not. There were distributor terms which applied as well as the manufacturer’s which was slightly confusing. Overall, the site was clearer than most and the terms were long but reasonably transparent (once located).

<sup>1632</sup> The impacts on vulnerable people are important consumer law considerations, especially as to detriment.

their utility bill.<sup>1633</sup> But simple language linked to definitions has its pitfalls too: Samsung's data sharing practices seem clear until simple terms like "affiliates" and "third parties" hyperlink to such expansive definitions, that they can share and aggregate consumer data with (almost) anyone they like. As such, complexity requires a multi-dimensional evaluation: all the factors discussed in this section may create contractual complexity which considered as a whole,<sup>1634</sup> may lack 'transparency'.<sup>1635</sup>

**Legalese and technicality:** legally robust clauses drafted for legal ends to withstand legal contest, are ill-placed in consumer communications.<sup>1636</sup> Plain English is possible,<sup>1637</sup> but as **Sched. 1** implies, not practised. For example, consumers may not understand a legalistic 'choice of law' provision or its practical implications should they wish to sue, or that indemnities, waivers and exclusion clauses may impose risk. Consumers may not understand legal context either: the prefacing phrase: "To the extent permitted by law" is common, but rarely overcomes the prevailing impression that a following disclaimer overrides consumer guarantee rights.<sup>1638</sup> Similarly, technicality<sup>1639</sup> creates information asymmetries where complicated concepts or terms of art are used to enable unexpected data use or conceal consumer risk.<sup>1640</sup>

**Positive framing (bias):** euphemistic language exploits positive over unattractive attributes, and is found in each contract considered. These wordings may omit material aspects or imply half-truth impressions whether by language, technicality or legalese, or fail to fairly, instil balance or clarity. For example, Samsung introduce broad variation rights including to unilaterally limit features, restrict user access or to 'brick' devices, with this line:

"We're always trying to improve the Services, so they may change over time..."<sup>1641</sup>

---

<sup>1633</sup> OAIC, above n 458: 40. The figures as to privacy policies were too long (52%), too complicated (20%) and too boring (9%).

<sup>1634</sup> ACL section 24(2)(b).

<sup>1635</sup> ACL section 24(2)(a).

<sup>1636</sup> As the ACCAN study found, the contracts they reviewed "tended to be overly comprehensive regarding descriptive elements that are unlikely to be of interest to a consumer, and too obscure on these points that are likely to be of interest...": ACCAN, above n 1367: 25.

<sup>1637</sup> A lawyer rewrote Instagrams 5000 plus word Terms into one page, using plain English which young people found much easier to understand: Amy Wang, 'Teens finally understand rights after lawyer translates Instagram terms into plain English' *The Sydney Morning Herald* (9 Jan 2017 accessed 7 Feb 2017) <<http://www.smh.com.au/technology/web-culture/teens-finally-understand-rights-after-lawyer-translates-instagram-terms-into-plain-english-20170108-gtny6d.html>>

<sup>1638</sup> Another common (US) example is: 'SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU...' The obvious point is that this confuses consumers. See Sched. 1 for examples.

<sup>1639</sup> Obar, above n 1569; Nissenbaum, above n 1624; Solove, above n 1624.

<sup>1640</sup> An analogous situation might be Medical Information Sheets, which must explain contraindications even where the risk is small.

<sup>1641</sup> Samsung, 'Smart Things Terms of Use' (n.d. accessed 9 Apr 2016)

<<http://www.securingtomorrow.com/blog/knowledge/3-key-security-challenges-internet-things/>>

Fitbit's long but clear Terms include:

Use of the Fitbit Service should not replace your good judgment and common sense.  
Please read and comply with all safety notices that accompany your Fitbit product...<sup>1642</sup>

While sensible in language and tone, the associated (non-mandatory) hyperlink leads to (important) instructional warnings as to product-related dermatitis and pacemaker interference.<sup>1643</sup> It is perhaps a fine line between positive and misleading, but most CIOT Terms read more as marketing spiels peppered with legalese (or vice versa), than as balanced consumer communications.

**Comprehension:** a 2015 study found that 46% of Australians were not sufficiently prose literate to confidently read a newspaper or to understand medicine packet instructions.<sup>1644</sup> In other words, written consent is a poor means to communicate information to half the population, especially for vulnerable groups such as children.<sup>1645</sup> A 2016 UK study confirmed this: finding that “impenetrable and largely ignored” terms require “postgraduate reading level”,<sup>1646</sup> which means that consumers are contracting personal information away, unknowingly.<sup>1647</sup> Undoubtedly, many terms require comprehension levels which exceed those of the average consumer, such that upon expert evidence, a court might consider them ‘unfair’.

Clearly, these issues point to potentially systemic informational asymmetry. It seems obvious to assert that legally-binding “regulation or guidelines should be established for how terms, conditions and privacy statements are written and presented.”<sup>1648</sup>

---

<sup>1642</sup> Fitbit, ‘Terms of Service’ (last updated 2015) <<https://www.fitbit.com/au/legal/terms-of-service>>

<sup>1643</sup> Fitbit, ‘Wear and Tear’ <<https://www.fitbit.com/au/productcare>>

<sup>1644</sup> Lisa McWhirter and Lisa Eckstein, ‘Australian Consent Study’ (2015 accessed 20 Mar 2016) <http://www.utas.edu.au/law-and-genetics/research-and-projects/australian-consent-project> The study included persons aged 15 and over.

<sup>1645</sup> Ibid. These groups include intellectually or cognitively -impaired people, those with a mental illness, as well as children, non-English speakers and Aboriginal and Torres Strait Islanders.

<sup>1646</sup> UK Office of the Children’s Commissioner, ‘Growing up digital: a report of the growing up digital taskforce’, (Jan 2017 accessed 2 Mar 2017) <<http://apo.org.au/node/72332>>

<sup>1647</sup> Ibid. The study reviewed Instagram’s 5000 word, 17-page policy which was accepted by 56% of 13- 15-year-old children in the UK. The Report calls for a US-style children’s legislation to control data use of children, citing that the uncertainty of Brexit means that the continuation of GDPR protection as to children’s information is “not guaranteed”: Ibid: 12.

<sup>1648</sup> FORBRUKERRÅDET, ‘250,000 words of app terms and conditions’ (14 May 2016 accessed 22 Aug 2016) <<https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/>>

Consumer “informational overload” generates confusion and “sub-optimal” decision-making:<sup>1649</sup> one survey found that one in five consumers have ticked a consent box to unknowingly extend a contract, or accidentally accepted non-cancellation clauses.<sup>1650</sup> In the CIOT, these online risks multiply with serious consequence: consumers may sign-away information privacy,<sup>1651</sup> or sign-up for constant surveillance,<sup>1652</sup> unknowingly. Taking these evidence- based asymmetries into account, and given greater provider bargaining power, use of non-negotiable and legally protective over consumer-friendly contracts, there seems little consumer incentive to read much less understand, CIOT terms. In other words, perhaps a rational – and irrational - consumer would not read them at all.

And that, is a big consumer protection gap.

### 6.3 Rational consumers & certain choices

*“Notice and choice, in a highly complex and connected environment is next to impossible...”<sup>1653</sup>*

*“There are essentially no defenders anymore of the pure notice-and-choice model... It’s no longer adequate.”<sup>1654</sup>*

*“Consent should be granular.”<sup>1655</sup>*

Failing to read contracts entails consumer detriment: it leaves consumers ill-informed and disempowers them in the marketplace. Asking *why* is critical to consumer policy making, with an answer which undermines extant consumer protection approaches. There are two streams of thought as to this disempowering behaviour: one drawn from neo-classical economics, upon which classical ‘notice and choice’ theory is premised, and the other from behavioural economics, which draws upon psychology and economics. At its simplest, neo-classical economics deductively assumes that humans are *rational* decision-makers,<sup>1656</sup> that is, informed consumers will make choices reflecting their best interests and

---

<sup>1649</sup> Patrick Xavier, ‘Behavioural Economics and Customer Complaints in Communications Markets’ *ACMA Research* (2011 accessed 5 Jul 2016) :5 <<http://www.acma.gov.au/Industry/Telco/Reconnecting-the-customer/Public-inquiry/communications-behavioural-economics-research-reconnecting-the-customer-acma>>

<sup>1650</sup> *Ibid.*

<sup>1651</sup> Bailey, above n 51.

<sup>1652</sup> Peppet, above n 283:139- 143.

<sup>1653</sup> Jedidiah Bracy, ‘On Building Consumer-Friendly Privacy Notices for the IoT’ *Privacy Tech* (6 Nov 2015 accessed 29 Apr 2016) <https://iapp.org/news/a/on-building-consumer-friendly-privacy-notices-for-the-iot/>

<sup>1654</sup> Daniel Weitzner, a senior policy official at the NTIA, cited in Steve Lohr, ‘Redrawing the route to online privacy’ *Taipei Times, NY Times News Service* (3 Mar 2010 accessed 10 Jan 2016) <<http://www.taipetimes.com/News/editorials/archives/2010/03/03/2003467037>>

<sup>1655</sup> Article 29 WP, above n 638. The Art 29 WP identified bundled consent as one area where forced consent should be prohibited and consumers must be given a free choice to accept or reject data processing and still use the service.

<sup>1656</sup> Richard A. Posner, ‘Rational Choice, Behavioural Economics, and the Law’ *Stanford Law Review* 50: 5 (May, 1998) 1551-1575 <http://www.jstor.org/stable/1229305> Posner refers to the classic definition as “choosing the best means to the

minimising personal detriment. In considering why consumers fail to read contracts, a recent EU study concluded it “rational” cost: benefit- driven behaviour: reading costs are high (due to length, etc.) and the benefits are low given contracts are non-negotiable and the desired transaction cannot occur without ‘acceptance’:

It would be unrealistic but arguably also unnecessary to expect all consumers to read and comprehend all T&Cs...In most cases, these T&Cs will not have an impact on the performances by the parties...<sup>1657</sup>

Behavioural economics (BE) challenges neo-classical economics by inductively considering irrational behavioural traits, to understand why consumers do not necessarily act in their own best interests, and the complex processes underpinning consumer decision-making.<sup>1658</sup> BE is increasingly informing consumer policy making internationally: <sup>1659</sup>

It does not necessarily counsel heavy-handed paternalistic consumer protection regulation...A sensible approach ... seek[s] to install relatively less intrusive measures that inform and ‘nudge’<sup>1660</sup> more informed, empowered consumers towards better decisions (e.g. through the use of greater transparency and information disclosure and default options that recognise behavioural tendencies), without unduly raising service provider compliance costs...

Acquisti et al conclude that informed consumer decisions as to online data collection are “severely hindered” because consumers have imperfect or asymmetric information as to when, why and what consequences it entails.<sup>1661</sup> They identify three themes: consumer uncertainty as to privacy trade-offs and preferences,<sup>1662</sup> powerful context-dependence<sup>1663</sup> and privacy preference malleability, by those with

---

chooser’s ends” [page 1551]. He points out that it long ago abandons the idea of consumers as “hyperrational” and argues BE is “antitheoretical”.

<sup>1657</sup> EC, ‘Study on consumers’ attitudes towards Terms and Conditions (T&Cs) Final’ (2016 accessed 2 Dec 2016) report<[http://ec.europa.eu/consumers/consumer\\_evidence/behavioural\\_research/docs/terms\\_and\\_conditions\\_final\\_report\\_en.pdf](http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/terms_and_conditions_final_report_en.pdf)>

<sup>1658</sup> Patrick Xavier, above n 1649: 5 – 6.

<sup>1659</sup> It may be defined broadly, as “the application of inductive scientific method to the study of economic activity”: Pete Lunn, ‘Regulatory Policy and Behavioural Economics’ *OECD* (2014 accessed 16 Feb 2016): 20 <<http://dx.doi.org/10.1787/9789264207851-en>>

<sup>1660</sup> A ‘nudge’ means a policy of libertarian paternalism which “sets the architecture” based upon a benefit arising through free choice; so where a regulator has responsibility in an environment where consumers are making suboptimal decision, the nudge has two aspects: firstly, free choice is retained by not preventing the suboptimal choices; and secondly, BE is used to alter the decision-context such that better decisions become more likely. Note a nudge requires a positive regulatory impact analysis such that ex-ante outcomes are an improvement: *Ibid*.

<sup>1661</sup> Acquisti, above n 579.

<sup>1662</sup> Uncertainty arises through information asymmetry especially where privacy harms can be hidden or intangible as well as human uncertainly generally as to preferences: *Ibid* 510.

<sup>1663</sup> This means that the extent of privacy concern – from apathy to extreme concern – may depend upon the situation: *Ibid*: 511.

greater information.<sup>1664</sup> Consumers also suffer “consent fatigue”<sup>1665</sup> and potential biases or misperceptions, including:<sup>1666</sup>

**Choice overload:** comparing too many products and features creates consumer confusion, random choice-making or failure to choose at all. ‘Bundled consent’ may be an example of this: consumers may object to one of multiple uses but feel pressure to consent to all – or do nothing about the one.

**Default inertia:** may operate as to ‘opt out’ decisions, which take more effort than ‘opting in’.<sup>1667</sup> Default settings as to device operation and contract inclusions, are thus important to consumer protection outcomes. Research suggests that best practice privacy and security by default settings with an opt-out would improve consumer choice and CIOT security/ privacy. But predictive advertising experience suggests that vested or self-interests may pressure manufacturers against consumer-protective defaults.<sup>1668</sup> as such, incentivising defaults may require mandatory regulation.

**Endowment:** consumers value something owned more than pre-purchase, and may be reluctant to give it up – this favours incumbent brands as consumers may exhibit misplaced loyalty or reluctance to acknowledge poor past choices. Recent research bears out brand-adherence in smart homes.<sup>1669</sup>

**Framing bias:** consumer choice and decision-making is influenced by information presentation mode, with effect size depending if options are perceived as a loss or gain.<sup>1670</sup> For example, the Fitbit term extract cited above encourages sensible trust, downplaying its warnings-based intent.

---

<sup>1664</sup> Alessandro Acquisti, Laura Brandimarte and George Lowenstein, ‘Privacy and human behaviour in the age of information’ *Science* (30 Jan 20125) 347: 6221: 509 -514.

<sup>1665</sup> This means where users are so used to ticking privacy policies to continue browsing or purchasing online that the gesture has “lost all significance”: Felicity Turton, IFCLA Conference 2016, ‘Shifting the burden of consent under the GDPR’ (18 Feb 2016 accessed 24 Apr 2016) <<http://www.scl.org/site.aspx?i=ed46562>>

<sup>1666</sup> Xavier, above n 1649: 4- 5.

<sup>1667</sup> See for example, ACMA, ‘Community research on informed consent’ (2011 accessed 4 Jul 2016) <<http://www.acma.gov.au/theACMA/informed-consent-research>>. A recent example is that Jetstar had its insurance default set to ‘yes’ and the ACCC has recently persuaded it to change that due to consumer complaints.

<sup>1668</sup> Mathews-Hunt, above n 185.

<sup>1669</sup> Parks Associates, ‘Parks Associates: Safety and Home/Away Use Cases Dominate Smart Home Interoperability Matrix’ (29 Nov 2016 accessed 22 Jan 2017) <<http://www.marketwired.com/press-release/parks-associates-safety-home-away-use-cases-dominate-smart-home-interoperability-matrix-2179177.htm>>

<sup>1670</sup> Briedis, above n 1367: 44.

One privacy study found that people desiring privacy protections (a 'gain') prefer to opt-"in" (72%) rather than "out" (46%),<sup>1671</sup> but also that framing decreases as perceived risk increases.<sup>1672</sup>

**Heuristics:** complex decision-making may be short-circuited by consumer short cuts, such as following other's actions/ advice. This explains why regulators are actively pursuing fake online review cases to prevent consequential market failure – and why reviews are increasingly valued as self-corrective consumer mechanisms.<sup>1673</sup>

**Hyperbolic discounting** occurs because consumers and providers use short-sighted decision-making: they over-value immediate (over future) costs and benefits. In a CIOT world, this may mean engaging in privacy-sacrificial behaviours without factoring in likely, less certain future privacy detriments.<sup>1674</sup>

**Unrealistic optimism or overoptimism** means that consumers have an over-inflated view of themselves and are unskilled at assessing the likelihood of experiencing a negative event.<sup>1675</sup> An example is a consumer's belief s/he is less likely to experience data loss harm than others; therefore, perceived risk (if any) is assessed as relatively low or lower than it is. Susceptibility to this bias increases with increased numbers of CIOT devices owned.<sup>1676</sup> For example, a smart car Snapshot device collects driving data for insurance premium calculations, but recently, to also increase 'bad' driver premiums. It is predicted that as users retain a sense of control, they may underestimate their risk of a premium increase.<sup>1677</sup>

**Risk/loss aversion preference** is greater than gains preference, which may inhibit consumers from switching products or suppliers for fear that new unknown one(s) may be worse, which may reduce market competition

BE factors may influence consumer decisions as to purchase, 'accepting' CIOT contracts and post-contract decisions as to complaints. As Bar-Gill argues, consumer contracts form through the interaction

---

<sup>1671</sup> T Baek, Y Bae, I Jeong, E Kim and J Rhee, 'Changing the default setting for privacy protection: What and whose personal information can be better protected?' (2014 accessed 2 Dec 2016) 51 *Social Science Journal* 524-33 cited in Briedis et al, above n 1367: 44.

<sup>1672</sup> Ibid.

<sup>1673</sup> ACCC, 'Fake online reviews' webpage <<https://www.accc.gov.au/business/advertising-promoting-your-business/managing-online-reviews>>

<sup>1674</sup> See Bailey's discussion of this where she suggests that IOT consumers are more likely to be hyperbolic discounters because the immediate benefit (buying the device) is certain whereas the privacy trade-off (via the contract) is uncertain into the future: Above n 51: 1040.

<sup>1675</sup> Bailey, above n 51:1035.

<sup>1676</sup> Ibid: 1043. The bias impacts both the idea that a person is less likely than an average person, but also, that the actual probability of something occurring is less likely than it is.

<sup>1677</sup> Ibid: 1045.

of market forces and consumer psychology, and the latter entails a “myriad of biases and misperceptions” which influence market outcomes.<sup>1678</sup> Competition does not help and may even exacerbate, certain resulting market failures.<sup>1679</sup> Indeed, they may shape supplier behaviours anti-competitively; for example if Google Home can ‘lock in’ consumers via non (or limited) product interoperability (generating high switching costs), and endowment works in their favour, then Google are not incentivized to provide good customer service, unless consumers convey its importance. Absent that, business is de-incentivized to invest in service, consumers may (optimistically) assume Google to be no worse than others, such that a competitor which does invest may reduce or not improve its market share and may even lower its profit margin. In the long term, it may make market sense to let customer service decline while already service-poor firms have little incentive to improve.<sup>1680</sup>

Sellers operating in a competitive market, have no choice but to align contract design with the psychology of consumers. Put bluntly, competition forces sellers to exploit the biases and misperceptions of their customers.... Better legal policy can help consumers and enhance market efficiency.<sup>1681</sup>

This is market failure which a regulator might correct through policy; for example, by increasing consumer market information, by publishing service metrics and/ or by prosecuting suppliers whose poor service breaches the law.

As identified above, due to implicit technicality, complexity and novelty (amongst other things) the CIOT market evidences “information asymmetry”, whereby providers have greater information and consumers have inadequate information upon which to make positive, efficient decisions. But even where adequate information exists, behavioural tendencies may generate sub-optimal decisions – a pro-competition framework requires better quality information disclosure in structured, understandable formats:

Behavioural economics underlies the importance of making use of ‘smarter information – thinking carefully about its framing, the context in which information is read, and the ability of consumers to understand it.<sup>1682</sup>

A recent EU study adopted recommendations to improve the “substantive quality” of consumer contracts through firstly, “increasing transparency” (to shorten and simplify) - assuming that consumers are

---

<sup>1678</sup> Bar-Gill, above n 51: 8.

<sup>1679</sup> Ibid.

<sup>1680</sup> Xavier, above n 1649: 5.

<sup>1681</sup> Bar-Gill, above n 51: Introduction (page 2).

<sup>1682</sup> Xavier, above n 1649: 5.

motivated to understand certain terms, so as to forestall any economic consequences<sup>1683</sup> - to create “effortless awareness”.<sup>1684</sup> This focussed on consumer awareness of contract quality (rather than content), using a quality cue such as a trust mark or trusted-body endorsement system indicating a contract is “fair”.<sup>1685</sup> These may be communicated visually as well as through text, and convey either a summary of key actionable metrics or a more generalised (often settings-implicit) ‘trust’ rating:



Graphics 6.2(left) and 6.3(right) Traffic light and Privacy dashboard approaches  
Sources: Open Notice<sup>1686</sup> and Privacync IAPP<sup>1687</sup>

The study concluded that contract simplification offers “beneficial effects” such as higher readership, better understanding and a more positive consumer attitude, while a quality cue increases trust levels and purchase intent.<sup>1688</sup> UC Berkeley suggest that from a privacy information perspective, a dashboard is effective for any service which collects, aggregates or processes user PI, especially if that information changes over time and/ or is collected or aggregated in ways that might be “unexpected, invisible or easily forgotten”, or where users have access, correction and deletion options.<sup>1689</sup> It seems the ‘pictures’

<sup>1683</sup> Under Article 5 of the Unfair Contract Terms Directive the EU Court of Justice has emphasized that contracts must be in plain, simple language such that the “average consumer can foresee, on the basis of clear, intelligible criteria, the economic consequences which derive from those terms for the consumer”: CJEU, Case No C-26/13, ECLI:EU:C:2014: 282 (Kasler) at point 73, cited Ibid: footnote 1.

<sup>1684</sup> While the trustmark provides an instant cue, the study recognised the importance of the related regulatory strategy of education: that is, to better inform consumers as to their legal rights generally; such that they know their entitlements so the terms are irrelevant in that context: Ibid: 29- 30.

<sup>1685</sup> Ibid: 7.

<sup>1686</sup> Open Notice, Mark Lizar and John Wunderlich, ‘Kantara Consent Receipt Presentation’ (n.d. accessed Apr 2017) <https://kantarainitiative.org/wp-content/uploads/2014/10/Kantara-Consent-Receipt-Presentation.pdf>

<sup>1687</sup> Privacy dashboard as to US Fitbit – as such its findings relate to the US FIPPS: Bracy, above n 1653.

<sup>1688</sup> Ibid: 68. Note that some of the effects upon simplification were described as “small”. Notably consumers did not feel they missed any relevant information (although they may have). The obvious point here is that lawyers may feel that certain information cannot be missed which preserves length.

<sup>1689</sup> UC Berkeley School of Information, ‘Privacy dashboard’ (n.d. accessed 20 Nov 2016) <<https://privacypatterns.org/patterns/Privacy-dashboard>>

can simplify while words ‘complicate’: ironically, while consumer regulators and unfair contract terms laws favour shorter, simpler terms, other regulation may impose requirements generating length and complexity,<sup>1690</sup> as may prudent legal advice. In the event of a dispute, a less comprehensive contract may disadvantage the provider, especially in a global context, but perhaps ‘comprehensive’ should be distinguished from ‘complex’.<sup>1691</sup> Indeed, if providers want to retain flexibility and freedom to contract without increasingly consumer-protective content prescription (which seems probable over time), then they need to respond proactively to improving contract content and consent practices overall. This highlights the need to incentivize better practices to recreate a consumer-friendly online-contracting ‘language’, through both mandatory contract ‘transparency’ regulation, and identifiable, independent consumer cues, such as dashboards, traffic light systems and trust marks.<sup>1692</sup>

Behavioural economics insights represent practical, targeted, time and cost efficient solutions. In an information asymmetry scenario, market performance may be improved using BE insights to:

- Identify the behavioural changes and outcomes sought;
- Align information with business incentives to garner support;
- Align information with the wider “pro-competitive regulatory system” and existing regulation, such as the ACL and PA;
- Frame information to be simple and of value to consumers and business, to incentivize mutual behavioural changes; and
- Regulatory information should incentivize “best/ good practice” behaviours, including invoking reputational impact concerns.<sup>1693</sup>

Recent evidence<sup>1694</sup> also supports that view that ‘notice and choice’-based policy fails to empower consumers and is flawed in a privacy terms context. Data-collection practices of industry, app providers<sup>1695</sup> and others – as contractually expressed - are usually justified in policymaking as a trade-

---

<sup>1690</sup> Ibid: 27- 28.

<sup>1691</sup> For example, Microsoft finally implemented a comprehensive privacy dashboard in 2015 to create “straightforward terms and policies that people can easily understand” and has refined multiple services policies into one, plus a renewed privacy policy: Horacio Gutierrez, ‘Improving the Microsoft Services Agreement and Privacy Statement for consumers’ Microsoft (4 Jun 2015 accessed 5 Jan 2016) <<https://blogs.microsoft.com/blog/2015/06/04/improving-the-microsoft-services-agreement-and-privacy-statement-for-consumers/>>

<sup>1692</sup> Any third-party mark, logo, picture, or symbol provided to dispel consumer concern as to security and privacy, and to increase firm-specific trust levels: K Damon Aiken and David M Boush, ‘Trustmarks, Objective-source Ratings, and Implied Investments in Advertising: Investigation Online Trust and the Context-specific Nature of internet Signals’ *Journal of the Academy of Marketing Science*, 34:3 (2008) 308- 323 <<http://jam.sagepub.com/ggi/content/abstract/34/3/308>>

<sup>1693</sup> Xavier, above n 1649 :6.

<sup>1694</sup> Turow, above n 466.

<sup>1695</sup> For a clear explication of how privacy consents are managed on smartphones, see Florian Schaub, Rebecca Baleako, Adam L. Durity & Lorrie Faith Cranor, ‘A design space for effective Privacy Notices’ 2015 Symposium on Usable privacy and security, USENIX Association, Submission to FTC PrivacyCon (2016 accessed 5 Apr 2016): 11 <<https://www.ftc.gov/policy/public-comments/initiative-623>>

off regime whereby consumers fully understand the opportunities and costs of allowing or volunteering PI collection and use, and choose to do so. The privacy paradox<sup>1696</sup> - that consumers give information despite personal objection - is factored into their decision-making calculus, so the argument runs, and justifies the present approach. But as evidenced above, most consumers do not read the contracts legitimising data collection and use, so information asymmetry is real. This prima facie undercuts conceptions of consent. Further, many consumers “overestimate the extent to which the government protects them from discriminatory pricing” and 65% think a website privacy policy means that their PI will not be shared.<sup>1697</sup> The study identifies many other surprising examples of consumer misconceptions<sup>1698</sup> and concludes that privacy-sacrificing decisions are commonly based upon incorrect information. In Australia, the ACL Survey 2016 suggests likewise: it found that most consumers (incorrectly) believe that businesses which treat consumers ‘unfairly’ will be detected (51%) and penalised (42%).<sup>1699</sup> Further, while consumers are aware of the APC (47%),<sup>1700</sup> 69% are more concerned about online privacy but 65% do not read privacy policies,<sup>1701</sup> and only 7% would report PI misuse. One suspects that few Australians understand from its title, that the ‘privacy’ Act is not premised upon privacy ‘protection’ per se, but rather, upon disclosure and (often implied) consumer consent.

Turow et al found that Americans are not playing loose with their PI: they do not view ‘data for discounts’ (or download or analytics, etc.) as a “square deal”, nor do informational asymmetries as to use practices explain their willingness to provide PI to entities like CIOT providers.<sup>1702</sup> Instead, Turow’s study finds that consumers are “resigned” to giving up PI without choice. Consumers regard the undesirable outcome (surveillance and disclosure) is inevitable and feel “powerless to stop it”:

---

<sup>1696</sup> Turow, above n 466: 5. Surveys often reveal this: for example, consumers may want real-time shopping promotions (60%) but only 14% wants to share their browsing history and 20% will share their location – both of which are required to provide the former.

<sup>1697</sup> Ibid: 4.

<sup>1698</sup> Aswini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti & Ruogo Kang, ‘Expecting the Unexpected: Understanding mismatched Privacy Expectations Online’ *Submission to ACM Conference on Human Factors in Computing* (2016 accessed 5 Apr 2016) <[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00081-99936.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00081-99936.pdf)>

<sup>1699</sup> Australian Government, ‘Australian Consumer Survey 2011’ *Sweeney Research* (2011 accessed 22 Oct 2015) [http://consumerlaw.gov.au/files/2015/09/Australian\\_Consumer\\_Survey\\_Report.pdf](http://consumerlaw.gov.au/files/2015/09/Australian_Consumer_Survey_Report.pdf)> Conversely, businesses report a \$3.5B decline in compliance costs, from \$21.56B to \$18.03B.

<sup>1700</sup> The OAIC 2013 study showed 82% were aware of the PA with 17% not aware and 1%, unsure. The study did not test consumer understanding as to content (beyond the Act’s name) and provided a definition of PI to consumers to assist them to answer questions OAIC, above n 458 [Research Report & Survey Appendix]; The 2017 Survey found that less than half (47%) are aware of the Privacy Commissioner (APC), but only 7% would report misuse of information to the APC. Worse, nearly half (47%) were unable to name any agency for such a report to, with the most likely choice being the police (12%): OAIC, above n 458: iii.

<sup>1701</sup> Ibid (2017).

<sup>1702</sup> Turow, above n 466.

Our study reveals that more than half do not want to lose control over their information but also believe this loss of control has already happened.<sup>1703</sup>

OAIC 2017 data shows few Australians will trade PI for rewards and benefits (33%) or for a chance to win a prize (20%).<sup>1704</sup> This conforms to many studies evidencing that consumers value privacy and do not like PI use and exploitation.<sup>1705</sup> Further, that value is contextual: people regard their (smart) homes, bodies and cars as private spaces, which is an important consumer trust factor to which CIOT contracts often feign indifference.

That indifference leads to another fundamental consumer IOT issue without norms, which requires urgent regulatory attention.

#### 6.4 But I own my own data... don't I?

*In short, there is no uniform approach...*<sup>1706</sup>

*Who owns the data in IOT? The answer is, it's complicated...*<sup>1707</sup>

*"A tipping point could be reached where people will realize "that data belongs to me,"*<sup>1708</sup> – Tim Berners-Lee

Smart home, car and self surveys suggest that consumers believe they should own their own data.<sup>1709</sup> That view is shared by the Productivity Commission,<sup>1710</sup> EU activist groups<sup>1711</sup> and the Obama FCC,<sup>1712</sup> but a *question* ultimately determined by "presumptively market-alienable" rights<sup>1713</sup> determined by CIOT

---

<sup>1703</sup> Turow, above n 466.

<sup>1704</sup> OAIC, above n1700: ii.

<sup>1705</sup> OAIC, above n 1700.

<sup>1706</sup> Mercer, above n 88.

<sup>1707</sup> Gareth Corfield, 'Internet of Things Security? Start with Who Owns the Data' *The Register* (28 Sept 2016 accessed 4 Dec 2016) <[http://www.theregister.co.uk/2016/09/28/cambridge\\_wireless\\_iot\\_event\\_defence\\_sig/](http://www.theregister.co.uk/2016/09/28/cambridge_wireless_iot_event_defence_sig/)>

<sup>1708</sup> Klint Finley, 'Tim Berners Lee, 'Inventor of the web, plots a radical overhaul of his creation' *WIRED* (4 Apr 2017 accessed 4 Apr 2017) <[https://www.wired.com/2017/04/tim-berners-lee-inventor-web-plots-radical-overhaul-creation/?mbid=nl\\_4417\\_p2&CNDID=>](https://www.wired.com/2017/04/tim-berners-lee-inventor-web-plots-radical-overhaul-creation/?mbid=nl_4417_p2&CNDID=>)>

<sup>1709</sup> Turton, above n 1665.

<sup>1710</sup> PC, above n 179. The Paper states: "A key element is to increase the control of individuals over their data".

<sup>1711</sup> See for example, [www.mycarmydata.eu](http://www.mycarmydata.eu)

<sup>1712</sup> "The bottom line is that it's your data. How it's used and shared should be your choice." Former Obama FCC Chair Wheeler on the announcement of the Trump-defunct new Rules as to ISP data use: Federal Communications Commission (FCC), 'In the Matter of Protecting the Privacy of Customer of Broadband and Other Telecommunications Services' Notice of Proposed Rulemaking (1 Apr 2016 accessed 2 Aug 2016) (WC Docket No. 16-106) <https://www.fcc.gov/document/fcc-releases-proposed-rules-protect-broadband-consumer-privacy>

<sup>1713</sup> Margaret Jane Radin, 'Incomplete Commodification in the Computerized World', in Niva Elkin-Koren & Neil Weinstock Netanel eds. *The Commodification of Information* (2002): 17. 'It makes a big difference whether privacy is thought of as a human right, attaching to persons by virtue of their personhood, or as a property right, something that can be owned and controlled by persons.

contracts. At law, there is no property right in a piece of data,<sup>1714</sup> nor is there a “uniform approach”<sup>1715</sup> to data ownership or databases across jurisdictions.<sup>1716</sup> Depending upon the terms and conditions of CIOT collection agreements, consumers may have all rights, shared rights or (effectively) none at all – save for the ‘right’ to cease data flow by turning an (expensive) device off. Consumer data collected within the CIOT ecosystem may be governed by the terms, or by third party terms, and even by linked social media terms. Through these, data ownership (aka use rights) very quickly dissipate beyond consumer control. Hoofnagle et al even assert that some firms use data industry “gag notices” imposing confidentiality as to data transfers upon third party recipients.<sup>1717</sup>

CIOT industry approaches differ: few promise not to use data and most reserve extensive rights to do so. Samsung, for example, marketed that consumers will own their smart home data:<sup>1718</sup>

“You own your User Submissions and Device Data, and SmartThings does not claim any ownership over your User Submissions or Device Data...”

But Samsung are granted a license:

“...you hereby do and shall grant SmartThings a worldwide, non-exclusive, perpetual, irrevocable, royalty-free, fully paid, sub-licensable and transferable license to use, modify, reproduce, distribute, share, prepare derivative works of, display, perform, and otherwise fully exploit the User Submissions and Device Data in connection with the Services, and SmartThings' (and its successors' and assigns') business...”<sup>1719</sup>

---

<sup>1714</sup> Adam Rendle, ‘Who owns the data in the Internet of Things?’ *Taylor Wessing* (Feb 2014 accessed 19 Nov 2015) <[http://united-kingdom.taylorwessing.com/download/article\\_data\\_lot.html](http://united-kingdom.taylorwessing.com/download/article_data_lot.html)>

<sup>1715</sup> Mercer, above n 88.

<sup>1716</sup> Database rights may be relevant. In Australia, the *Copyright Act 1968* (Cth) states a compilation (s. 10) or database must demonstrably be an original literary work, (s. 32) and the High Court has found that absent the relevant authorship and originality, and regardless of significant expense or labour, copyright is not the appropriate means to protect such works. In summary, in the EU, there must be a database as defined; that is, ‘a collection of independent data which are arranged in a systematic or methodical way and which are individually accessible’. This would usually include the “capture, transfer and analysis of data” so it seems likely that IoT data captured by a device, transferred and analysed by an app falls within that definition. Further the maker must have a substantial investment in that process of collection and arrangement, which seems assumed in an IoT product development context. Finally, the maker of the database must have a substantial business or economic connection with an EEA state, which means incorporation plus a principal place of business or business administration in that state or have its registered office within a state together with its operations linked with that state economy in an ongoing basis: Rendle, above n 1714. See *Desktop Marketing Systems Pty Ltd v Telstra Corporation Limited* [2002] FCAFC 112 where the Full Federal Court found “originality” in Telstra’s White Pages, which was a compilation of Telstra customer information provided to it free-of-charge by customers. *Telstra Corporation Limited & Anor v Phone Directories Company Pty Ltd & Ors* [2010] FCA 44; *Nine Network Pty Limited v IceTV Pty Limited* [2009] HCA 14. The case concerned a subscription-based electronic TV guide which the court held did not reproduce a “substantial portion” of channel 9’s TV programme schedule, and so did not infringe the Copyright Act, despite significant labour or expense involved. In the UK, the Copyright and Rights in Databases Regulations 1997 implemented the 1996 EC Council Directive on the legal protection of databases from 1 January 1998.

<sup>1717</sup> Hoofnagle, above n 55.

<sup>1718</sup> Hong, above n 322.

<sup>1719</sup> The clause concludes: “including without limitation for promoting and redistributing part or all of the Services in any media formats and through any media channels (including, without limitation, third party websites and services)...”: Samsung, ‘Samsung Smart Home Terms of Service (UK)’ (3 Sept 2015 accessed 2 Aug 2016)

And should a third party dispute their PI being used, the consumer must provide an enforceable warranty:

"You represent and warrant that you own or otherwise control all rights to such User Submissions and Device Data and that disclosure and use of such User Submissions and Device Data by SmartThings... will not infringe or violate the rights of any third party.<sup>1720</sup>

While it has extensive user rights, Samsung does not promise to preserve data either:

"...SmartThings has no obligation to maintain or persist your User Submissions or Device Data for any specified period of time, to guarantee access to User Submissions or Device Data,  
...<sup>1721</sup>

From a BE perspective, providers "transfer business costs" to consumers every time PI is transferred to another party, as well as transfer business risk via terms and poor attendant security.<sup>1722</sup> VTech children's toys were hacked, resulting in unauthorised access to the PI of 11.2 million people,<sup>1723</sup> so they inserted a (now-removed) term outsourcing risk back to consumers:

"You acknowledge and agree that any information you send or receive ... may not be secure and may be intercepted or later acquired by unauthorised parties. ... [and that] your use of the site and any software or firmware downloaded therefrom is at your own risk."<sup>1724</sup>

This clause is likely void as unfair in the UK<sup>1725</sup> and infringes the consumer guarantee provisions under the ACL, as well as section 18 for misleading consumers as to their rights. It may also be 'unfair' in Australia by imposing greater risk burden on consumers which causes them detriment, and given APP11 imposes security obligations, is not 'reasonably necessary' to protect VTech's legitimate business interests.<sup>1726</sup> The problem is of course, that consumers who read and accept the terms are misled and may not pursue redress, those who complain to the provider will be referred to the terms and mostly 'switched off', and regulators will never know unless a persistent (or legally informed) consumer complains - or an industry sweep occurs. As these clauses suggest, industry practices vary, and many incidents of data ownership are reserved if not appropriated contractually by providers.

---

<<https://www.smarthings.com/uk/terms>> The same terms appears on the Australian website here:  
<https://account.samsung.com/membership/etc/specialTC.do?fileName=smarthome.html>

<sup>1720</sup> Ibid.

<sup>1721</sup> Ibid.

<sup>1722</sup> Hoofnagle, above n 55.

<sup>1723</sup> Patto, above n 618.

<sup>1724</sup> The Australian privacy policy is a scroll wrap document and as to security, includes: "...no data is entirely secure and safe from a breach or failure of data backup and security. Accordingly, whilst we take reasonable steps in relation to security of its services, we exclude all warranties and disclaim to the full extent permitted by law all liability in relation to data backup and security." VTech Electronics (Australia) Pty Ltd, 'Privacy Policy (Australia)' (n.d. accessed 20 Feb 2017)  
<[https://www.vtech.com.au/privacy\\_policy/](https://www.vtech.com.au/privacy_policy/)>

<sup>1725</sup> Data Protection Directive 95/46 EC and Consumer Rights Act 2015 (UK).

<sup>1726</sup> ACL ss 24 (1)(a)-(c) inclusive.

Indeed, some assert outright ownership:

...you acknowledge and agree that all information you communicate to Nestlé through the Internet... becomes and will remain our exclusive property with unrestricted rights to use it...<sup>1727</sup>

Smart cars present an industry-wide controversial example: it seems likely that consumers will not “own” their driving or vehicle information detected/ recorded by their smart car as manufacturers assert that their software and algorithms are proprietary technology, licensed for use with the consumer-owned device (their car).<sup>1728</sup> Tesla for example, disclose that electronic modules collect vehicle driving and systems data – including trip, acceleration, braking, systems deployment, speed, location, direction and the uniquely-identifying VIN<sup>1729</sup> – all wirelessly transmitted to Tesla. They use data for service and “various purposes” and aside from “its [unidentified] partners” do not disclose it to third parties without owner agreement or consent or that of any “leasing company”, which raises the interesting prospect that in-car app permissions onscreen may be used to achieve such consents. Disclosure exceptions are court order, official police request, Tesla lawsuit defence, anonymised research purposes or to its data management providers or any [undefined] “Tesla affiliated company”. As to ownership, the Manual is silent,<sup>1730</sup> save for this:

Tesla does not disclose the data recorded to an owner unless it pertains to a non-warranty repair service and in this case, will disclose only the data that is related to the repair.

The argument was first controversially-put by John Deere, to significant criticism that they were using copyright to undermine tractor ownership and to prevent non-dealer repair.<sup>1731</sup> Consumers can ‘opt-out’ of providing data, but Tesla’s privacy statement contains a strong caution:

...if you opt out from the collection of Telematics Log Data or any other data from your Tesla vehicle... [excluding Data Sharing]<sup>1732</sup>... we will not be able to notify you of issues applicable to

---

<sup>1727</sup> Nestlé Australia Disclaimer dated 27 Nov 2001 accessed <<http://www.nestle.com.au/info/disclaimer>> Note that their smart self device app communicates to Nestlé via the internet, though query whether this broad international website disclaimer is intended to apply where there are more explicit terms. The position seems unclear.

<sup>1728</sup> Weins, above n 410. In Australia, this argument has played out in apparent attempts by the manufacturers to inhibit the after-market car repair industry (so the latter assert): AAAA, above n 401. In the US, data sharing is agreed, but in Australia after-market participants complain the manufacturers have failed to comply with a non-binding Code and are hoping a new enquiry into the industry will result in a binding code or regulation to compel cooperation.

<sup>1729</sup> Tesla, above n 1128 ‘Model S Owner’s Manual v 5.9’ at page 180 under ‘Vehicle Telematics/ data Recorders’.

<sup>1730</sup> Personal data (defined as saved music favourites, imported contacts, ‘Homelink’ programming, addresses etc) can be deleted to reinstate defaults: Ibid: 103 but there is no indication whether such data has already been transmitted to Tesla and so could be retained by them.

<sup>1731</sup> Weins, above n 410; Steve Brachman, ‘John Deere, GM push back against consumer modifications of vehicle software’ IPWatchdog (1 Jul 2015 accessed 3 Jul 2016) <<http://www.ipwatchdog.com/2015/07/01/john-deere-gm-push-back-against-consumer-modifications-on-vehicle-software>>. John Deere’s position is best explained here: Agpro, ‘Deere memo clarifies equipment/software ownership’ (19 May 2015 accessed 3 Jul 2016) <<http://www.agprofessional.com/news/deere-memo-clarifies-equipmentsoftware-ownership>>

<sup>1732</sup> This system uses the car’s external cameras to collect short video clips to improve Tesla’s systems for recognition of traffic lights, lane lines, street signs, and traffic light positions. Consumers can opt out and Tesla assures users it is not

your vehicle in real time, and this may result in your vehicle suffering from reduced functionality, serious damage, or inoperability, and it may also disable many features of your vehicle including periodic software and firmware updates, remote services, and interactivity with mobile applications and in-car features such as location search, Internet radio, voice commands, and web browser functionality.<sup>1733</sup>

BE would call this a 'push' and possibly an example of hyperbolic discounting, that is, consumers prefer to avoid the short-term cost of losing "certain services" over the longer-term benefit of withholding information. Consumers may also exhibit over-optimism as to the negative impacts of vehicle data collection. Based upon recent European analyses,<sup>1734</sup> it is possible that service denial for coercive (non-legitimate) purposes may be an unfair term in Australia (depending upon the facts); however, the example cited appears legitimate insofar as real time notifications and software updates are important safety features. It may however be that privacy-by-design systems should be designed to make opting out granular; such that safety features are not bundled with others. The GDPR addresses 'freely given' consent explicitly which the Australian PA does not,<sup>1735</sup> and considers "consent fatigue" and coercion – such as contract performance being conditional upon data use consents not necessary to perform the contract.<sup>1736</sup> For example, a general 'warning' may not adequately inform consumers:

You can choose not to provide us with certain types of information, but if you do so we may not be able to provide you with certain services or it may affect your ability to use or receive some services.<sup>1737</sup>

In other words, excessive data gathering bundled into other legitimate collection rationales – a practice common in the CIOT industry - may be illegal, unethical and/ or render consents invalid, at least under the GDPR.

Consumers are justifiably wary and it seems likely car manufacturers will experience pushback. A multi-country EU study of ten thousand consumers found that 90% felt that car-generated data should be owned by the vehicle owner (or driver) and 91% wanted the option to turn off all communication

---

relatable back to their vehicle: Tesla, 'Customer Privacy Policy' (accessed 10 May 2017) <[https://www.tesla.com/en\\_AU/about/legal](https://www.tesla.com/en_AU/about/legal)>

<sup>1733</sup> Tesla, 'Customer Privacy Policy' (accessed 10 May 2017) <[https://www.tesla.com/en\\_AU/about/legal](https://www.tesla.com/en_AU/about/legal)>

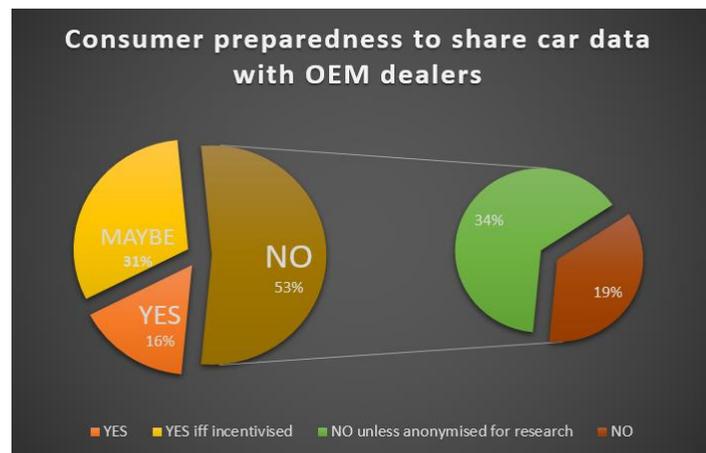
<sup>1734</sup> Article 29 WP, above n 638.

<sup>1735</sup> Article 7 Conditions for Consent; Article 8 as to child's consent.

<sup>1736</sup> GDPR Article 7(4). A precis of this clause Conditions for Consent, is: (1) the controller must demonstrate consent; (2) any request must be clearly distinguishable from other matters, intelligible and transparent and any part infringing the article (2) is not binding; (3) consent may be (easily) withdrawn at any time as a right but this does not affect data gathered prior to that occurring.

<sup>1737</sup> This clause raises risk without explaining what will happen; as such it may be misleading. It is likely to persuade consumers to avoid the risk.

altogether,<sup>1738</sup> though presumably without wholesale loss of functionality. Consumers want the right to know what data is shared when they drive, and while the disclosures discussed above are as transparent as any, they may still lack the granularity necessary. After all, only manufacturers collect vehicle data, so are best placed to disclose where that valuable treasure trove flows and who uses it for what. Further, consumer willingness to ‘share’ data is limited:



Graphic 6.4 Consumer preparedness to share car data  
Source: author using data from McCarthy<sup>1739</sup>

US evidence suggests that advertisers are pressuring manufacturers for data access,<sup>1740</sup> and while the non-binding *Auto Manufacturers’ Privacy Principles* cite respect for context, they include broad use notices and consents, and targeted advertising.<sup>1741</sup> The NTC reports that “...some in industry” want greater certainty about vehicle data access “for commercial purposes”,<sup>1742</sup> while Clayton Utz recommends “regulatory prescription”,<sup>1743</sup> and the consumer federation, FIA, lobbies for greater transparency including industry-specific data legislation,<sup>1744</sup>

<sup>1738</sup> Federation Internationale de L’Automobile, ‘What Europeans think about Connected Cars’ (Jan 2016 accessed 21 Apr 2016) <[http://www.fiaregion1.com/download/20160129\\_fia\\_survey\\_brochure\\_2016\\_web\\_fin\\_fin.PDF](http://www.fiaregion1.com/download/20160129_fia_survey_brochure_2016_web_fin_fin.PDF)>

<sup>1739</sup> Niall McCarthy, ‘Connected Cars by the Numbers’ *Statista Report* (28 Jan 2015 accessed 20 Jun 2016) <<https://www.statista.com/chart/3168/connected-cars-by-the-numbers/>>

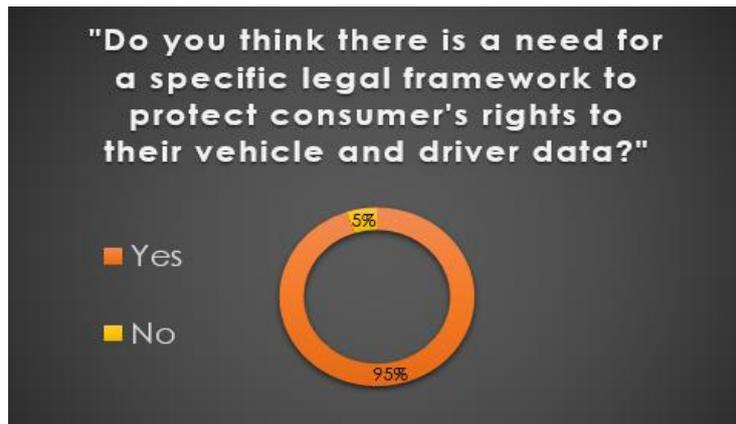
<sup>1740</sup> United States Senate Committee on Commerce, Science and Transportation, ‘Hands Off: The Future of Self-Driving Cars’ <<http://www.commerce.senate.gov/public/index.cfm/2016/3/hands-off-the-future-of-self-driving-cars>>

<sup>1741</sup> The phrase is “...Using Covered Information to provide Owners or Registered Users with information about goods and services that may be of interest to them”. “Covered Information” means 1) Identifiable Information that vehicles collect, generate, record, or store in an electronic form that is retrieved from the vehicles by or on behalf of a Participating Member in connection with Vehicle Technologies and Services; or 2) Personal Subscription Information provided by individuals subscribing or registering for Vehicle Technologies and Services – but excludes that altered or combined with the information so that the information can no longer reasonably be linked to the vehicle from which the information was retrieved: Auto Alliance, above n 399.

<sup>1742</sup> NTC, ‘Regulatory Reforms for Automated Road Vehicles’ *Policy Paper* (Nov 2016 accessed 11 Nov 2016) <[https://www.ntc.gov.au/Media/Reports/\(32685218-7895-0E7C-ECF6-551177684E27\).pdf](https://www.ntc.gov.au/Media/Reports/(32685218-7895-0E7C-ECF6-551177684E27).pdf)>

<sup>1743</sup> Clayton Utz, ‘Driving into the Future: Regulating Driverless Vehicles in Australia’ (17 Aug 2016 accessed 20 Aug 2016) <<http://www.lexology.com/library/detail.aspx?g=08533855-ae66-405c-b5ff-0482b99e60be>>

<sup>1744</sup> FIA, above n 1738, via its MyCarMyData campaign here: [www.mycarmydata.eu](http://www.mycarmydata.eu)



Graphic 6.5 Consumers (95%) want smart car user data protected by legislation  
 Source: Author using data from Federation Internationale de L'Automobile <sup>1745</sup>

So too, consumer and after-market repairer access to vehicle data (including diagnostics) is inhibited by manufacturer proprietary software, allegedly for safety as well as financial reasons. Although a voluntary data sharing code was agreed,<sup>1746</sup> under shadow of government intervention,<sup>1747</sup> it has (allegedly) functioned poorly,<sup>1748</sup> with the result that the AAAA seek a mandatory code acknowledging a consumer right to assign electronic log books and telematics data access to a chosen repairer. They argue that consumers are suffering detriment from technological lock-in and their inability to access “critical diagnostic information”,<sup>1749</sup> such as car software updates. The car companies argued that allowing access will compromise their systems and intellectual property,<sup>1750</sup> but the US Copyright Office ruled that like dvd digital rights management, people own their smart car as a physical object, but only have limited rights to its controlling software which is ©manufacturer.<sup>1751</sup> This prevents software changes, whether to

<sup>1745</sup> FIA, above n 1738.

<sup>1746</sup> AAAA, above n 1082. Stuart Charity, AAA Chair says: “Since 2009, AAAA also has advocated for a mandatory industry code that ensures manufacturers make service and repair information available to independent workshops for a fair price. A mandatory code will create a level playing field with both dealerships and independent workshops able to operate using the latest technical data. Consumers will then benefit greatly because they will have genuine choice of repairer opportunities.”

<sup>1747</sup> Discussion with Ms Lesley Yates, AAMA.

<sup>1748</sup> “Since the voluntary agreement was signed December 2015, only a handful of car companies have increased the availability of repair and service data to independent workshops via their websites. And only one out of the 68 car brands selling in Australia has fully complied with the voluntary agreement by sharing all the critical information required for today’s vehicles, such as technical service bulletins and software updates and pin-codes for the many computers built into them.”: Stuart Charity quoted in AAAA, ‘AAAA score political parties’ policies: vehicle data sharing’ (28 June 2016 accessed 30 June 2016) <<https://www.aaaa.com.au/news.asp?id=244>>

<sup>1749</sup> This includes fault codes, turn off check engine light, identify the correct oil, access a PIN code or to install a new component.

<sup>1750</sup> Steve Brachman, above n 1731; Autoblog, ‘GM claims that it owns your car’s software’ (20 May 2015 accessed 12 Nov 2016) <<http://www.autoblog.com/2015/05/20/general-motors-says-owns-your-car-software/>>; Evan Ackerman, ‘It’s Now (Temporarily) Legal to Hack Your Own Car’ (1 Nov 2016 accessed 12 Nov 2016) <<http://spectrum.ieee.org/cars-that-think/transportation/systems/its-now-temporarily-legal-to-hack-your-own-car>> The U.S. Copyright Office agreed that people should be able to modify the software that runs cars that they own, and as of December 2016 that ruling came into effect for the next two years.

<sup>1751</sup> Under the *US Digital Millennium Copyright Act*, manufacturers can potentially sue those who seek to interfere with copyrighted programming

fix problems, counteract obsolescence, or to improve security, and (detrimentally) ties consumers into parts purchases from the manufacturer only. In the US, the DMCA has granted an exemption for purposes of "...lawful diagnosis and repair, or aftermarket personalization, modification, or other improvement ...by the lawful owner of the vehicle" – excluding the vehicle entertainment system, telematics or changes which otherwise break laws (for example, emissions legislation).<sup>1752</sup>

The case illustrates both how CIOT manufacturers may use data and systems ownership anti-competitively<sup>1753</sup> and that for repairers with lesser bargaining power, a voluntary industry code may not work.<sup>1754</sup> In Australia, the copyright position is less clear. Further, a 2014 enquiry found that a lack of after-market repair access "...may lead to repair market failure and/ or consumer detriment".<sup>1755</sup> The question remains unresolved.<sup>1756</sup>

## 6.5 Consumer liability: a new era?

CIOT device data may assist to accurately allocate consumer liability, individualise insurance premiums and enhance liability efficiency, depending upon diverse factors such as device reliability, data accuracy and absent inaccurate adverse inferences or consumer profiling. Volvo assert:

*"If there is a crash and the car is in self-driving mode, even if the driver is reading a newspaper, then we – Volvo – are responsible.... However, because each self-driving car will be bristling*

---

<sup>1752</sup> Ackerman, *Ibid*. The wording is: "Allow[s] circumvention of TPMs [technological protection measures] protecting computer programs that control the functioning of a motorized land vehicle, including personal automobiles, commercial motor vehicles, and agricultural machinery, for purposes of lawful diagnosis and repair, or aftermarket personalization, modification, or other improvement ...by the lawful owner of the vehicle..." subject to the exceptions noted.

<sup>1753</sup> "Australian independent workshops want nothing more and nothing less than the same data that these same car companies share through mandatory schemes in Europe, Canada and the USA.": above n 1748. The AAA also assert that "Current Australian consumer law is not sufficiently protecting vehicle owners' rights. In many comparable international jurisdictions, the issue of vehicle data ownership is recognised and is protected through special provisions to ensure competition is maintained in this important market...":

<sup>1754</sup> Charity says: "The vehicle makers deny there is a problem. They tell government 'All the data is out there'. The truth is that only information the vehicle makers are prepared to share is made available." "Their offerings do not include critical diagnostic information that allows independent workshops to interpret fault codes, turn off the check engine light, to identify the correct blend of oil, to access a PIN code to reinstall a new component, and to download the latest software update for the car's computer system. Car companies also told government independent repairers want the data for free. This also is not true. Workshops are prepared to pay a fair commercial price, but they need all the data that dealers get.": AAAA, 'Make it Mandatory: Automotive Repair Code of Practice' *Press release* (29 June 2016 accessed 2 Jul 2016)

<<https://www.aaaa.com.au/policy-advocacy/make-it-mandatory-automotive-repair-code-of-practice/>>  
<sup>1755</sup> CAANZ, 'Sharing of Repair Information in the Automotive Industry' *Final Report* (27 Nov 2012 Accessed 30 Jun 2016)

<<http://www.aaaa.com.au/data/Final-report-on-sharing-of-repair-information-in-the-automotive-industry.pdf>>  
<sup>1756</sup> "The car industry has also been put on notice that it must take all necessary steps to make the required information available to the independent aftermarket over the next 12 months. If they don't, the Government will be forced to regulate.": AAAA, above n 401. Note that outgoing Senator Ricky Muir proposed an Automotive Repair Code of Practice, but was not re-elected.

*with cameras, radar and laser sensors all feeding data continuously to an on-board “black box” recorder, any mistakes by other car users will be used... against other motorists...<sup>1757</sup>*

As this suggests, CIOT data may be sought for or against consumers in criminal or civil proceedings, by way of manufacturer defence, or via discovery or subpoena. This issue is contractual insofar as the terms govern data ownership, custody and control as well as the provider’s right to respond to court orders, which means that CIOT data is potential ‘evidence’. Courts are also starting to hear applications for smart device data access or admissibility in both civil<sup>1758</sup> and criminal proceedings. Potentially probative evidence as to life, injury, location, accident causation, home occupancy, building security status, drug and energy consumption, utility data<sup>1759</sup> and so on, is discernible from CIOT data and factually useful. In 2016, Arkansas prosecutors sought smart meter data to evidence an accused’s water usage consistent with probable cause theory in a murder trial.<sup>1760</sup> Police also seized an Amazon Echo voice assistant and sought its server data by warrant.<sup>1761</sup> Amazon provided the accused’s device account details, enabling the Police to access on-device recordings, but resisted providing retained server recordings,<sup>1762</sup> though its terms entitled it to do so. There are obvious publicity concerns, as well as parallels with the US Apple iPhone cases: which range from prosecutor requests to access device contents such as contacts, through to requests to devise encryption-defeating software.<sup>1763</sup> There are also obvious parallels to surveillance: WikiLeaks’ recent ‘Vault 7’ dump shows that the CIA hacking methods include smart homes and cars:

---

<sup>1757</sup> Erik Coelingh, Senior Technical Leader at Volvo Cars cited pre-London and Guttenberg (Sweden) smart cars trials: Steve Connor, ‘First self-driving cars will be unmarked so that other drivers don’t try to bully them’ *The Guardian* (30 Oct 2016 accessed 30 Oct 2016) < [https://www.theguardian.com/technology/2016/oct/30/volvo-self-driving-car-autonomous?utm\\_source=esp&utm\\_medium=Email&utm\\_campaign=GU+Today+AUS+v1+-+AUS+morning+mail+callout&utm\\_term=197124&subid=19742650&CMP=ema\\_632](https://www.theguardian.com/technology/2016/oct/30/volvo-self-driving-car-autonomous?utm_source=esp&utm_medium=Email&utm_campaign=GU+Today+AUS+v1+-+AUS+morning+mail+callout&utm_term=197124&subid=19742650&CMP=ema_632)>

<sup>1758</sup> The authors cite an example of the Kilmore East Bushfire class action where the cause of a powerline failing was significant: *Matthews v AusNet Electricity Services Pty Ltd* [2014] VSC 663 at [75]. In future, IoT data may monitor and record fatigue events and record actions in response, which if accurate, are potentially significant in liability.

<sup>1759</sup> *Ibid.*

<sup>1760</sup> *Commonwealth v Risley*, Criminal Docket: CP-36-CR-0002937-2015 (Lancaster Cty., Pa., printed Nov. 16, 2015) The night of the murder, 140 gallons of water were used between 1 - 3 a.m. The victim was found dead in a hot tub. Prosecutors allege the water was used to wash away evidence of a bloody struggle, as the victim was allegedly strangled then drowned in the hot tub. The accused, James Bates is charged with first-degree murder, and tampering with physical evidence. If convicted of murder, he faces 10 - 40 years’ jail or life imprisonment.

<sup>1761</sup> Eric Ortiz, ‘Prosecutors Get Warrant for Amazon Echo Data in Arkansas Murder Case’ *NBC News* (28 Dec 2016 accessed 14 Jan 2017) <<http://www.nbcnews.com/tech/internet/prosecutors-get-warrant-amazon-echo-data-arkansas-murder-case-n700776>>

<sup>1762</sup> The prosecutors indicated that they may not pursue the server access, as they could access the device itself and this evidence formed part only of their case. It seems likely they were fishing for evidence- relying upon the window within which an ‘on’ device records background voices. Adam Roberts, ‘Bentonville warrant for Amazon Echo records in murder case gets privacy advocates’ attention’, *4029 News* (28 Dec 2016 accessed 14 Jan 2017) <<http://www.4029tv.com/article/bentonville-warrant-for-amazon-echo-records-in-murder-case-gets-privacy-advocates-attention/8539414>>; Yuna Lee, ‘Amazon challenges search warrant in Benton County murder case’ (22 Feb 2017 accessed 24 Feb 2-17) <<http://www.4029tv.com/article/amazon-responds-to-local-search-warrant-in-murder-case/8964554>>

<sup>1763</sup> *In Re Order requiring Apple, Inc. to assist in the execution of a search warrant issued by the court, Memorandum and Order*, U.S. District Court, Eastern District of New York (Brooklyn), 1:15-mc-1902 (JO), February 29, 2016 per Orenstein, J.

*All those new online devices are a treasure trove of data if you're a "person of interest" to the spy community. Once upon a time, spies had to place a bug in your chandelier ... With ...the "smart home," you'd be sending tagged, geolocated data that a spy agency can intercept in real time when you use the lighting app on your phone...*<sup>1764</sup>

In Australia, the collection of surveillance-related data is governed by legislation,<sup>1765</sup> but mandatorily-retained metadata is not accessible for use in civil proceedings.<sup>1766</sup> As to obtaining CIOT data for discovery or by subpoena, the question is essentially, who is in 'possession, custody, or control' of data, how it is retained and whether it may be identified and extracted without excessive cost, burden or contractual issues. That determination may once again, depend upon construction of the relevant contracts – but it seems likely, that the manufacturer will have any of custody, possession or control, so whether the data is accessible by the consumer directly or via subpoena from the manufacturer, its software provider or its cloud storage provider, the data is potentially available. As Basten JA stated:

'The ultimate justification for compulsory production and disclosure of information which might otherwise remain confidential, is the legitimate furtherance of judicial proceedings'.<sup>1767</sup>

Where data includes PI, the court may order disclosure but the recipient party cannot, without court leave, use it for any purpose until it is admitted into evidence.<sup>1768</sup> Courts will also assess privacy and confidentiality by weighing it against open justice; and making orders preventing publication or information disclosure if deemed necessary.<sup>1769</sup>

While Australian judges may be cautious,<sup>1770</sup> the CIOT may open people's homes, cars and bodies to even greater court scrutiny than ever before. That CIOT data is not always accurate and is potentially

---

<sup>1764</sup> Spencer Ackerman, 'CIA Chief: We'll Spy on you through Your Dishwasher' *WIRED* (15 Mar 2012 accessed 5 Jun 2016) <<https://www.wired.com/2012/03/petraeus-tv-remote/>>

<sup>1765</sup> This is beyond scope, but see the *Surveillance Devices Act 2004* (Cth) as to federal law enforcement agencies covertly using data, optical, listening and tracking surveillance devices. Note the Australian Security Intelligence Organisation (ASIO), the Australian Security Intelligence Service (ASIS) or the Defence Signals Directorate (DSD) are governed by the Australian Security Intelligence Organisation Act 1979 (Cth) and the Intelligence Services Act 2001 (Cth.) See also the *Telecommunications (Interception and Access) Act* (Cth) as to warrants required to intercept communications passing over a telecommunications system and also, the new mandatory data retention scheme which allows metadata access to 22 agencies, without a warrant.

<sup>1766</sup> Australian Government, 'Review of whether there should be exceptions to the prohibition on civil litigant access to retained telecommunications data' (Apr 2017 accessed 2 May 2017) <<https://www.ag.gov.au/Consultations/Documents/Access-to-telecommunications-data/Review-civil-litigant-access-to-retained-telecommunications-data.pdf>>

<sup>1767</sup> *Lowery v Insurance Australia Ltd* [2015] NSWCA 303, cited in Michael Legg & Claire Golding, 'How the Internet of Things will affect the future of litigation' *Law Society Journal* (November 2016 accessed 2 Dec 2016) <<http://www.law.unsw.edu.au/news/2016/11/how-internet-things-will-affect-future-litigation>>

<sup>1768</sup> *Hearne v Street* (2008) 235 CLR 125 at 154-162; [2008] HCA 36).

<sup>1769</sup> Legg, above n 1767. See, for example, *Court Suppression and Non-Publication Orders Act 2010* (NSW).

<sup>1770</sup> Technology is starting to impact court processes however; for example, in *McConnell Dowell Constructors (Aust) Pty Ltd v Santam Ltd & Ors* (No 1) [2016] VSC 723, predictive coding was accepted as an approach to discovery. It involves

malleable and hackable, suggests that prosecutors, civil litigants and courts should exercise caution before relying upon it. While potentially enabling contemporaneous, relevant information and disputes resolution using “objectively recorded data, rather than recollections or expert opinions”, it may also, open costly and time-consuming applications for discovery, disputes as to data-subject identity, validity, relevance and accuracy, as well as invasive privacy breach. But while consumers face cost and risk in this scenario, CIOT suppliers are unlikely to be adversely implicated, as most contracts (and the PA) contain a clause entitling them to respond to lawful court orders without liability to consumers. As such, the risk (or benefit) falls upon the consumer.

## 6.6 Recommendations

This chapter employs studies, behavioural economics concepts and case examples to examine why online CIOT contracting entails inherent ‘unfairness’ disempowering consumers, both by exacerbating extant online contracting problems and cumulatively, creating new ones. Contracts are unfair in form and content, employ ‘unfair’ BE factors collapsing choice and present ‘take-it-or-leave-it’ options, with little market pressure or incentive to improve. As Solove summarizes it, “severe cognitive problems” undermine online self-management conceptually, and structural problems such as unknown downstream data collectors/recipients and fused, reconstituted data over time, renders it “virtually impossible” for consumers to understand or exercise online contract self-management,<sup>1771</sup> or the reasonably expect the sorts of uses to which data is ultimately put. For these reasons, consumer detriments require regulatory action to incentivize industry behavioural change and increase consumer awareness. The approaches discussed here include clear ACL regulation as to meaningful ‘transparency’,<sup>1772</sup> privacy and data use limitations as defaults with (if any) voluntary opt-outs; choice of law reflecting a consumer’s location and essentially, contractual ‘fairness-by-default’. As previously recommended, this might be comprehended within an ACL ‘unfair’ commercial practices regime, provided sufficiently clear criteria are specified for court consideration. Further, best practice model contracts or clauses (such as those developed by the

---

software which is ‘trained’ to review discoverable documents, by an agreed protocol which learns from a human categorization of a sample document set as well as corrections overturning its decisions, until the parties agree it is sufficiently accurate. As judicial comfort levels increase, one might imagine greater alacrity to accepting CIOT-generated data may follow.

<sup>1771</sup> Solove, above n 1624.

<sup>1772</sup> This is not ‘transparency’ as contemplated under the ACL; rather it extends across multiple areas as to comprehension and comprehensibility: contract clarity, length, layout, simplicity, language use and reading skills requirements, technical features such as the provision of consumer-protective defaults with or without opt out facilities, and exploitation of BE factors, etc.

UK's ICO)<sup>1773</sup> can absolve users of liability and trust mark-style cues as to ACL, privacy and security compliance could be developed consultatively and overseen by regulators or CIOT-industry groups – both may reset online norms and enhance consumer confidence online. Neither of these proposals is mutually-exclusive and both enhance the other. Consumer data ownership also requires regulatory attention; to instil acceptable standards and impose consumer-friendly controls – for example, defaults preventing data use beyond that required for safety functionality (aka data minimisation) and granular opt-outs to clarify collection content, purpose and all possible uses.

## 6.7 Conclusion

**Part III** evidences that the CIOT raises significant actual and potential consumer detriment, through its structure, inextricable links with other emerging technologies and by its very scope, scale and stakes. As **Ch. 3** suggests, it is complex and insecure, neither of which favour consumer protection. As **Chs. 4** and **5** suggest, it will challenge existing weaknesses in consumer protection legislation, and expose new ones. As **Ch. 6** suggests, it will exacerbate online contracting woes, which in turn will compound consumer detriments as to rampant data optimisation, sharing and (mis)use. And as **chapter 1** suggests, it is that quantitatively and qualitatively different, that a comprehensive regulatory and industry response is required to promote consumer protection consistent with the ACPF. It is thus appropriate to move beyond Step 2 of the **Ch. 2** Framework, to resolve a policy position next.

---

<sup>1773</sup> These cover transfers of personal data and where used in entirety (even if in conjunction with other clauses which do not change their import) constitute sufficient safeguards as to as offering adequate safeguards as to Article 26(2) compliance: ICO, 'Model Contracts Clauses: International transfers of personal data (v. 1.0)' <[https://ico.org.uk/media/1571/model\\_contract\\_clauses\\_international\\_transfers\\_of\\_personal\\_data.pdf](https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf)>

## Part IV PROPOSAL FOR ACTION

---

### Chapter 7 Regulating CIOT: policy recommendation

*...Technology typically advances faster than policy, leaving a gap ... the IoT is advancing quicker than previous technological developments, this traditional gap is ... a chasm...<sup>1774</sup>*

*"There is a lack of urgency, and the rhetoric is very different to other key markets... there is no sense of crisis..."<sup>1775</sup>*

It is worthwhile briefly revisiting the argument holistically: the CIOT is developing rapidly, though consumer adoption, demand and penetration in Australia is, as yet, low. This will accelerate from late 2017, as consumer adoption of smart home devices increases through increasing baked-in 'smarts', smart self devices continue in popularity and formalised smart car testing presages the first consumer-driven 'smart-er' cars on Australian roads. Thousands of smart devices thus become millions, Australian-generated data collation and big data grows exponentially, algorithms and predictive analytics uses continue to explode - all to collate more minute-by-minute, high quality, granular, personal consumer information. Absent appropriate controls, that information may provide unprecedented insights into consumer's lives, thoughts, actions, habits and even intentions. While such insights offer great public benefit in some contexts, they also pose significant risks to consumer privacy, data security and autonomy. Technically, the CIOT ecosystem (devices->apps->cloud, etc.) is not sufficiently mature or secure to reliably protect personal data, which exposes consumers to data breach, identity fraud and theft. Data anonymisation is likewise a contestable concept, with many asserting that big data fusion, fuelled by voluntary social media and other disclosures, combined with involuntary online tracking and always-on CIOT information, creates an unprecedentedly granular consumer self-portrait and means at best, that anonymisation is temporary (time, technology and data dependent) or at worst, a fraud. Consequently, consumers face rampant collection, data abuse and privacy breach, as well as potentials for data-based discrimination, profiling and targeted marketing through applied algorithms and data analytics. At present, CIOT culture as revealed through contractual terms, is one of big data and little transparency, where principles of data minimisation and timely end-use destruction are neither evidenced or practised. Current regulatory reliance upon 'notice and choice' has failed; lengthy, impenetrably legalistic and (usually) unfair contracts function more as disclaimers than disclosure, and confound rather than facilitate, informed or implied consumer consent. Little wonder consumers ignore them. Indeed, even

---

<sup>1774</sup> President's NSTAC Report, above n 65.

<sup>1775</sup> Greg Austin, Australian Centre for Cyber Security, quoted in ComputerWorld ANZ, 'CyberThreat looms large: is Australia doing enough as to cybersecurity?' (July 2016 accessed 11 Jul 2016)  
<[http://docs.media.bitpipe.com/io\\_13x/io\\_132733/item\\_1376580/ANZ\\_ISM\\_0716\\_ezine\\_FINAL.pdf](http://docs.media.bitpipe.com/io_13x/io_132733/item_1376580/ANZ_ISM_0716_ezine_FINAL.pdf)>

where consent is sought in a reasonably open manner, consumers are opaquely warned of unexplained, designed-in 'lost functionality' if they decline data-sharing, and so the desire to use or download a product frames positive acceptance from the start. As this reveals, consumers suffer detriment across the CIOT environment, and despite (largely) principles-based, technology-neutral privacy and consumer legislation and traditional contract-law approaches, lack adequate protection from practices which regardless of ill-enforced or inapposite legal obligation, persist every day, right across the globe.

This **Part IV** proposes certain approaches to redress these issues, drawn from existing regulation, research and best practice. These are not 'solutions' per se, but nor are they 'in search of a problem'. Observably, few companies will select the more expensive, time-consuming or pro-consumer option where regulatory tolerance and legal gaps or uncertainties permit others which are cheaper and more commercially lucrative - which is what CIOT consumer regulation is presently allowing. This section commences by recapping the ACPF objective and problem identification, discusses various regulatory approaches and justifies the author's multi-faceted approach, which justifies the recommendations and principles in **chapter 8**.

## 7.1 STEPS 1 & 2: Revisiting Ch. 2 CIOT "problems"

The ACPF policy objective envisages improving consumer protection and empowerment to enable confident participation in fairly-trading markets, through six operational objectives.<sup>1776</sup> These are refined into four concepts accepted by this thesis:

- that consumer wellbeing<sup>1777</sup> (as opposed to economic exploitation) is a laudable social, political and economic policy objective, and is enhanced by empowered<sup>1778</sup> and educated control and choice, as well as regulatory protection (hard or soft law and/ or other protective mechanisms);
- that effective competition is good for markets and produces desirable consumer outcomes;<sup>1779</sup>
- that consumers have the right to be confident within the marketplace; and
- finally, that fairness is a desirable marketplace objective.

---

<sup>1776</sup> Recital C, Intergovernmental Agreement, above n 501.

<sup>1777</sup> The EC assert that "consumer protection is at the heart of well-functioning markets":

<sup>1778</sup> Above n 501.

<sup>1779</sup> The 2008 Australian Productivity Commission Review found that educated and informed consumers are a best defence against predatorial firms, as well as create effective demand for competitive and innovative markets: above n 498.

Six identified consumer IOT ‘problems’ were examined in **Part III**, exhibiting a range of possible sources first identified in **Ch. 2**:

Problem	Possible source(s)	Agency & chapter
<b>Complexity: Consumers confused by product and industry complexity</b>	Business conduct (design issues) Informational failure (complexity and cognitive overload) Consumer behaviour (heuristics, overconfidence, framing) Regulatory failure (low consumer education or proactive enforcement)	ACCC (limited) <b>Ch. 1</b>
<b>Security: Consumers confused by complex product security – is it secure or how to make it secure?</b>	Business conduct (design issues) Business conduct (framing) Informational failure (complexity and volume) Consumer behaviour (heuristics, overconfidence, framing, defaults) Regulatory failure (low consumer education; legal gaps; low enforcement)	ACCC (limited) <b>Ch. 3</b>
<b>Performance &amp; safety: Suppliers or products do not fulfil their promises or meet consumer expectation</b>	Business conduct (fraudulent sale deceptive sales; unfair contract terms, unconscionability; competitive issues) Consumer behaviour (overconfidence, framing) Regulatory failure (low enforcement, international supply chains) Consumer behaviour (heuristics, overconfidence, framing)	ACCC <b>Ch. 4</b>
<b>Privacy: Consumers confused by complex product data flows and privacy – who has it, is data private or how to make it so?</b>	Business conduct (informational issues) Informational failure (complexity and volume) Consumer behaviour (heuristics, overconfidence, framing)	OAIC <b>Ch. 5</b>
<b>Consent: Consumers do not understand product ‘legals’ (terms and conditions, instructions, privacy and software terms)</b>	Business conduct (misleading/unfair terms; exploitation of ‘consent’) Business conduct Informational failure (complexity and overload) Regulatory failure (complexity, length & access may make terms unfair or beyond consumer competence to understand; inadequate enforcement)	OAIC ACCC <b>Ch. 6</b>
<b>Data analytics &amp; discrimination: Consumers unaware that data is stored and may be</b>	Business conduct (informational and disclosure issues) Business conduct (security and anonymisation failures)	ACCC, OAIC, & Anti-discrimination Commissioner

used by others or how it is used	Regulatory failure (low consumer education or proactive enforcement) Consumer behaviour (heuristics, overconfidence, framing)	(all limited) <b>Ch.3</b> (briefly)
----------------------------------	--	--

Table 7.1 Problem definition & source  
Source: author

**Chapters 1, and 3 to 6** demonstrated various forms of actual and potential consumer detriment, whether personal or structural, apparent or hidden, financial and non-financial, as well as identified regulatory ‘gaps’ in Australian consumer, privacy and contract law. For the purposes of this thesis, and based upon **Chs. 3- 6**, it is assumed that these detriments are sufficiently serious to justify policy action under Step 3 of the ACPF.<sup>1780</sup>

The next steps are therefore evaluated below.

## 7.2 STEP 4: Set policy objectives and identify the range of policy actions

Based upon the ACPF objective, there are multiple possible interventions, ranging from consumer empowerment (demand-side) to improving information quality, type and availability, to modifying poor business practices (supply-side) to incentivizing industry self-regulation to mandate better practice or protect against those which entail consumer detriment. Policy options thus include no action, soft law, hard law and ‘alliance’.

A regulatory impact statement approach<sup>1781</sup> to deal with the identified problems suggests four options:<sup>1782</sup>

<sup>1780</sup> This is of course, an evaluative and partly subjective exercise, and possibly one requiring extensive economic analysis to justify itself. Further, a cautious approach might require evidence of real detriment within the Australian market (or at least consumer submissions to that effect), before committing to substantive policy action (other than encouraging industry-driven self-regulation). This paper however, takes a more pre-emptive approach having regard to the nature of the technology in question, its rapid evolution, intertwined nature and its significant potential and long-lasting consumer impacts. By analogy, the amendments expanding the unfair terms jurisdiction to include small business, did not overly rely upon either of these approaches.

<sup>1781</sup> The model for this approach was the consideration of section 23 ACL here:  
<[http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5497\\_ems\\_b35077f3-dbb6-4c5a-81b0-7b885634fd81/upload\\_pdf/503040.pdf;fileType=application%2Fpdf](http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5497_ems_b35077f3-dbb6-4c5a-81b0-7b885634fd81/upload_pdf/503040.pdf;fileType=application%2Fpdf)>

<sup>1782</sup> The inspiration for this appraisal came from this report Table 0.1, but uses the author’s content: EC, above n 52.

- Option 1: **No action: “the status quo”**. Consistent with *permissive innovation*<sup>1783</sup> as the “optimal policy default”,<sup>1784</sup> no action is taken until a compelling case of serious harm can be evidenced, so that CIOT innovation may proceed unimpeded and its problems dealt with “later” - aftermarket failure or other problems have demonstrably emerged.<sup>1785</sup> In the meantime, court cases may resolve instances of detriment.
- Option 2: **Soft Law: Light-touch with non-regulatory responses**. This presumes some industry actions which may or may not be binding, or cover all CIOT-industry participants. Those actions may include self-regulatory, voluntary codes and where incentivized, could include standardised contractual terms<sup>1786</sup>- using simple language, which are fair and balanced, flexible and adaptable and ISO compliant - to standardise privacy, data ownership and other practices. Meanwhile, regulators continue to monitor, subject to industry negotiation if problems arise
- Option 3: **Hard Law: Legislation** that is CIOT-specific and/ or amendments to existing legislation to capture CIOT concerns. This has high-level efficacy, provided compliance incentives are adequate; for example, that enforcement is funded and pursued. It may entail some negative externalities<sup>1787</sup> requiring legal refinement to manage its efficiency and impacts, and to ensure it does not impede CIOT innovation and implementation.
- Option 4: **Alliance: Combined legal approaches** including a mix of industry-initiated codes and a range of policy-led initiatives, as well as some hard law in the form of generic principles-based legislation or specific rule-based gap-filling as required. Legislative amendment may extend or improve consumer privacy, security and consumer law rights to better address CIOT detriments, together with incentivising complementary industry actions, including Codes of Practice, improved disclosure, improved data management

---

<sup>1783</sup> Thierer, above n 161. (Permissionless Innovation) The essential premise is that innovation requires that the market be allowed to shape and develop technology until any material damage occurs.

<sup>1784</sup> Ibid (Testimony).

<sup>1785</sup> Adam Thierer, ‘The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation’ *Mercatus Center* (19 Nov 2014 accessed 3 Mar 2016) <<http://mercatus.org/publication/internet-things-and-wearable-technology-addressing-privacy-and-security-concerns-without>> 21 *Rich. J.L. & Tech.* 6 (2015), <http://jolt.richmond.edu/v2li2/article6.pdf>

<sup>1786</sup> See for example the SLALOM terms devised by the EC in relation to cloud contracting. The Service Level Agreement and open model seeks to devise standardised ‘ready to use’ terms and SLAs to “a baseline of fair, transparent and understandable templates and guidelines aimed at increasing the uptake of cloud services and making it easier for customers to migrate efficiently to the cloud”: Mason, Hayes and Curran, ‘Can SLALOM Transform Cloud Computing Contracts and SLAs?’ *Tech law blog* (15 Sept 2016 accessed 16 Sept 2016) <<http://www.mhc.ie/latest/blog/tech-can-slamon-transform-cloud-computing-contracts-and-slas>>

<sup>1787</sup> A ‘negative externality’ is a cost that is suffered by a third party (for example a consumer) as a result of an economic transaction: [www.economicsonline.co.uk/Market\\_failures/Externalities.html](http://www.economicsonline.co.uk/Market_failures/Externalities.html)

transparency, etc., as well as generating improved and ongoing consumer education and information from both regulator and regulated. This approach engages bottom-up localised power with top-down regulatory power to locate the most targeted and efficient outcomes. Market players retain freedom to the extent they are prepared to take mandatory code-based responsibility, shaped by government policy and consumer protection objectives. Further, negative externalities are often more readily industry-identified, so an alliance between regulators, industry and consumers may be highly effective and responsive.

Present structures suggest that principle-based regulation supplemented by industry Codes and standards is the preferred consumer-protection approach in Australia, but there are also 'bright line' and complex or detailed 'rule-based' approaches<sup>1788</sup> in both the ACL and PA. As the ALRC found in 2008, best practice suggests that principle-based regulation alone does not address circumstances where more specific rules may respond better to different industry or policy considerations. Further, principles-based frameworks can also adopt differing degrees of rule-based prescription and detail within high-level principles, while industry involvement may improve efficacy and help to create a regulatory model which addresses the problem at least cost to "business and the community".<sup>1789</sup>

Step 5 undertakes that evaluation.

### 7.3 STEP 5: Evaluate Options & set a policy action

**Option one** reflected the federal government approach at the commencement of 2016, and remains as to smart self and home devices. Smart car on-road trials have undergone the extensive NTC review process, resulting in *Guidelines* as a "first step" designed to provide industry "clarity".<sup>1790</sup> Perhaps

---

<sup>1788</sup> J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 10; Black illustrates each: 'An organisation must not collect personal information relating to an individual's sexuality' ('Bright line'); 'An organisation must not collect personal information unless it is necessary for one of its functions or activities' ('principle'); 'An organisation [defined] must not collect [defined] PI [defined] unless all of the following conditions are met: [list of conditions]...' ('Complex/detailed rule').

<sup>1789</sup> Victorian Government, *Victorian Government Guide to Regulation* (2011 updated Jul 2014 accessed 20 Apr 2016) *Dept of Treasury and Finance* < <http://www.dtf.vic.gov.au/Publications/Victoria-Economy-publications/Victorian-guide-to-regulation>>

<sup>1790</sup> NTC, 'Guidelines for Trials of Automated Vehicles in Australia' (April 2017 accessed 20 Apr 2017): *Foreword* <<https://www.ntc.gov.au/current-projects/automated-vehicle-trial-guidelines/>> Note that the Guidelines are an overview; for example, they require a safety management plan to be submitted with trial applications (to state regulators) and cite broad headings, without specifics. "Security" for example requires safety criteria as to "security" which includes vehicle hacking and personal information access, without specifying more. In response, manufacturers will presumably refer to the usual vehicle

reflecting high difficulty, risk and few simple solutions, the enquiry has deferred addressing the smart car consumer-problem(s) identified here.<sup>1791</sup> However **Part III** clearly reveals that current regulation does not adequately protect consumers against CIOT detriments, while there are significant incentives for providers to exploit that situation, such as optimising big data collation, use and sale.

**Option two** is favoured by industry based upon current Reports.<sup>1792</sup> While yet to attract public debate,<sup>1793</sup> industry-led self-regulatory risk management and compliance guidelines are usually preferred over hard law regulatory responses, absent evidence of market failures or inhibited industry development requiring legislative solution.<sup>1794</sup> The Australian IOT Alliance for example, is currently providing non-binding top-level Guidelines, which are not (yet) consumer-focussed.<sup>1795</sup> This approach is a valuable complementary step but alone, given the likely diversity of CIOT industry players, is unlikely (at least initially) to prevent ongoing consumer detriment, especially where compliance is voluntary. This is not expected to adequately or systematically address the identified problems nor overcome consumer detriments, without greater industry compliance incentives.

**Option three** is usually opposed by industry groups for its inflexibility and the possibility of stifling CIOT innovation. More generally, concerns to remove rather than strengthen industry barriers are also important, as well as promoting international competitiveness on a level-playing field. Arguably, hard law alone will not systematically address CIOT problems for Australian consumers and could impose additional compliance costs which impede industry competitiveness. Given the nascent state of the technology and any Australian CIOT industry, legislation without substantial industry buy-in may be counterproductive to future industry development and prosperity. This approach alone may fail to strike an appropriate balance between industry development, innovation, and consumer interests and risk. It is thus probable that Option four provides a more flexible and holistic approach to addressing CIOT issues at this stage, while preserving and promoting consumer rights and protections in an Australian context and encouraging Australian businesses and consumers to take reasonable steps to protect their own interests in an CIOT context.

---

systems as mitigation – and it seems unlikely state authorities will criticise those: Ibid: 10. Note that hacking could pose a risk to other road users however, so should be seriously addressed especially if vehicles are unmanned.

<sup>1791</sup> Ibid.

<sup>1792</sup> Australian IOT Alliance and Communications Alliance, for example.

<sup>1793</sup> The Australian IOT Alliance (IOTAA) website appears here: [www.aiota.com.au](http://www.aiota.com.au) While it is a well-organised and resourced group, it is predominantly big-player, industry- led. The author's involvement however suggests the group is very open to all viewpoints and will broaden with time and traction. It is presently developing Guidelines which are an advisory form of non-binding recommendation – as such they are very general and have attracted little media interest to date.

<sup>1794</sup> See the observations and recommendations in Communications Alliance, above n 119.

<sup>1795</sup> Peter Gutierrez, 'IoTAA releases IoT security guidelines' *IoT Hub* (28 Feb 2017 accessed 4 Mar 2017) <<https://www.iothub.com.au/news/iotaa-releases-iot-security-guidelines-452893>>

**Option four** is the preferred option. Based upon evidence-based research, consumer surveys, international cases and ACPF analysis, demonstrable consumer detriment from CIOT is either occurring or likely to occur, at least until CIOT industry maturation. It is therefore recommended that existing legal protections as to privacy, security and consumer protection are strengthened to, for example, address critical privacy and security detriments by design and default. This approach alone is expected to substantially promote best practice risk management processes, significantly reducing avoidable security flaws, and reducing the incentive for misleading or unfair terms, and excessive data collection or use. **Chapters 3-6** recommend certain ACL and PA amendments to codify certain high risk elements within CIOT manufacture, sales and consumer use, together with complementary soft regulatory approaches. These should better achieve an appropriate balance between protecting those consumers who wish to protect their data and self-autonomy in the CIOT world, but who may lack sufficient information, resources or bargaining power, while reinstating contractual transparency and certainty, and encouraging businesses to better justify consumer trust. These recommendations are detailed in **chapter eight**.

Smart cars provide an interesting current example.<sup>1796</sup> The Auto Alliance non-binding principles weakly address consumer smart car privacy and security issues<sup>1797</sup> [option two]. International governments are anxious to facilitate on-road testing: the UK has a non-mandatory Code [option two],<sup>1798</sup> the US has a federal bill,<sup>1799</sup> some US states<sup>1800</sup> and South Australia<sup>1801</sup> enacted legislation [Option three],<sup>1802</sup> while

---

<sup>1796</sup> Internationally in March 2016, the United Nations Economic Commission for Europe (UNECE) revised the Vienna Convention on Road Traffic (1968), to allow automated driving systems on roads, providing that they meet UN vehicle regulations or a driver can control or disable the system: Lennart S. Lutz, 'Automated Vehicles in the EU: A Look at Regulations and Amendments' *GenRe Publications* (Mar 2016 accessed 5 Apr 2016) <<http://www.genre.com/knowledge/publications/cmint16-1-en.html>>

<sup>1797</sup> Auto Alliance, above n 399.

<sup>1798</sup> Minister for Roads and Road Safety, 'Victoria Leading the Way on Autonomous Vehicle Trials' *Press release* (15 Dec 2016 accessed 18 Jan 2017) <<http://www.premier.vic.gov.au/victoria-leading-the-way-on-autonomous-vehicle-trials/>>

<sup>1799</sup> The federal Autonomous Vehicle Privacy Protection Act of 2015 (HR3876) has stalled: H.R. 3876 — 114th Congress: Autonomous Vehicle Privacy Protection Act of 2015. (2015) <https://www.govtrack.us/congress/bills/114/hr3876> Note it principally concerned governmental readiness.

<sup>1800</sup> As to the states in mid 2016: (approx.) 5 have enacted legislation, 13 bills have failed and 13 states have bills under consideration: Gabriel Weiner and Bryant Walker Smith, 'Automated Driving: Legislative and Regulatory Action' (n.d. accessed 10 Nov 2016) <[cyberlaw.stanford.edu/wiki/index.php/Automated\\_Driving:Legislative\\_and\\_Regulatory\\_Action](http://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:Legislative_and_Regulatory_Action)> Pittsburgh currently has a large Uber test fleet on road without any regulation at all, which has seen journalists supervising in the 'engineer's' seat.

<sup>1801</sup> *Motor Vehicles (Trials of Automotive Technologies) Amendment Act 2015* (SA). This exempts autonomous vehicle tests from certain laws, enabling public road testing. To some extent the unilateral SA action reflects pressure from industry and the state's threatened automotive base: local suppliers had already conducted testing with Volvo, Tesla and Bosch which rather forced a proactive response.

<sup>1802</sup> Belle-Isle, above n 716.

the NHTSA has two criticised<sup>1803</sup> non-binding preliminary statements<sup>1804</sup> [option two] and late in 2016, issued its federal policy<sup>1805</sup> which unusually, is both in force *and* open for public comment:

...the speed with which HAVs are advancing, combined with the complexity and novelty of those innovations, threatens to outpace ... conventional regulatory processes and capabilities...<sup>1806</sup>

The NTC exhibited similar hesitancy:<sup>1807</sup> adopting open-ended guidelines [option two], but stalling on other issues, opting to avoid and defer:<sup>1808</sup>

... Additional issues should continue to be monitored by governments as the technology develops. These include potentially increased safety risks related to vehicle modification, maintenance and repair, resolving complex liability scenarios, privacy protection and access to data to determine fault and civil liability.<sup>1809</sup>

---

<sup>1803</sup> Former NHTSA head Joan Claybrook extensively criticised these as a secretive “kumbaya” between a regulatory agency and an “industry seeking to avoid regulation”. She contends the Principles abrogate regulatory responsibility, victim-blame drivers for accidents and ignore that regulatory actions (over collaboration) and imposed standards are precisely why “NHTSA estimates that over 600,000 deaths have been prevented by such safety rules since the 1960s.”: Belle Isle, above n 709.

<sup>1804</sup> NHTSA, ‘Preliminary Statement of Policy concerning Automated vehicles’ (2013) <<http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development>>; NHTSA, ‘Policy Statement Concerning Automated vehicles’ (2016 update accessed 2 Jul 2016) <http://www.nhtsa.gov/About+NHTSA/Press+Releases/dot-initiatives-accelerating-vehicle-safety-innovations-01142016>; NHTSA, ‘Policy update to NHTSA, ‘Preliminary Statement of Policy concerning Automated Vehicles’ (2016 accessed 2 Aug 2016) < <http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Autonomous-Vehicles-Policy-Update-2016.pdf>>

<sup>1805</sup> NHTSA, above n 327 & Fact Sheet: <[https://www.transportation.gov/sites/dot.gov/files/docs/DOT\\_AV\\_Policy.pdf](https://www.transportation.gov/sites/dot.gov/files/docs/DOT_AV_Policy.pdf)>

<sup>1806</sup> NHTSA, above n 327.

<sup>1807</sup> NTC, above n 397: 98- 100 (Discussion Paper). The NTC found over 716 legislative barriers, especially as to the human ‘driver’ liability and determining ‘control’. The Vienna Convention on Road Traffic expresses the guiding principle that human drivers exercising human judgement are responsible to drive a motor vehicle. Australia is not a signatory but the Australian Road Rules provide that “a driver must not drive... unless the driver has proper control of the vehicle”: Regulation 297 (1) Australian Road Rules (Accessed 2 Jul 2016) <[http://www.austlii.edu.au/au/legis/sa/consol\\_reg/arr210/s297.html](http://www.austlii.edu.au/au/legis/sa/consol_reg/arr210/s297.html)> Reg 297(2) prohibits driving unless the driver has “a clear view of the road, and traffic, ahead, behind and to each side of the driver.”

<sup>1808</sup> While asserting “Australia should aim for a high level of privacy protection for drivers and occupants” they fail to appraise current systems or consider research, shelving the issue for ‘later’: NTC, above n 397: 107 (Discussion Paper) and above n 1742: 17 (Policy Paper). While pressing ‘on-road’ issues may have justified not resolving a clear policy position as to privacy, data collection/ use and third party access and liability scenarios, it remains concerning the NTC did not look more resolutely at these issues. It did suggest that no ‘different’ privacy issues arise, but they failed to evidence their conclusion and seemed to hide behind future ‘unknowns’ rather than identifying the many ‘knowns’ – such as current practices for example. Note that the C-ITS Platform Final Report (Brussels, 2016) WG4 found that C-ITS data is ‘personal data’ (as VIN access indirectly leads to driver identity) but query if the PA would include it: EC, ‘C-ITS Platform Final Report’ (Jan 2016 accessed 20 Dec 2016) <https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf> While raised, the NTC reports do not revisit this issue: NTC, above n 397: 109, deferring to an Austroads privacy impact assessment anticipated mid-2016. They also contradict themselves in finding a ‘legislative gap’ requiring regulation insofar as certain ‘enforcement agencies’ are not bound by the Privacy Act - but “later”. For the record, the ACCC and OAIC did not make a submission, nor is there any evidence that a legal analysis was conducted to assess privacy and surveillance law efficacy in a smart car context. In discussion with the author, Natasha Bolsin, Policy Adviser on 22 November 2016 mentioned that a lack of submissions on these topics is perhaps reflected in the report. This issue is not to be construed as criticism of the enquiry, which was well-conducted- but it is difficult not to suspect that avoiding the issue was the easiest option given testing protocols were the priority.

<sup>1809</sup> NTC, above n 1742.

Deferral and soft law approaches may reflect industry power or credibility,<sup>1810</sup> but may also abrogate regulatory responsibility. As former NHTSA Head Claybrook puts it,<sup>1811</sup> hard law and enforcement are precisely why “...over 600,000 [US crash] deaths have been prevented... since the 1960s.”<sup>1812</sup> Her view seems supported by an unprecedented spate of global recalls,<sup>1813</sup> record US industry fines<sup>1814</sup> and multiple safety scandals of recent years.<sup>1815</sup> As such, sound regulation in a smart context where the stakes are high, may well require a mix of approaches.

To summarize, **Option one** does not address the detriments and regulatory gaps identified; as such it is not sufficient to address the CIOT as is. **Option two** has significant potential to address some issues but depends upon industry preparedness to embrace its own flaws (or those of its worst elements) and to take positive steps to address those flaws. The option does not address those industry participants who choose not to adopt or to comply with Codes, nor that industry has, to date, not proposed such solutions for CIOT problems. Industry preference as to smart cars suggests that voluntary codes are preferred, though may entail a lower bar than relevant hard law and entail weak enforceability. **Option three** offers the most rigorous methodology to impose legal clarity and to enforce industry compliance, provided hard laws are rigorously monitored and enforced. **Option four** offers the broadest and most holistic approach, but also the most flexible. It meets the objective to establish clear legal guidance whilst avoiding unnecessary prescription, and preserves flexibility to accommodate rapidly evolving and dynamic technology, as well as new business models.<sup>1816</sup> The most serious problems and gaps can be redressed through hard law, general principles-based compliance can be assisted through industry codes which emphasize and explicate the law practically to create an industry culture of compliance, and future or emerging consumer detriments can be swiftly addressed through industry actions influenced by

---

<sup>1810</sup> Note in Australia the car industry and government have long had a close and trusting relationship which the author believes has been effective for all parties, including consumers. Recent international industry behaviours are less reassuring: Brent Snavely, ‘Auto industry thrives despite scandals’ USA TODAY (25 Jul 2016 accessed 5 Aug 2016) <<http://www.usatoday.com/story/money/cars/2016/07/25/auto-industry-thrives-despite-scandals/87517968/>>

<sup>1811</sup> (US) DOT, above n 716.

<sup>1812</sup> Belle-Isle, above n 716.

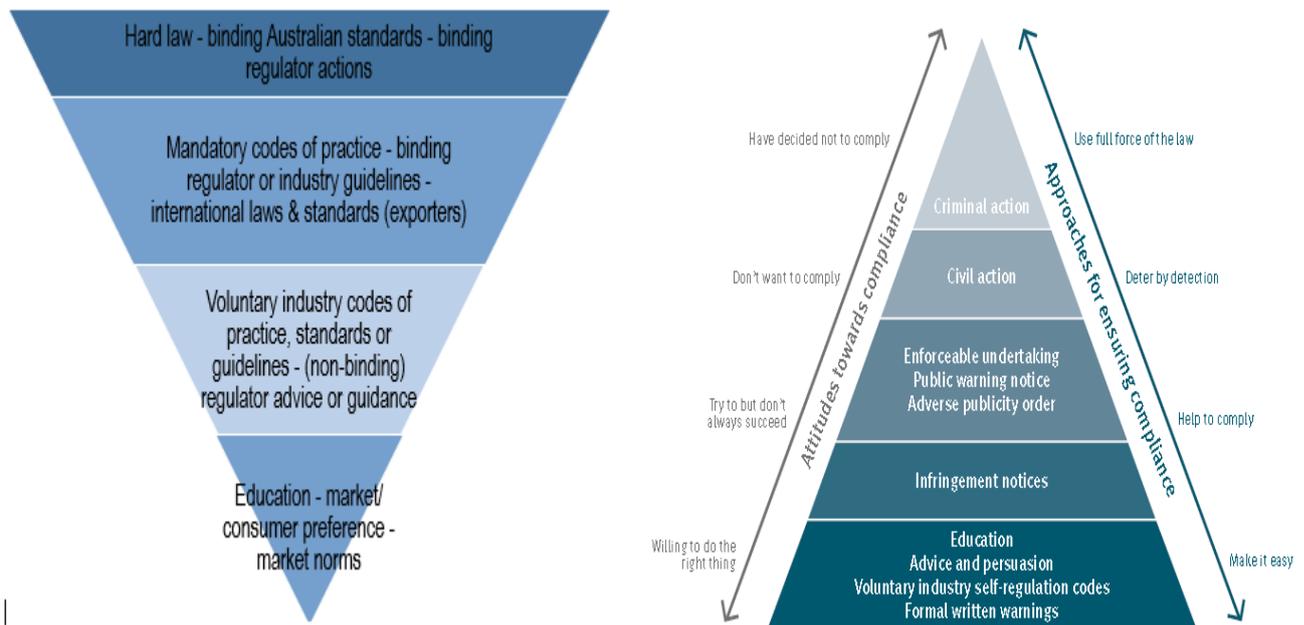
<sup>1813</sup> For example, the Takata air bag recall is the largest in US history and affecting 32 million vehicles across 33 brands. The defect has caused more than 100 injuries and at least ten fatalities, yet industry vehicle sales are at record levels: Snavely, above n 1809. In early 2017, there is some suggestion that Takata may file for bankruptcy.

<sup>1814</sup> For example, in 2014 Toyota Motor Sales paid \$1.2 billion fine to avoid criminal prosecution and admitted in the settlement to misleading consumers through “deceptive statements”. GM has also paid \$900 million fine to settle federal criminal charges as to faulty Chevrolet ignition switches, which killed at least 124 people. GM admitted to knowing of the problem for over a decade in congressional hearings: Doron Levin, ‘Here are some of the worst car scandals in history’ *Fortune* (26 Sept 2015 accessed 2 Jan 2016) <<http://fortune.com/2015/09/26/auto-industry-scandals/>>

<sup>1815</sup> ACCC, above n 939. For global actions, see Boston, above n 932.

<sup>1816</sup> These objectives emerged from the FTC, ‘Mobile Privacy Disclosures: Building Trust Through Transparency: A Federal Trade Commission *Staff Report*’ (Feb 2013 accessed 17 Mar 2016): 13- 14 <<https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf>>

government policy, incentivized (where necessary) by threatened regulation. As such, the latter model best responds to the broad problems identified and those which may emerge, and guards consumer interests proactively, so is (arguably) at least cost to the community overall. The author depicts this below, showing that as regulatory power increases, compliance should do likewise.<sup>1817</sup> The ACCC's regulatory tools graphic reflects alliance-style policy: the strongest (and most expensive) methods cover the smallest footprint and are reserved for those with the weakest compliance attitudes and observance.



Graphics 7.1 Alliance approach & 7.2 ACCC Compliance and Enforcement  
 Source: Author & ACCC respectively<sup>1818</sup>

<sup>1817</sup> This view should be distinguished from that of “responsive regulation” advocates in this recent Australian article: M. Richardson, R. Bosua. K. Clark, J. Webb, A. Ahmad, & S. Maynard, ‘Towards responsive regulation of the Internet of Things: Australian perspectives’, *Internet Policy Review* (2017) 6:1 <DOI: 10.14763/2017.1.455> That model views regulation (ideally) as a minimal but effective (if necessary, escalating) market intervention and proposes a ‘participatory solution’ over one that is ‘repressive’ (i.e., top-down and coercive) or ‘autonomous’ (i.e. based upon laissez faire legal approaches such as the common law doctrines). Their IOT regulation solution proposes privacy by design as the base of a pyramid, with consumer and data protection standards in the middle and privacy-based doctrines on top. That the OAIC sees privacy by design as within APP1 (albeit more implied than explicit) suggests that the authors may be understating its relevance already. Compliance-driven (ISO 9001) companies employ many elements of it in their business practices now.

<sup>1818</sup> ACCC, ‘Compliance and Enforcement policy’ (Jan 2017 accessed 2 Feb 2017) <<https://www.accc.gov.au/about-us/australian-competition-consumer-commission/compliance-enforcement-policy>>

## 7.4 Conclusion

Having regard to dual CIOT imperatives of industry innovation and consumer protection, as well as the seriousness of consumer detriments identified, the regulatory gaps found and the need for flexibility to adapt to future product and industry developments, this paper concludes that an **alliance regulatory approach** is the most flexible, responsive, adaptable and open to stakeholder inputs – all of which promote industry acceptability and compliance, as well as responsiveness to evolving consumer issues and flexibility to meet challenges ahead. That approach forms the basis for the recommendations in **chapter eight**.

## Chapter 8: Recommendations and draft principles

*“...the culture, standards and policy structures that have been applied to big data analytics may need to move out of the back room and into the showroom if community confidence and wide opportunity for innovation are to be maximised...”<sup>1819</sup>*

*“Trust is the foundation of the IOT and that needs to be underpinned by security and privacy. And it’s a conversation we all need to start having now ...”<sup>1820</sup>*

*“With consumer concerns comes the very real prospect of regulatory intervention...”<sup>1821</sup>*

This final chapter locates an ambitious mix of self-regulatory and regulatory approaches to address the problems identified in the ACPF analysis. It then sets out **eight draft principles**, which capture simple, best practice approaches to a “human-centred”<sup>1822</sup> consumer-respectful internet of things, at least as to smart cars, home and self. Indeed, should all else founder upon government, industry, pro-innovation, anti-regulation, money, power, uncertainty - or other resistance - these principles express the baseline fundamentals, to start afresh.

### 8.1 Intended application

*Don’t start with the technology, start with the audience...”<sup>1823</sup>*

*Innovation is not always about technology. It can be about changing people’s behaviour. It’s not always about making things smaller or faster...”<sup>1824</sup>*

The recommendations proposed employ a range of targeted complementary mechanisms using industry, regulator and consumer inputs. Their purpose is to establish a clear, comprehensive, cooperative framework to set industry laws, standards and practices as norms early in CIOT development – before rusted-on (mis)behaviours are entrenched - to create an ethical compact justifying industry confidence and consumer trust. They are also aimed to ensure some degree of conceptual parity between Australian and EU CIOT approaches, reflecting Australian Standards harmonisation<sup>1825</sup> and the clear international

---

<sup>1819</sup> Productivity Commission Chair cited by Timothy Pilgrim, above n 1406.

<sup>1820</sup> Samani above n 553.

<sup>1821</sup> IAB (US), ‘Privacy and Tracking in a Post CookieWorld’ *White Paper* (Jan 2014 accessed 9 Apr 2015) [7]

<[http://www.iabaaustralia.com.au/uploads/uploads/2014-11/1415289600\\_3ee3de01b67c04945704bce1e7964095.pdf](http://www.iabaaustralia.com.au/uploads/uploads/2014-11/1415289600_3ee3de01b67c04945704bce1e7964095.pdf)>

<sup>1822</sup> EC, above n 93.

<sup>1823</sup> Ken Shillinglaw, controller BBC2 and BBC4 cited in Accenture, above n 24: 45.

<sup>1824</sup> Dean Takahashi, ‘The Internet of Things: A Toaster That Can Tell You the Weather And A Lung Cancer Sniffer’ VB (26 Oct 2016 accessed 28 Oct 2016) <http://venturebeat.com/2016/10/26/the-internet-of-things-a-toaster-that-can-tell-you-the-weather-and-a-lung-cancer-sniffer/> quoting ARM chief technology officer Mike Muller {ARM set up wearables for good}.

<sup>1825</sup> Leading harmonisation bodies are the International Standardization Organization (ISO), the International Telecommunication Union (ITU) and the International Electrotechnical Commission (IEC). Approximately 80% of Australian Standards are aligned with international standards and Standards Australia (SA) and government have agreed via MOU that

role of the EU in shaping the IOT, especially as to privacy and data processing.<sup>1826</sup> That approach must inevitably evolve over time with increasing industry sophistication, capability and consumer knowledge, so requires a mix of coercive and flexible responses. To that end, ongoing industry, consumer, regulator and other stakeholder involvement is imperative.

While the position as to the broader IOT is distinguished,<sup>1827</sup> these consumer IOT proposals address extant online 'on-air' issues, as well as CIOT-specific or CIOT-exacerbated issues. As such, they may also have application beyond smart cars, self and homes, depending upon context.

## 8.2 Recommendations

Specific recommendations are detailed in the conclusions to **Chs. 4-6**. Those of most import appear here; note that some are complementary while others have elements of duplication or even, inconsistency. Reliant upon the impossibility of all (if not any) being implemented, these proposals are inclusive.

### Legislation

#### 8.2.1 Australian Consumer Law (ACL)

Amend the ACL to address the proposals identified in **Ch 4 Table 4.2**, including:

- (a) insert a general prohibition upon unfair business practices (which could include as 'relevant matters' for consideration, data use and contractual transparency, further defined by Guideline);

---

this percentage be maximised, with any exceptions "well justified". Note the MOU (1988) includes that no Australian standard will developed where an acceptable international standard exists, nor will an SA contravene World Trade Organization requirements or be used as non-tariff free trade barriers: Standards Australia, 'Submission to Standing Committee on Economics, Finance and Public Administration, Inquiry into the state of Australia's manufacturing industry now and beyond the resources boom (2006).

<sup>1826</sup> Warwick Ashford, 'EU data protection rules affect everyone, say legal experts' *ComputerWeekly* (11 Jan 2016 accessed 18 Jul 2016) <<http://www.computerweekly.com/news/4500270456/EU-data-protection-rules-affect-everyone-say-legal-experts>>

<sup>1827</sup> Large industrial IOT industry is capable of setting specifications, mandating standards compliance and insurance, and imposing other protective mechanisms with CIOT- suppliers contractually. It is questionable whether the industrial CIOT is less likely to generate direct consumer harms, with its focus upon industry because of course, the industrial CIOT (partly) presupposes production of goods which consumers may use. By analogy, the view is often expressed that had this carefully considered process occurred earlier in the development of the internet, many of its extant and potentially insurmountable security and privacy issues – which now imperil national security, and enable the world's greatest criminal and illegal surveillance activity - might have been at least, ameliorated. From a consumer perspective, that focus might have earlier fallen upon other internet 'issues' such as online behavioural advertising and online tracking, which remain substantially unregulated in Australia, and which the author has argued elsewhere, are despite some positive but belated EU regulation and US industry efforts, somewhat out of control internationally.

- (b) insert a general ‘safety’ provision (including as ‘relevant matters’ for consideration, ‘privacy’ and ‘security’);<sup>1828</sup>
- (c) expand section 29 to prohibit false representations as to goods’ safety, privacy, security or related data collection and use practices;<sup>1829</sup>
- (d) amend section 58 to insert an ongoing obligation upon hybrid device/ software manufacturers to establish, maintain and demonstrate reasonable **security-by-design** and **automatic software security update** practices throughout the reasonable product lifecycle;<sup>1830</sup>
- (e) expand unfair terms laws, to contracts unfair ‘overall’, include monetary penalties and representative regulator actions; and delete insurer exemption;
- (f) mandate by ACL regulation a model consumer guarantees disclosure format by comparative table<sup>1831</sup> and an Australian-law compliant version of the OTA IOT consumer checklist (**Annex. D**) as to safety, privacy and security of IOT devices;<sup>1832</sup> and
- (g) increase penalties and allow criminal penalties for breaches of section 18.

### 8.2.2 Privacy Act 1988 (Cth) (PA)

Amend the PA to address the issues identified in **Ch. 5. Table 5.1** including:

- (a) **Amend the ‘PI’ definition** to include identifying information or opinion, when linkable to other information or opinion in the possession, custody or control of an entity;<sup>1833</sup>

<sup>1828</sup> An alternative related approach might be to include ‘security’ in ACL section 9 as to the definition of a ‘safety defect’.

<sup>1829</sup> e.g. ‘Use’ includes anonymisation, de-identification, storage, retention, accuracy, correction and transfer to third parties and related bodies’ corporate.

<sup>1830</sup> This is an update to the old-style repair and repair facilities intent of section 58.

<sup>1831</sup> See (e.g.) Apple’s ‘Consumer Law webpage’: Apple, <<https://www.apple.com/au/legal/statutory-warranty/>>

<sup>1832</sup> This is similar to the Reg 90 requirement, so not an unknown approach in consumer law. Nearly 100 entities, from businesses, consumer and privacy advocates, academic institutions, international testing organizations, and U.S. law enforcement and governmental agencies contributed to the checklist: OTA, ‘Consumer IoT Checklist’ (4 Oct 2016) <http://otalliance.actonsoftware.com/acton/attachment/6361/f-0096/1/-/-/-/IoT%20Checklist.pdf>

<sup>1833</sup> *Grubb* appears to have been interpreted to mean that if data linkage is practically “unlikely” (we wouldn’t do that!) then there is no collection of PI: *DAB v. Byron Shire Council* [2017] NSW CATAD 104. This is inconsistent with international approaches, so clearly requires an explicit legislative statement.

- (b) insert in APP 1.2 an express obligation to comply with
- *privacy by design and*
  - *privacy by default,*<sup>1834</sup> *and*
  - *defence-in-depth privacy,*
- as defined in a (revised) OAIC Guideline;<sup>1835</sup>
- (c) insert ‘chain of liability’ by deeming the device/ app PI collector responsible to consumers for unauthorised third party PI uses, unless they have implemented industry-standard anonymisation and/ or contractual protections;
- (d) insert that privacy policies must include an explicit statement as to who owns S/PI collected by the device/ app and precisely to whom data will flow (beyond general categories);
- (e) insert a definition that S/PI collected by devices/ apps in smart home and smart self contexts belongs to the consumer, prohibit collection unnecessary beyond device operation, and inconsistent with data minimisation<sup>1836</sup> as well as any non-anonymised use without express consumer opt-in to each (fully disclosed) such use, presented in non-bundled form. Note this is to address the possibility that smart home data may not be PI as defined, where devices have multiple users;<sup>1837</sup>

While not CIOT-specific, a new tort would assist to redress consumer redress in a privacy-intrusive environment. As proposed by the ALRC, a statutory cause of action in tort for serious invasion of privacy,<sup>1838</sup> to cover intrusion into a person’s “seclusion or private affairs (including

---

<sup>1834</sup> EU, above n 49. The UK Information Commissioner points out that devices with minimal interfaces may have privacy by design features available, but unless they are activated by default, they are not ‘privacy-friendly’: ICO, ‘Response to Ofcom Consultation: ‘Promoting investment and innovation in the Internet of Things’ (1 Oct 2014 accessed 2 Feb 2016) <<https://ico.org.uk/about-the-ico/consultations/ofcom-consultation-promoting-investment-and-innovation-in-the-internet-of-things/>>

<sup>1835</sup> The recommendation in footnote 3 concurs with this view: Richardson, above n 1817.

<sup>1836</sup> GDPR Art 7 Conditions for Consent provides (4) When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional upon consent to the processing of personal data that is not necessary for the performance of the contract.

<sup>1837</sup> ICO, above n 1834: The UK Information Commissioner makes the point that “it is debateable” whether smart home devices are collecting PI where multiple users are not distinguished by the device; this may be so unless the collector has other data which it can use to link or infer identity. This may depend upon household ‘type’; for example, where there is one adult and a baby, it seems safe to infer that the ‘use’ is identifiable as the adult’s usage. Note it would also be unworkable where each home must be evaluated as to whether users are capable of being distinguished – hence the proposal that all such data is deemed PI and therefore must be anonymized before use.

<sup>1838</sup> ALRC, above n 1235.

by unlawful surveillance); and the “disclosure or misuse of private information” as to a person, whether true or not, is recommended.

### 8.2.3 Australian Standards

**Develop internationally-harmonised privacy/ security standards:**<sup>1839</sup>. While beyond scope, the Art 29 WP has recommended portable, interoperable, clear, self-explanatory data formats; which include raw and aggregated data formats; minimise strong identifiers to facilitate anonymisation; and certified standards as to baseline privacy and security requirements. Once developed these should become mandatory Australian Standards, such that any breach is enforceable under the ACL.

## Regulatory Guidelines

### 8.2.3 ACCC

- (a) **Create CIOT ACL guidance** as proposed above, and:
- Clarify required smart self device “accuracy” and consumer disclosure requirements;
  - Clarify that to comply with the ACL, collectors who transmit data with consumer permission to third parties must contractually (or by other enforceable mechanism) ensure those parties comply with the terms of the initial consents;
- (b) **Create online contract ‘transparency’ guidelines** (for OAIC adoption)<sup>1840</sup> including layout, process, disclosure, notices, consent format(s), length, links use, language, reading-age and other BE factors. In this regard, the ACCC could also work with industry

---

<sup>1839</sup> The Australian IOT Alliance has proposed a UK standard, Hypercat, which facilitates smart city (and other) interoperability and vertical integration: Hypercat Alliance Ltd, ‘Hypercat is a Global Alliance and standard (PAS 212) driving secure and interoperable Internet of Things (IoT) for Industry and cities,’ <<http://www.hypercat.io/>> For Hypercat Australia, see <http://www.hypercat.io/australia.html>

<sup>1840</sup> See for example, the UK good practice “blended approach”: ICO, ‘Privacy notices, transparency and control’ (7 Oct 2016 accessed 20 Oct 2016) <<https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/>>

to devise model contract clauses,<sup>1841</sup> dashboards etc. which satisfy or exemplify such Guidelines.<sup>1842</sup>

## 8.2.4 OAIC

- (a) **Revise APP Guidelines** to reflect CIOT concerns in **Chapter 5**;<sup>1843</sup>
- (b) **Guidance as to 'PI' definition:** to clarify hybrid device scenarios,<sup>1844</sup> how *Grubb* may impact those scenarios (for example, where data is linkable,<sup>1845</sup> or where several people use a device like a car, but identity inferences are illuminated by other information held, such as driving/ entertainment settings<sup>1846</sup> reveals individual driver identity);<sup>1847</sup>
- (c) **Mandate 'privacy by design'** which is 'expected' in the non-binding Privacy Management Framework guidance under APP1.2, but not 'enforced' by the APPs. The OAIC defines privacy by design as “a holistic approach where privacy is integrated and embedded in an entity’s culture, practices and processes, systems and initiatives from the design stage onwards”.<sup>1848</sup> This should be clearly defined in APP 1.2, to include “privacy, security, choice and ‘useability’ by design” and default<sup>1849</sup> with expected, evidenced use of the following:
  - privacy impact assessments pre-device release and as changes require during product life-cycle;<sup>1850</sup>

---

<sup>1841</sup> ICO, above n 1773.

<sup>1842</sup> The ICO, for example, has issued binding guidelines as to data sharing, together with model contract clauses which if adopted, avoid the requirement to conduct privacy impact assessments: ICO, ‘Data sharing code of practice’ (accessed 8 Aug 2016) <[https://ico.org.uk/media/for-organisations/documents/1068/data\\_sharing\\_code\\_of\\_practice.pdf](https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf)> Prepared under s. 52 of the Data Protection Act (UK), this is a statutory code but does not create additional legal obligations or authoritatively state the law, but may be used in evidence and must be considered in any legal proceedings.

<sup>1843</sup> Note that the OAIC already provides around twenty guides to enhance PA compliance; these would benefit from revision. The ICO has created a very user-friendly and attractive style of publication which is worth emulating.

<sup>1844</sup> See as to apps, Art 29 WP, above n 556.

<sup>1845</sup> *DAB v. Byron Shire Council* [2017] NSW CATAD 104.

<sup>1846</sup> For example, social media connections to driver profile can reveal identity, seat settings may reveal a shorter person, driving ‘style’ data may be analysable through linkage to reveal differing drivers (for example, time of day linked to acceleration patterns etc).

<sup>1847</sup> For example, apartment smart home data may be aggregated, such that the recipient cannot distinguish which apartment contributed which data, rather than collecting individual apartment data separately.

<sup>1848</sup> OAIC, above n 1316.

<sup>1849</sup> Vulkanovski, above n 110: 67.

<sup>1850</sup> OAIC, above n 1307. See for overseas approaches, ICO, ‘Privacy impact assessments’ (7 Oct 2016 accessed 20 Oct 2016) <<https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/>>; PIAF, ‘A Privacy Impact Assessment framework for data protection and privacy rights’ (21 Sept 2011 accessed 6 Mar 2016) <[http://www.piafproject.eu/ref/PIAF\\_D1\\_21\\_Sept2011Revlogo.pdf](http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf)>

- privacy management framework;<sup>1851</sup>
- privacy enhancing technologies:<sup>1852</sup> (e.g. consent receipts and age-checking);<sup>1853</sup>
- data minimisation and destruction<sup>1854</sup> and security;<sup>1855</sup> including defence-in-depth;<sup>1856</sup>
- mandatory data breach disclosure;

and *recommended* use of communication and privacy-enhancing tools such as:

- privacy certification schemes;<sup>1857</sup>
- privacy dashboards;
- trust mark, icons or symbols, such as traffic light systems; and
- cues such as clear graphics, colour, and sound.

The OAIC could work with industry to devise model contract clauses,<sup>1858</sup> dashboards etc. which satisfy ACCC/ OAIC transparency guidelines,<sup>1859</sup> and feed into a safety cue trustmark system.

- (d) Mandate **privacy by default**, to include device and app set-up requiring default passwords be changed and automatic (non-bundled) privacy updates. Where the latter is not practicable, consumers should be personally informed (by email or device prompt) and reminded to install to patches and updates.<sup>1860</sup> Include defence-in-depth approaches such as encryption;

---

<sup>1851</sup> OAIC, above n 1308.

<sup>1852</sup> ENISA, 'Privacy Enhancing Technologies: Evolution and State of the Art' (9 Mar 2017 accessed 20 Mar 2017) <<https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art>>

<sup>1853</sup> See British Standards PAS 1296 Age Checking code of practice which provides guidance as to confirming consumer's age-related eligibility and verified parental consent before children's data processing. Kantara's consent receipt specification enables consumers to communicate and manage the personal data they have shared: Open Notice, above n 1686.

<sup>1854</sup> As required by APP 3 and (partly) 11. The Guide is here: OAIC, above n 1316.

<sup>1855</sup> OAIC, above n 572: 2; OAIC, above n 1310.

<sup>1856</sup> 'Defence-in-depth' means that security measures are considered across multiple levels: a device may be secure but if it relies upon consumers' router security (which may be poor) then designers should develop additional device steps to encrypt or otherwise secure device-related data: FTC, above n 449: 30.

<sup>1857</sup> The US-based Online Trust Alliance promotes an CIOT Trust Framework with respect to smart homes and products and consumer wearables, which identifies 23 mandatory requirements and 12 recommended requirements, imposing security, user access, disclosures and transparency and data sharing requirements upon participants: Online Trust Alliance, 'IoT Trust Framework' (8 Feb 2016 accessed 3 Mar 2016) <[https://otalliance.org/system/files/files/initiative/documents/iot\\_trust\\_framework\\_2-8\\_no\\_fn.pdf](https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_2-8_no_fn.pdf)>

<sup>1858</sup> ICO, above n 1773.

<sup>1859</sup> ICO, above n 1842.

<sup>1860</sup> iPhone users would be familiar with reminders which persist until updates are either selected automatically or at a chosen time.

- (e) Address the 'bundling' of device functionality with data collection and use 'consent': reflecting GDPR positioning,<sup>1861</sup> collection should reflect data minimisation and device functionality should not be conditional upon consumer data use beyond that reasonably required;<sup>1862</sup>
- (f) Cooperate with industry and other regulators to devise an Australian anonymisation and de-identification standard, to prescribe best practice and provide a safe harbour from liability for compliant providers as to re-identification risk. That Standard should detail prescribed checks and balances, review and audit processes and quality control requirements to be built into best practice de-identification processes.

Additional CIOT specific regulatory guidance as to difficult, sensitive or rapidly evolving areas – such as the proposed new anonymisation guidance<sup>1863</sup> - is a soft law method of conveying regulatory-expectation, while preserving flexibility.

## Self-Regulation

### 8.2.5 Australian IOT Alliance or other industry body

- (a) **Best practice self- regulation:**<sup>1864</sup> for example, devise a new *consumer IOT Code* which meets best practice standards to create a plain English consumer-communications culture and content; provide comprehensive CIOT coverage across the industry; create a certified trust mark and console system,<sup>1865</sup> an approved independent complaints process; improve

---

<sup>1861</sup> Art 7 Conditions for Consent provides (4) When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional upon consent to the processing of personal data that is not necessary for the performance of the contract.

<sup>1862</sup> EU, Art 29, above n 49: 21. The Opinion states that many IOT stakeholders only need aggregated data and so should destroy raw data as soon as that has been obtained: [7.1].

<sup>1863</sup> The OAIC would be well-advised to adopt the style and approach of the ICO document, which Peter Leonard describes as "best practice": ICO, above n 1442. The old version is here: OAIC, 'De-identification of Data and Information' *Privacy Business Resource 4* (April 2014 accessed 20 Apr 2015) [http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-business-resources/privacy\\_business\\_resource\\_4.pdf](http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-business-resources/privacy_business_resource_4.pdf)

<sup>1864</sup> An example of a Code with some overlapping issues is the ADMA Charter and Code of Practice. This is transparent, well written and includes issues such as data use, collection, transparency and safety (data security). This industry arguably presents a lower risk profile than the consumer IOT, which may justify its strong self-regulatory success.

<sup>1865</sup> Another industry has addressed this: the ADMA uses a Data Pass program which is essentially data management compliance training and designed to differentiate their members in the marketplace. It covers the data lifecycle from collection, use, analysis and disclosure uses in advertising. See '<http://www.adma.com.au/connect/articles/how-can-you-show-that-you-are-a-trusted-marketer-the-answer-is-adma-data-pass/>

legal compliance through impact assessments, audited systems and reporting practices; improved disclosure and transparency through public complaints resolution; and appeals, sanctions and consumer remedies for Code breach.

- (b) **Voluntary industry codes**<sup>1866</sup> may also pre-empt legislative intervention, and promote good practice and consumer trust. The Australian IOTA supports an interoperability standard<sup>1867</sup> and is developing guidelines. Well-regarded stipulations abound, which suggests that many CIOT issues reflect poor compliance, rather than poor information. For example, OTA and OWASP provide authoritative CIOT privacy and security<sup>1868</sup> resources (**Annex. E**) and ENISA has smart home<sup>1869</sup> and privacy-enhancing technologies<sup>1870</sup> recommendations. As to online contracting, TRUSTe and a plethora of online tools exist to improve practices.<sup>1871</sup>
- (c) **Think laterally:** Tech companies pursue product defence strategies through Bug Bounty<sup>1872</sup> and security-gap programs incentivize white-hat hackers to locate product issues.<sup>1873</sup> These programs and competitions of similar ilk are a consumer-protective positive relevant to trust mark certification.

---

<sup>1866</sup> The ACCC Guidelines define these as setting out “specific standards of conduct for an industry in relation to the way it deals with its members as well as its customers”: ACCC, ‘Guidelines for developing effective voluntary industry codes of conduct’ (31 Aug 2011 accessed 2 Feb 2016): 1 < <https://www.accc.gov.au/publications/guidelines-for-developing-effective-voluntary-industry-codes-of-conduct> >

<sup>1867</sup> Late in 2016, it supported Hypercat, a UK interoperability standard which it hopes will become the Australian Standard. It aims to improve interoperability and “data discovery”, as well as enables a device catalogue to be published as a web repository of devices and related metadata: AIOTA,

<sup>1868</sup> See for example, NIST, GSMA or UK Security Foundation approaches.

<sup>1869</sup> ENISA, ‘Online privacy tools for the general public’ (17 Dec 2015 accessed 14 Jun 2016)

<https://www.enisa.europa.eu/publications/privacy-tools-for-the-general-public>; ENISA, ‘Privacy Enhancing Technologies: Evolution and State of the Art’ (9 Mar 2017 accessed 20 Mar 2017) <https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art>; ENISA, ‘Privacy and data protection by design – from policy to engineering’, (2014 accessed 14 Jun 2016) <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design>; ENISA, ‘PETs controls matrix - A systematic approach for assessing online and mobile privacy tools’ (20 Dec 2016 accessed 10 Feb 2016) <<https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools>>

<sup>1870</sup> ENISA, above n 34; ENISA, above n 357.

<sup>1871</sup> See Appendix B, OAIC, Big Data draft, above n 1316.

<sup>1872</sup> A bug bounty program may be defined as a deal offered by websites, software developers or companies with software-dependent products whereby recognition and compensation is given to people for reporting bugs, especially those as to vulnerabilities and exploits. See the long major corporate list here: Bugcrowd, (2017) ‘Bounty Programs’ (n.d. accessed 2 Mar 2017) <<https://bugcrowd.com/list-of-bug-bounty-programs>>

<sup>1873</sup> Tesla (up to \$10,000), Fiat Chrysler (\$1500) and even the US Dept. of Defense offer such programs: Andy Greenberg, ‘Chrysler launches Detroit’s First Bug Bounty for Hackers’ *WIRED* (13 Sept 2016 accessed 20 Oct 2016) <https://www.wired.com/2016/07/chrysler-launches-detroits-first-bug-bounty-hackers/> GM offers a reporting amnesty only.

## Regulator actions

### 8.2.6 ASIC, ACCC & OAIC

- (a) **Increase (targeted) regulatory audits:** the ACCC could readily audit online practices across the CIOT industry as to misleading, deceptive or unfair contractual terms, and the APC could likewise audit privacy policies.<sup>1874</sup> Either could take enforcement action where necessary in the interests of consumer protection, industry education and deterrence enforcement. This would incentivize a compliance-based attitude within the CIOT ecosystem;
- (b) **Use the Courts:** the ACCC and ASIC could also institute proceedings to pursue an Australian precedent as to the application of the unfair terms to consumers using 'freemium' services, as well as auditing (with the OAIC) downstream data recipients (ad networks/ data brokers) as to data minimisation, destruction and security.
- (c) **Use influence:** to encourage industry Codes of Practice<sup>1875</sup> to identify best practice in specific industry applications: for example, in CIOT security<sup>1876</sup> or privacy,<sup>1877</sup> or sectorally: for example, across smart cars,<sup>1878</sup> home<sup>1879</sup> (including voice assistant technology<sup>1880</sup>) and self devices and apps.
- (d) **Think laterally:** FTC-sponsored competitions seek solutions to difficult consumer IOT problems: for example, after the massive 2016 DDoS attack, they announced a

---

<sup>1874</sup> The Commissioner has power to conduct 'Commissioner initiated investigations' (formerly 'own-motion investigations') which might cover this approach though are principally designed to investigate a suspected interference with privacy, and can more formally conduct an 'audit' (now called an 'assessment') of governmental agencies with very limited powers as to private sector entities. See OAIC, <<https://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201314/chapter-seven-privacy-compliance#s8>>

<sup>1875</sup> ACCC, 'Product Safety: A Guide to Testing' (Oct 2013 accessed 2 Aug 2016) <https://www.accc.gov.au/publications/a-guide-to-testing-product-safety>; ACCC, 'Guidelines – Use of section 155 powers' (Sept 2016 accessed 5 Set 2016) [http://www.accc.gov.au/system/files/1119\\_ACCC%20Guidelines-use%20of%20section%20155%20powers\\_FA.PDF](http://www.accc.gov.au/system/files/1119_ACCC%20Guidelines-use%20of%20section%20155%20powers_FA.PDF); ACCC, Guidelines, above n 1866.

<sup>1876</sup> GSMA, above n 113.

<sup>1877</sup> Privacy code registration is rarely used by the private sector, nor is it compelled by the APC under s 26E (2). It offers a potentially useful sectoral approach. For the two codes registered, see: <<https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/>>

<sup>1878</sup> Note the industry guidelines are here: Auto Alliance, 'Framework for Automotive Cybersecurity Best Practices' (19 Jan 2016 accessed 2 Mar 2016) <<http://www.autoalliance.org/index.cfm?objectid=1E518FB0-BEC3-11E5-950000C296BA163>>But see also: GSMA, above n 583.

<sup>1879</sup> GSMA, above n 113.

<sup>1880</sup> Alta, above n 1224.

competition for a tool to automate software updates.<sup>1881</sup> There are a range of current CIOT problems identified in this paper – including device obsolescence<sup>1882</sup> and consumer liability for refusing updates<sup>1883</sup> - which could benefit from this kind of targeted solutions-based incentivisation.

## **Consumer Education**

### **8.2.7 A safer default environment**

- (a) If privacy and security by design and default is legally required, devices should arrive to consumers set to the safest mode practicable, relieving any (immediate) need to understand many operational questions.<sup>1884</sup> Answers to these questions should be disclosed upon device purchase and set-up. Wherever possible, device prompts (e.g.) mandating complex replacements for default passwords, are more effective than expecting consumers to initiate settings change;
- (b) Safety cues such as trustmarks and dashboards should be applied to devices, apps and online, and be promoted nationally, to develop high consumer recognition and incentivize industry participation.

### **8.2.8 Consumer actions**

Empowered consumers still share some CIOT-responsibilities including:

---

<sup>1881</sup> FTC, 'IoT Home Inspector Challenge' (4 Jan 2017 accessed 15 Feb 2017) <<https://federalregister.gov/d/2016-31731>> The prize for the competition is up to \$25,000, with \$3,000 available for honourable mention winner(s).

<sup>1882</sup> Patrick Thibodeau, 'Friday's IoT-based DDoS attack has security experts worried' *ComputerWorld* (25 Oct 2016 accessed 15 Feb 2017) <<http://www.computerworld.com/article/3134746/security/fridays-iot-based-ddos-attack-has-security-experts-worried.html>>

<sup>1883</sup> Eric A. Taub, 'Your Car's New Software Is Ready. Update Now?' *The New York Times* (8 Sept 2016 accessed 16 Oct 2016) <<https://www.nytimes.com/2016/09/09/automobiles/your-cars-new-software-is-ready-update-now.html>> Note consumers may potentially face liability for a failure to update their vehicle, if manufacturers do not make updates automatic.

<sup>1884</sup> For example, questions such as how the device works, what settings options exist, how when and why data is collected; whether all data sought is necessary to provide desired functionality; where the data will go and to whom; and what risks a device or app may entail under different settings.

- (a) The obligation to use resources - such as manufacturer-checklists<sup>1885</sup>- as well as to read all reasonable, 'transparent' instructions, warnings, terms, cues and privacy policies. This presupposes significant change in the style, content and provision of such information;
- (b) Non-users whose data is collected should be informed as to the presence of CIOT devices and the data type collected. While less significant for smart self devices, smart homes could display standardised stickers to fulfil notice purposes. Smart cars are more problematic: for example Tesla has just started random on-road vision data capture from its vehicle cameras: while subject to express driver consent, it is unclear how this may impact upon other road users' rights.<sup>1886</sup> This should be clarified.

### **Continuous Policy Review & Flexibility:**

**8.2.9** Of all the differing views as to the CIOT, perhaps the most dominant is that it is a rapidly evolving and requires policy *flexibility* to avoid stifling innovation.<sup>1887</sup> This presupposes a permanent monitoring body continuously reviewing the CIOT in practice; such a body as the Australian IOT Alliance with members from industry, retailers, consumers, regulators and government. Its brief should include:

- (a) to monitor and report upon the CIOT, including (without limitation) international problems, cases and research; secondly, to develop CIOT consumer education and awareness programs; thirdly to create an industry 'consumer first, risk minimisation culture' – ADMA for example adopt the hero principle "Consumer first through empowerment and protection" - and finally, to recommend research to address CIOT problems;<sup>1888</sup>
- (b) to identify Australian problem areas (e.g. market failures);
- (c) to recommend regulatory or other appropriate government actions in a timely manner; and
- (d) to provide CIOT-related submissions to government and other enquiries.

---

<sup>1885</sup> OTA, 'Consumer IoT Checklist' (4 Oct 2016) <http://otalliance.actonsoftware.com/acton/attachment/6361/f-0096/1/-/-/-/IoT%20Checklist.pdf> See Annex D.

<sup>1886</sup> Google Glass and other wearable glasses have recording capacity as well. Thierer asserts that social norms may control inappropriate uses – he argues that people do not use mobile phone cameras in locker rooms for example. While that may be so, people sensitive to norms don't - those who are doing so for privacy-intrusive reasons still do – as peeping-Tom court cases reveal.

<sup>1887</sup> There seems little debate on this point; the question is whether it is used to stifle sensible regulatory approaches in the meantime.

<sup>1888</sup> These four recommendations have their genesis in NSTAC's recommendation 6, above n 66.

This recommendation is consistent with the final Framework requirement: *Step 6: Implement and evaluate after time.*<sup>1889</sup>

It is suggested that these multi-faceted approaches represent the most efficient and responsive approach to guiding consumer IOT development and deployment, and minimising its socially-disruptive effects in Australia. Of course, Australian actions must work in concert with international actions, and in this respect, this research suggests that the European approaches are more advanced and consonant with the ACPF objective and its implicit social and ethical values, than US regulatory positioning at present.<sup>1890</sup> But this is a discussion Australians are waiting to have.

This regulatory wish-list rests upon the following draft foundational principles – which the author recommends form a baseline for CIOT implementation, regulation and consumer expectation in Australia.

---

<sup>1889</sup> OECD, above n 505. The Consumer Policy Toolkit is discussed in Ch. 2.

<sup>1890</sup> As previously noted, Australia has followed EU consumer law approaches as to strict products liability, unfair terms and standards harmonization; as such it seems clear that this judgment has already been made. Privacy appears to be an outlier at this stage which may reflect current (and past) government disinterest. The GDPR necessitates a reconsideration of privacy in 2018, as it will practically impact upon Australian exporters.

### 8.3 Draft CIOT principles

***RECOGNISING that the consumer Internet of Things (CIOT) promises unprecedented benefits to humanity through enabling human-centred services and pervasive data collection to fuel insightful analytics and enable improved public policy and universal metrics. RECOGNISING also that the CIOT represents an unprecedented risk to consumer privacy, information security and personal autonomy, RECOGNISING ALSO the normative values implicit within the Australian Consumer Policy Regulatory Framework, these draft principles are proposed for the consideration of Australian regulators, consumer groups, the CIOT industry and other interested parties.***

***The principles apply to CIOT goods and services provided to consumers and / or to persons whose personal information has been CIOT-collected.***

#### **Principle one: General & application**

Public interest and industry success depends upon a principled, morally-grounded and trusted consumer internet of things. Self-determination is an inalienable right of all human beings.<sup>1891</sup> CIOT products are inherently human-intrusive, so should be subject to these principles with respect to product design, manufacture, deployment, data collection and use, throughout the reasonable, sustainable device and data life-cycle.

CIOT industry or sectoral groups should develop CIOT-specific codes of practice<sup>1892</sup> to establish an effective, industry-appropriate compliance culture and prescribed methods to meet all applicable consumer laws and these Principles. For greatest efficacy, such Codes should be mandatory, registrable, legally and standards-compliant and meet best practice code requirements.

These Principles apply only to CIOT devices capable of collecting consumer personal information, and where applicable, include machine-to-machine communications which are not consumer-mediated.

---

#### **References in this section are not abbreviated as they form part of the principles.**

<sup>1891</sup> International Conference of Data Protection and Privacy Commissioners, 'Mauritius Declaration on the Internet of Things' (14 Oct 2014 accessed 12 Apr 2015): 1 <<http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf>>

<sup>1892</sup> See as to voluntary ACCC-registrable codes: ACCC, 'Guidelines for developing effective voluntary industry codes of conduct' (31 Aug 2011 accessed 2 Aug 2016) <https://www.accc.gov.au/publications/guidelines-for-developing-effective-voluntary-industry-codes-of-conduct> As to APP-registrable Codes see PA section 26C. Any breach of a registered code constitutes an 'interference with privacy' under the PA: OAIC, 'Guidelines for developing codes' (Sept 2013 accessed 2 Aug 2016) <https://www.oaic.gov.au/agencies-and-organisations/advisory-guidelines/guidelines-for-developing-codes> Note that code developers must undertake public consultation before making an application to register a code (ss 26F(2) which increases accountability.

## **Principle two: Examine ethics**

The CIOT is disruptive to ethics, so consumer products should only be released where they satisfy a proportionality test, such as an *ethical impact assessment*, comparing relative product benefits or uses to the cost or disruptions they may or will cause to consumers.

Such assessment must also include consumer empowerment and protection through factors such as transparency, fairness, honesty, consumer choice and security, and having regard to a reasonably practicable chain-of-responsibility approach to the product, security updates and related consumer data life-cycle.

Guidance: Wright (2011)<sup>1893</sup>

## **Principle three: Protect privacy**

The consumer IOT is disruptive to privacy, so products should only be released where they survive a proportionality test, such as a *privacy impact assessment*, and comply with privacy by design, privacy-by-default and privacy defence-in-depth principles.

Product privacy and default provision of product privacy-enhancing updates is a manufacturer obligation for the reasonable product lifecycle. Personal information anonymisation, minimisation, time-limited purpose use and timely destruction are privacy best practice.

Guidance: OAIC, 'Guide to undertaking privacy impact assessments'<sup>1894</sup>  
ICO, 'Conducting privacy impact assessments code of practice'<sup>1895</sup>  
Privacy Commissioner of Ontario, 'Privacy by Design'<sup>1896</sup>  
GSMA, 'IoT Privacy by Design Decision Tree'<sup>1897</sup>

---

<sup>1893</sup> See for example, David Wright, 'A Framework for the ethical impact assessment of information technology' *Ethics and Information Technology* 13: 3 (2011) 199–226 accessed 3 Mar 2016 <<http://dl.acm.org/citation.cfm?id=2035938>>

<sup>1894</sup> OAIC, 'Guide to undertaking privacy impact assessments' (May 2014 accessed 2 Jan 2016) <<https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments>>

<sup>1895</sup> ICO, 'Conducting privacy impact assessments code of practice' (Feb 2014 accessed 5 Mar 2016) <<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>>

<sup>1896</sup> Information & Privacy Commissioner of Ontario, 'Privacy by Design' (2013 accessed 5 Jan 2016) <<https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf>>

<sup>1897</sup> GSMA, 'IoT Privacy by Design Decision Tree' (8 May 2015 accessed 8 Mar 2016) <<http://www.gsma.com/iot/iot-knowledgebase/iot-privacy-design-decision-tree/>>

## Principle four: Secure insecurity

The CIOT is disruptive to device, data and network security, so products should only be released where they survive a proportionality test, such as a *security impact assessment*, and where personal information is likely to be collected, comply with security-by-design security-by-default and security defence-in-depth principles.

Product security including end-to-end encryption and default unbundled security updates provision remains an ongoing manufacturer obligation for the reasonable product lifecycle. Data minimisation, time-limited purpose use and timely destruction are security best practice.

Data collection solely for product or network security purposes by default is permissible provided no other use is made and personally-identifiable information is removed if shared with third parties for threat intelligence or prevention purposes.

Guidance: GSMA, 'IoT Security Guidelines Overview Document'<sup>1898</sup>  
OWASP, 'Security by Design Principles'<sup>1899</sup>  
Australian IOT Alliance, 'IOT Security Guideline'<sup>1900</sup>  
OAIC, 'Guide to information security'<sup>1901</sup>

## Principle five: Transparency to trust

Consumer trust is vital to CIOT development and success.

Trust is enhanced by provider integrity, accountability and transparency, and privileging consumer control and empowerment:

*Integrity* is enhanced by provider fairness, honesty and commitment to consumer empowerment and protection.

---

<sup>1898</sup> GSMA Security Guidelines: <http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/>; GSMA, 'Automotive IoT Security: Countering the Most Common Forms of Attack' (22 March 2016 accessed 2 Apr 2016) <<http://www.gsma.com/connectedliving/automotive-iot-security-countering-the-most-common-forms-of-attack/>>

<sup>1899</sup> OWASP, 'Security by Design Principles' (3 Aug 2016)

<[https://www.owasp.org/index.php/Security\\_by\\_Design\\_Principles](https://www.owasp.org/index.php/Security_by_Design_Principles)> See also OWASP, 'Consumer IoT Security Guidance' (14 May 2016 accessed 2 Jun 2016) <[http://www.owasp.org/index.php?title=IoT\\_Security\\_Guidance&oldid=216879](http://www.owasp.org/index.php?title=IoT_Security_Guidance&oldid=216879)>

<sup>1900</sup> Australian IOT Alliance, 'IoT Security Guideline V1.0' (Feb 2017 accessed 2 Mar 2017): 17- 18

<<https://static1.squarespace.com/static/573853ed1d07c093e27aefd2/t/58ab9bf8ebbd1a2b74e2aa2d/1487641596432/IoTAA+Security+Guideline+V1.0.pdf>>

<sup>1901</sup> OAIC, 'Guide to information security' (April 2013 accessed 10 Apr 2015) [2] < <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-securing-personal-information>>

*Accountability* is enhanced by providers adhering to these Principles and prompt disclosure and remedial actions as to product defect and data breach.

*Transparency* is enhanced through clear consumer-friendly language, fair terms, accurate and honest disclosure of data collection purpose and data flows, and the provision of simple control-enhancing mechanisms as to device operation, settings and preferences. It is not enhanced through coercive settings or mechanisms, or reducing functionality unnecessarily where consumers do not accept data sharing or certain uses.

*Consumer control and empowerment* is enhanced by best practice information communication on-device, in-app or (where a limited interface) online, and control-enhancing technologies such as granular opt-in systems, dashboards, cues and trust marks.

Consumer trust is promoted by provider adherence to best practices in product design, privacy and security, consent and data management, together with ongoing, documented, product assessment, improvement and update practices over the reasonable product lifecycle.

Guidance: ICO, 'Privacy notices, transparency and control – a code of practice on communicating privacy information to individuals'<sup>1902</sup>  
Online Trust Alliance IoT Trust Framework (**Annex. E**)

### **Principle six: Create choice**

CIOT personal information belongs to the consumer from whom it was collected.

CIOT providers may use consumer data for the primary purpose of providing the CIOT goods and services, and for secondary purposes 'reasonably expected' or consented-to by a consumer. Best practice suggests that any non-primary purpose uses and sharing of consumer data should require express, granular, affirmative "opt-in" consents by consumers. Default settings should exclude all uses save for those of a primary nature.

Providers must provide simple, accessible and clear methods for consumers to easily, at their option, obtain access to or to correct data and to opt in or out of data sharing, without disincentive. Best practice data management requires providers to ensure that consumer data is readily accessible, correctable, trackable and destructible upon reasonable consumer request.

---

<sup>1902</sup> ICO, 'Privacy notices, transparency and control – a code of practice on communicating privacy information to individuals' (24 Mar 2016 accessed 20 Apr 2016) <https://ico.org.uk/media/about-the-ico/privacy-notices-transparency-and-control-0-0.pdf>

Example: EU General Data Protection Regulation (GDPR) 2016/679

### **Principle seven: Always anonymise**

Anonymisation of consumer data is best practice. Anonymisation practices require an ongoing assessment of best practice and re-identification risk. Where re-identification exceeds a 'low or remote' risk, providers must not provide such data to third parties.

Providers sharing consumer data with third parties must not do so unless consumer consent is first obtained. Best practice requires that providers use contractual and technical means to ensure that such data is thereafter used and retained consistently with the terms of that consent.

Guidance: EU, Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques'<sup>1903</sup>  
ICO, 'Anonymisation Code of Practice'<sup>1904</sup>  
OAIC, 'De-identification of data and information'<sup>1905</sup>

### **Principle eight: Future harmonisation & development**

Providers and regulators must monitor best practice international developments impacting upon the consumer IOT, including regulation, technical developments, product defects, security or data breach and responses to market failure or other problem. Where necessary or useful, best international practice should be incorporated into Australian products and regulation (as applicable) in a timely manner.

These Principles should evolve over time due to the highly dynamic nature of CIOT technology and the monitored experience and assessment of consumers, regulators and industry.

### **Glossary**

**consumer IOT** refers to internet of things devices and applications which are intended for consumer use, where 'consumer' is as defined in the ACL

---

<sup>1903</sup> EU, Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (10 Apr 2014 accessed 2 Jan 2016) < [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf) >

<sup>1904</sup> ICO, 'Anonymisation Code of Practice' (accessed 8 Aug 2016 <<https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>>

<sup>1905</sup> OAIC, 'De-identification of Data and Information' Privacy Business Resource 4 (April 2014 accessed 20 Apr 2015) <[http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-business-resources/privacy\\_business\\_resource\\_4.pdf](http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-business-resources/privacy_business_resource_4.pdf)>

**defence-in-depth** means that even where one control is reasonable, more controls approaching risks in “different fashions” are preferable. Controls used in depth render severe vulnerabilities difficult to exploit and so lessen the likelihood of occurrence<sup>1906</sup>

**personal information** and **sensitive information** are as defined in the Privacy Act 1988 (Cth) and included in references to consumer ‘data’ in these principles

**product(s)** include(s) CIOT devices and related software apps

**proportionality** refers to an approach whereby there must be a legitimate aim for a measure, the measure must be suitable, necessary and reasonable to achieve the aim, considering other competing interests or approaches. Relevant factors include the harm to be guarded against, the cost of measures, the state of the art as at product release date, the nature, scope, context, purpose and cost of a product; and the nature and severity of consumer risk.

---

<sup>1906</sup> OWASP, ‘Security by Design Principles’ (3 Aug 2016 accessed 20 Sept 2016)  
<[https://www.owasp.org/index.php/Security\\_by\\_Design\\_Principles](https://www.owasp.org/index.php/Security_by_Design_Principles)>

## Conclusion

*“It isn’t really about things. It’s about Us. The Internet of Us.*

*The human and digital experiences no longer sit side by side; they are bound ever tighter by this new way of life...”<sup>1907</sup> - Microsoft*

Seismic technological events happen - and portend vast disturbances and recreate human experience. The consumer internet of things – in its highly disruptive technological moment - is one such event. This digital ‘skin’ portends almost organic innovation, unprecedented capabilities and analytics, extraordinary efficiencies and will in many ways, greatly enhance consumer life and human well-being. Smart cars alone, will undoubtedly save lives, while smart self and home will enable unprecedented enhancements to human health, fitness, environment and lifestyle management. The CIOT promises an efficient, metrics-driven and consumer-responsive world. The critical question is whether that world will also entail a principled, morally-grounded and trusted consumer IOT; whether it will ultimately empower or transform us all into “hostages of technology”.<sup>1908</sup> For in locating and activating consumer’s most intimate ‘darkest’ data, the smart world will also locate, activate and weaponize the worst attributes of ubiquitous digital surveillance and the big data analytics ecosystem, perpetuate the greatest flaws of consumer power imbalance, rampant information asymmetry, online ‘notice-and-choice’ contracting, privacy-trading, exponentially-greater data gathering and algorithm-driven profiling. The CIOT will thus both challenge and expose the very bounds of consumer and privacy protection in this country.

This thesis has drawn a uniquely Australian snapshot of the CIOT, by mapping out its scope, scale and stakes from limited Australian information enhanced by sharper international statistics, and reflecting critically upon international studies and consumer experience, which should inform Australia’s earliest policy-making and regulatory steps. The analysis explores six serious problems which the consumer IOT creates or exacerbates, examines actual and potential detriments which consumers may suffer, identifies specific consumer and privacy law gaps in responding to CIOT-based issues, proposes flexible but effective alliance-based regulatory responses to those problems and finally, devises a set of simple baseline principles, informed by best practice international research and expert recommendations. It is hopefully, some help towards a national conversation, already overdue by international standards. While industry is working hard to excite government interest, it is difficult not to note inaction, or the fact that there are significant social, legal and ethical issues attached to this technology which warrant a reflective,

---

<sup>1907</sup> GSMA, above n 113.

<sup>1908</sup> EC, above n 93: 29.

values-based community debate, to preface policy development and a required regulatory response. As Julie Brill warned over three years ago:

*“Academics technologists, lawyers... consumer advocates and policymakers all have a role to play in developing these [consumer] protections. The time to start is now.”*<sup>1909</sup>

Given CIOT is here now, its inevitably disruptive impacts, its evidenced serious detriments, and the many consumer protection gaps identified in this thesis, it is time that Australian consumer protection regulators take the consumer IOT head-on. This thesis proposes recommendations and principles to that end, as at best, a proactive high ground and at worst, a working starting point. It is to be hoped that regulators will respond to strengthen consumer empowerment and protection now, before Australians venture forth into a dauntingly vast, but excitingly-transformational, brave new world... the consumer internet of things.

---

<sup>1909</sup> Brill, above n 446.

## Bibliography

---

Please note- commonly used acronyms (such as ACCC) appear by long form title alphabetically under bold headings, for ease of reference.

### A

AA, 'Motoring Costs, UK' (2014 accessed 2 Jan 2016)  
<<http://www.theaa.com/resources/Documents/pdf/motoring-advice/running-costs/diesel2014.pdf>>

AAP, 'Black boxes in cars raise privacy concerns' *The Australian* (9 Dec 2012 accessed 18 Mar 2016)  
<http://www.theaustralian.com.au/news/latest-news/black-boxes-in-cars-raise-privacy-concerns/story-fn3dxix6-1226532985229>

Abbott, Mike, 'Testimony of Mike Abbott, General Partner, Kleiner Perkins Caulfield and Byers' (11 Feb 2015 accessed 7 Mar 2016) <<http://www.commerce.senate.gov/public/index.cfm/2015/2/the-connected-world-examining-the-internet-of-things>>

Abelson, Michael F., 'Statement to U.S. Senate Committee on Commerce, Science and Transportation' *General Motors Co.*, (15 Mar 2016 accessed 16 Mar 2016) <  
[http://www.commerce.senate.gov/public/\\_cache/files/b853b8b4-3b5e-46e1-b7b9-e7050b234e40/742AAAE9051055EF518448D3C9B9F49D.mfa-gm-statement-03-15-2016.pdf](http://www.commerce.senate.gov/public/_cache/files/b853b8b4-3b5e-46e1-b7b9-e7050b234e40/742AAAE9051055EF518448D3C9B9F49D.mfa-gm-statement-03-15-2016.pdf)>

ABI Research, 'The Internet of Things will drive Wireless Connected devices to 40.9 Billion in 2020' *Press Release* (20 Aug 2014 accessed 26 Mar 2016) <<https://www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect/>>

Ablon, Lillian, Paul Heaton, Diana Lavery & Sasha Romanosky, 'Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information' *Rand* (2016 accessed 10 Jun 2016)  
<[http://www.rand.org/pubs/research\\_reports/RR1187.html](http://www.rand.org/pubs/research_reports/RR1187.html)>

Ablon, Lillian 'Keeping Hackers Away from Your Car, Fridge and Front Door' *The National Interest* (7 Dec 2015 Accessed 10 Jun 2016) <<http://nationalinterest.org/feature/keeping-hackers-away-your-car-fridge-front-door-14525?page=show>>

Abraham, Tony & Marguerite Oneto, 'Consumers as data brokers: Should they Sell their Own Personal Data?' (n.d. accessed 5 Apr 2016)  
<[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00075-98123.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00075-98123.pdf)>

Accenture, 'Eighty Percent of Consumers Believe Total Data Privacy No Longer Exists, Accenture Survey Finds' (28 May 2014 accessed 2 Jun 2016)  
<<https://newsroom.accenture.com/news/eighty-percent-of-consumers-believe-total-data-privacy-no-longer-exists-accenture-survey-finds.htm>>

Accenture, 'Digital Trust in the IoT Era' (2015 accessed 2 Feb 2016)  
<[https://www.accenture.com/t20151008T065801\\_\\_w\\_\\_us-en/\\_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub\\_18/Accenture-Digital-Trust.pdf#zoom=50](https://www.accenture.com/t20151008T065801__w__us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_18/Accenture-Digital-Trust.pdf#zoom=50)>

Accenture, 'Connections with leading thinkers: Rebecca Schindler' (2015 accessed 10 Jan 2016) [WeissAssets/DotCom/Documents/Global/PDF/Dualpub\\_2/Accenture-Institute-Conversations-Rebecca-Schindler.pdf](https://www.accenture.com/us-en/~/media/Assets/DotCom/Documents/Global/PDF/Dualpub_2/Accenture-Institute-Conversations-Rebecca-Schindler.pdf)

Accenture, 'Industrial Internet of Things: Reimagine the Possibilities' (2015 accessed 5 Mar 2016) <[https://www.accenture.com/us-en/\\_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf](https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf)>

Accenture, 'Winning with the Industrial internet of Things; (2015 accessed 3 June 2016) <[https://www.accenture.com/us-en/~/\\_media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Digital\\_1/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.pdf](https://www.accenture.com/us-en/~/_media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Digital_1/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.pdf)>

Accenture, 'Connected Vehicle Survey' (2016 accessed 2 Sept 2016) <https://www.accenture.com/us-en/insight-automotive-connected-vehicle>

Accenture Digital, 'The Era of Living Services' (2016 accessed 23 Mar 2016) <https://www.accenture.com/us-en/insight-living-services-from-accenture-digital.aspx>

Accenture, 'Igniting Growth in Consumer Technology' 2016 Accenture Digital Consumer Survey (2016 accessed 24 Mar 2016) <[https://www.accenture.com/\\_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf](https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf)>Acker, Joe, 'Toyota, Ford, GM Topple Car Hacking Claims' *Law360* (25 Nov 2015 accessed 16 Aug 2016) <<https://www.law360.com/articles/731922/print?section-automotive>>

Ackerman, Evan, 'It's Now (Temporarily) Legal to Hack Your Own Car' (1 Nov 2016 accessed 12 Nov 2016) *IEEE Spectrum* <<http://spectrum.ieee.org/cars-that-think/transportation/systems/its-now-temporarily-legal-to-hack-your-own-car>>

Ackerman, Spencer and Sam Thielman, 'US intelligence chief: we might use the internet of things to spy on you', *The Guardian* (20 Feb 2016 accessed 5 Jun 2016) <<https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper>>

Ackerman, Spencer 'CIA Chief: We'll Spy on you through Your Dishwasher' *WIRED* (15 Mar 2012 accessed 5 Jun 2016) <<https://www.wired.com/2012/03/petraeus-tv-remote/>>

Acquisti, Alessandro, Laura Brandimarte and George Lowenstein, 'Privacy and human behaviour in the age of information' *Science* (30 Jan 2012) 347: 6221: 509 -514.

Acquisti, Alessandro, Curtis R. Taylor and Liad Wagman, 'The Economics of Privacy', *Journal of Economic Literature*, 52:2, (8 Mar 2016) Sloan Foundation Economics Research Paper No. 2580411, <<http://ssrn.com/abstract=2580411>>

Acquity Group, 'The Internet of Things: The Future of Consumer Adoption' *Accenture Interactive* (2014 accessed 3 Mar 2016) <<http://quantifiedself.com/docs/acquitygroup-2014.pdf>>

Adams, Andrew, 'Man says Tesla car started on its own, crashed into trailer' *KSL.com* (11 May 2016 accessed 2 Jun 2016) <<https://www.ksl.com/?sid=39727592&nid=148&title=utah-man-says-tesla-car-started-on-its-own-crashed-into-trailer>>

Adrian, Angela. 'Has a digital civil society evolved enough to protect privacy?' *Alternative Law Journal* 37:3 (Jul 2012 accessed 2 Mar 2016) 183-185. <  
<http://search.informit.com.au.ezproxy.bond.edu.au/documentSummary;dn=290658274671538;res=IELAPA>> ISSN: 1037-969X. [cited 25 Sep 16].

Ahuja, Anjana, 'Beware the electronic gossips eavesdropping in our homes' *ft.com* (24 Dec 2015 accessed 26 Mar 2016) <<http://app.ft.com/cms/s/69d6f4ae-a8b4-11e5-9700-2b669a5aeb83.html?sectionid=stream/topicsId/YmJiOTlyZTgtMmYwMC00MWFILTk2MGMtNDQzOGFjMzRiZjZj-VG9waWNz>>

AIA, 'The Case for Incentivising Health: Using Behavioural Economics to improve health and wellness' White Paper (2016 accessed 2 Sept 2016)  
<[http://www.aia.com.au/content/dam/au/en/docs/key\\_moments\\_content/The\\_Case\\_for\\_Incentivising\\_Health\\_Using\\_behavioural\\_economics\\_to\\_improve\\_health\\_and\\_wellness.pdf](http://www.aia.com.au/content/dam/au/en/docs/key_moments_content/The_Case_for_Incentivising_Health_Using_behavioural_economics_to_improve_health_and_wellness.pdf)>

Aiken, K Damon and David M Boush, 'Trustmarks, Objective-Source Ratings, and implied Investments in Advertising' *Journal of the Academy of Marketing Science* 34 (2006) 308- 323

Alba, Davey, 'FTC Warns of the Huge Security Risks in the Internet of Things' *Wired* (27 Jan 2015 accessed 18 Mar 2016) <http://www.Guido.com/2015/01/ftc-warns-huge-security-risks-internet-things/>  
Alert Logic, *Cloud Security Report* (Spring 2014 accessed 10 July 2014) [12]  
<<http://www.findwhitepapers.com/force-download.php?id=37838>>

Alexander, Charles, Lucy McGovern and Helen Paterson, 'Some issues relating to privacy and young people' *Minter Ellison Privacy Law Bulletin* (Mar 2015 accessed 2 Jun 2016)  
<<http://www.minterellison.com/files/Uploads/Documents/Publications/Articles/Some%20issues%20relating%20to%20privacy%20and%20young%20people.pdf>>

Alison, Conor, 'This smart condom ring will track your sexual activity' *WAREABLE* (3 March 2017 accessed 7 Mar 2017) <https://www.wearable.com/wearable-tech/smart-condom-sex-activity-tracker-4012>

Allen & Overy, 'The EU General Data Protection Regulation' (2016 accessed 2 Sept 2016)  
<http://www.allenoverly.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf>

Allens, 'Submission to the Australian Consumer Law Review' (2016 accessed 10 Sept 2016)  
<http://consumerlaw.gov.au/files/2016/07/Allens.pdf>

Alliance of Automobile Manufacturers Inc. and Association of Global Automakers, Inc. (**Auto Alliance**), 'Consumer Privacy Protection Principles' (12 November 2014 accessed 16 Mar 2016)  
<<http://www.autoalliance.org/index.cfm?objectid=CC629950-6A96-11E4-866D000C296BA163>>

Allcott, Shirleen. 'Car auto-dials 911 to report accident after driver allegedly commits hit-and-run' *ABC News* (4 Dec 2015 accessed 25 Apr 2016) <http://abc7chicago.com/technology/car-auto-dials-911-to-report-accident-after-driver-allegedly-commits-hit-and-run/1109554/>

Alta Associates' Executive Women's Forum, 'Voice Privacy Guiding Principles' (Version 1, Feb 2016 accessed 15 Mar 2016) <[http://c.ymcdn.com/sites/www.ewf-usa.com/resource/collection/CAA076AF-9566-4E1E-9F07-6421154DE0EA/Voice\\_Privacy\\_Guiding\\_Principles\\_Public\\_\(final\).pdf](http://c.ymcdn.com/sites/www.ewf-usa.com/resource/collection/CAA076AF-9566-4E1E-9F07-6421154DE0EA/Voice_Privacy_Guiding_Principles_Public_(final).pdf)>

Anderson, Mark, 'Black Hat 2014: Hacking the Smart Car' *IEEE Spectrum* (6 Aug 2014 accessed 16 Mar 2016) <<http://spectrum.ieee.org/cars-that-think/transportation/systems/black-hat-2014-hacking-the-smart-car>>

Angwin, Julia, Jeff Larson, Surya Mattu and Lauren Kirchner, "Machine Bias" (23 May 2016) *ProPublica* <<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>>

AP, 'Hello Barbie and Security Not the Perfect Couple, Claims Lawsuit' *Investor's Business Daily* (n.d. 2015 accessed 15 Jan 2017) <<http://www.investors.com/news/technology/hello-barbie-security-not-the-perfect-couple-claims-lawsuit/>>

Arias, Andrea, 'The NIST Cybersecurity Framework and the FTC' *FTC Blog* (31 Aug 2016 accessed 1 Sept 2016) <[https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc?utm\\_source=govdelivery](https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc?utm_source=govdelivery)>

Arieff, Allison, 'Driving Sideways' *The New York Times Opinionator* (23 Jul 2013 accessed 3 Mar 2016) <<https://opinionator.blogs.nytimes.com/2013/07/23/driving-sideways/#more-146616>>

Armstrong, Stephen, 'Just how smart do we want our homes to be?' in *Raconteur*, 'Internet of Things' *The Times* (30 Mar 2016 accessed 30 Mar 2016): 8 <<http://raconteur.net/internet-of-things>>

Arnold Bloch Leibler, (27 May 2016 accessed 20 Aug 2016) <[http://consumerlaw.gov.au/files/2016/07/Arnold\\_Bloch\\_Leibler.pdf?>](http://consumerlaw.gov.au/files/2016/07/Arnold_Bloch_Leibler.pdf?>)

Arsens, Liviu, 'Hacking Vulnerable Medical Equipment Puts Millions at Risk' *InformationWeek* (10 Apr 2015 accessed 2 Aug 2016) <<http://www.informationweek.com/partner-perspectives/bitdefender/hacking-vulnerable-medical-equipment-puts-millions-at-risk/a/d-id/1319873>>

Arthur, Charles, 'The "things" are smart and will work for us' in *Raconteur*, 'Internet of Things' *The Times* (30 Mar 2016 accessed 30 Mar 2016): 3 <<http://raconteur.net/internet-of-things>>

## **Article 29 Data Protection Working Party (Art29WP)**

Art29WP, 'Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)' (Adopted on 19 July 2016 accessed 26 Apr 2017) <[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf)>

Art29WP, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (16 Sept 2014 accessed 6 Jan 2016): 21 [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf)

Art29WP, 'Opinion 03/2013 on Purpose Limitation' (adopted 2 Apr 2013 accessed 6 Jan 2016) <[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf)>

Art29WP, 'Opinion 05/2014 on Anonymisation Techniques' (adopted 10 Apr 2014 accessed 6 Jan 2016) <[https://cnpd.public.lu/fr/publications/groupe-art29/wp216\\_en.pdf](https://cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf)>

Art29WP, 'Opinion 04/2007 on the Concept of Personal Data' (adopted 20 Jun 2007 accessed 6 Jan 2016) <[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf)>

Ashford, Warwick, 'EU data protection rules affect everyone, say legal experts' *ComputerWeekly.com* (11 Jan 2016 accessed 18 Jul 2016) <<http://www.computerweekly.com/news/4500270456/EU-data-protection-rules-affect-everyone-say-legal-experts>>

Ashford, Warwick 'Target agrees to \$10m breach compensation' *Computer Weekly* (19 Mar 2015 accessed 19 Nov 2015) < <http://www.computerweekly.com/news/2240242624/Target-agrees-to-10m-breach-compensation>>

Ashford, Warwick 'Cybercrime costs worldwide business an estimated at £265bn a year, a study has revealed' (9 Jun 2014 accessed 19 Nov 2015)  
<http://www.computerweekly.com/news/2240222189/Cybercrime-costs-business-265bn-a-year-report-reveals>

Ashford, Warwick 'IoT security: lack of expertise will hurt, says Bruce Schneier' *Computer Weekly* (10 Jun 2016 accessed 19 Jun 2016)  
[https://www.schneier.com/news/archives/2016/06/iot\\_security\\_lack\\_of.html](https://www.schneier.com/news/archives/2016/06/iot_security_lack_of.html)

Ashford, Warwick, 'EU data protection rules affect everyone, say legal experts' *ComputerWeekly* (11 Jan 2016 accessed 18 Jul 2016) <<http://www.computerweekly.com/news/4500270456/EU-data-protection-rules-affect-everyone-say-legal-experts>>

Ashley, Paul, Steve Shillington & Mike Neuenschwander, 'An Internet of Personas', *Anonyme Labs Inc Submission to FTC Privacycon 2016* (n.d. accessed 6 Apr 2016)  
<[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00022-97628.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00022-97628.pdf)>

Ashton, Kevin 'That 'Internet of Things' thing' *RFID Journal* (22 Jun 1999 accessed 3 Apr 2016)  
<http://www.rfidjournal.com/articles/view?4986>>

Ashton, Kevin, 'That 'Internet of Things' Thing: In the real world, things matter more than ideas.' *RFID Journal* (2009 accessed 8 Apr 2016) <<http://www.rfidjournal.com/articles/view?4986>>

Associated Press & APTN, 'Anton Yelchin: parents of Star Trek actor sue Jeep manufacturer for wrongful death' *The Telegraph* (3 Aug 2016 accessed 16 Sept 2016)  
<http://www.telegraph.co.uk/news/2016/08/02/anton-yelchin-parents-of-star-trek-actor-sue-jeep-manufacturer-f/>

Association for Data-driven Advertising and Marketing, '2016 Regulatory Landscape' (1 Mar 2016 accessed 2 Mar 2016) <<http://www.adma.com.au/comply/regulatory-newsletter/2016-regulatory-landscape/>>

Association for Data-driven Marketing and Advertising, 'Best Practice Guideline: Big Data' (2013 accessed 28 Mar 2015) <<http://www.adma.com.au/assets/Uploads/Downloads/Big-Data-Best-Practice-Guidelines.pdf>>

Association of British Insurers, 'How data makes insurance work better for you' (2015 accessed 2 Jul 2016)

<<https://www.abi.org.uk/~media/Files/Documents/Publications/Public/2015/Data/How%20data%20makes%20insurance%20work%20better%20for%20you.pdf>>

Atherton, Kelsey, 'Tesla model S owners can pay more to unlock their full battery' *Australian Popular Science* (6 May 2016 accessed 15 May 2016) < <http://www.popsci.com.au/tech/cars/tesla-model-s-owners-can-pay-more-to-unlock-their-full-battery,419168>>

Atlantic Council, 'Smart Homes and The Internet of Things' [Greg Lindsay, Beau Woods And Joshua Corman] *Issue Brief* (30 Mar 2016 accessed 2 Jun 2016)  
<<http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the-internet-of-things>>

Attorney-General's Department, Law Council of Australia, 'Access to telecommunications data in civil proceedings' (24 Jan 2017 accessed 2 Feb 2017)  
<<https://www.lawcouncil.asn.au/resources/submissions/access-to-telecommunications-data-in-civil-proceedings>>

Attorney-General's Department, 'Identity Crime and Misuse in Australia' (2013- 4 accessed 5 Aug 2016)  
<<https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Identity-Crime-and-Misuse-in-Australia-2013-14.pdf>>

Auchard, Eric, 'Exclusive: Big data breaches found at major email services – expert' *Reuters* (4 May 2016 accessed 5 May 2016) <http://www.reuters.com/article/us-cyber-passwords-idUSKCN0XV116>

Auchard, Eric and Tova Cohen, 'Mobileye says Tesla was 'pushing the envelope in terms of safety' (14 Sept 2016 accessed 20 Sept 2016) *Reuters* <http://www.reuters.com/article/us-mobileye-tesla-idUSKCN11K2T8>

### **Australian Automobile Aftermarket Association (AAAA)**

AAAA, 'AAAA Demands Better Consumer Law protection for Car owners' (15 July 2016 accessed 30 June 2016) <<https://www.aaa.com.au/news.asp?id=242>>

AAAA, 'AAAA welcomes ACCC market study: New Car Retailing Industry' (20 Jun 2016 accessed 30 Jun 2016) <<https://www.aaa.com.au/news.asp?id=243>>

AAAA, 'AAAA score political parties' policies: vehicle data sharing' (28 June 2016 accessed 30 June 2016) <<https://www.aaa.com.au/news.asp?id=244>>

AAAA, 'Make it Mandatory: Automotive Repair Code of Practice' *Press release* (29 June 2016 accessed 2 Jul 2016) <https://www.aaa.com.au/policy-advocacy/make-it-mandatory-automotive-repair-code-of-practice/>

AAAA, 'AAAA Vehicle Data Sharing Federal Election Scorecard (29 Jun 2016 accessed 30 June 2016)  
<<http://www.aaa.com.au/data/AAAA%20Vehicle%20Data%20Sharing%20Federal%20Election%20Scorecard.pdf>>

AAAA, Agreement on Access to Service and Repair Information for Motor Vehicles 2014, Code of Practice", (2014 accessed 30 June 2016)  
<<https://www.aaa.com.au/files/issues/Signed%20Agreement%20-%20Access%20to%20Service%20and%20Repair%20Information%20151214.pdf>>

## **Australian Bureau of Statistics (ABS),**

ABS, '8501.0.55.007 - Information Paper: Measurement of Online Retail Trade in Macroeconomic Statistics, 2013' (19/08/2013 accessed 17 July 2014)

<http://www.abs.gov.au/AUSSTATS/abs@.nsf/Latestproducts/8501.0.55.007>

Main%20Features12013?opendocument&tabname=Summary&prodno=8501.0.55.007&issue=2013&num=&view=

ABS, 'Paid Cloud Computing in Australian Business' 2013-14 Business Characteristics Survey (16 Jul 2015 accessed 2 Aug 2016)

<http://www.abs.gov.au/AUSSTATS/abs@.nsf/Latestproducts/8129.0Main%20Features32013-14?opendocument&tabname=Summary&prodno=8129.0&issue=2013-14&num=&view=>

ABS, 'Household Use of Information Technology, Australia, 2014-15' (18 Feb 2016 accessed 10 May 2016) <<http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0>>

ABS, '8153.0 – Internet Activity, Australia, December 2015 (accessed 2 Mar 2016)

<<http://www.abs.gov.au/ausstats/abs@.nsf/PrintAllPreparePage?>>

## **Australian Communications Media Authority (ACMA)**

ACMA 'The Internet of Things and the ACMA's areas of focus: Emerging issues in media and communications' *Occasional Paper* (Nov 2015 accessed 26 Nov 2015)

file:///C:/Users/Kate/Desktop/ACMA%20Internet%20of%20Things\_occasional%20paper%20pdf.pdf>

ACMA, 'Australian Consumer Law Review ACMA submission in relation to equipment and device supply' (June 2016 accessed 4 Sept 2016)

<[http://consumerlaw.gov.au/files/2016/07/Australian\\_Communications\\_and\\_Media\\_Authority.pdf](http://consumerlaw.gov.au/files/2016/07/Australian_Communications_and_Media_Authority.pdf)>

ACMA, "Evidence-informed regulatory practice: An adaptive response (April 2015 accessed 10 Mar 2016)

<<http://www.acma.gov.au/~media/Regulatory%20Frameworks%20and%20International%20Engagement/Report/PDF/Evidence-informed%20regulatory%20practice%2>>

ACMA, 'The Internet of Things and the ACMA's area of focus— Emerging issues in media and communications occasional paper' Consultation number: IoT2015 (Nov 2015 accessed 10 Mar 2016)

<<http://www.acma.gov.au/theacma/internet-of-things-and-the-acmas-areas-of-focus-occasional-paper>>

ACMA, Mobile apps—Emerging issues in media and communications, Occasional Paper 1 (May 2013)

<<http://www.acma.gov.au/theACMA/Library/researchacma/Occasional-papers/emerging-issues-in-media-and-communications-occasional-papers-1>>

ACMA, 'The cloud: services, computing and digital data—Emerging issues in media and communications', *Occasional Paper 3* (June 2013)

< <http://www.acma.gov.au/theACMA/About/The-ACMA-story/Connected-regulation/privacy-and-digital-data-emerging-issues>>

ACMA, 'Community research on informed consent' (2011 accessed 4 Jul 2016)

<<http://www.acma.gov.au/theACMA/informed-consent-research>>.

ACMA, Privacy and personal data—Emerging issues in media and communications, Occasional Paper 4 (June 2013) <  
<http://www.acma.gov.au/~media/Regulatory%20Frameworks%20and%20International%20Engagement/Information/pdf/Privacy%20and%20digital%20data%20protection%20Occasional%20paper%204.pdf>>

ACMA, 'Report 2 – Australia's Progress in the Digital Economy: Participation Trust and Confidence' (2012 accessed 13 July 2014) [25]  
<[http://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=>](http://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=)

### **Australian Competition and Consumer Commission (ACCC)**

ACCC, 'Review of the Australian product safety recalls system' (2010 accessed 3 Apr 2016)  
<<https://www.accc.gov.au/system/files/Review%20of%20the%20Australian%20product%20safety%20recalls%20system.pdf>>

ACCC, 'Guidelines for developing effective voluntary industry codes of conduct' (31 Aug 2011 accessed 2 Feb 2016) < <https://www.accc.gov.au/publications/guidelines-for-developing-effective-voluntary-industry-codes-of-conduct>>

ACCC, 'Guidelines for developing effective voluntary industry codes of conduct' (31 Aug 2011 accessed 2 Aug 2016) <<https://www.accc.gov.au/publications/guidelines-for-developing-effective-voluntary-industry-codes-of-conduct>>

ACCC, 'Unfair Contract Terms Review' (2013 accessed 2 Feb 2016)  
<<https://www.accc.gov.au/system/files/Unfair%20Contract%20Terms%20-%20Industry%20Report.pdf>>

ACCC, 'Product Safety: A Guide to Testing' (Oct 2013 accessed 2 Aug 2016)  
<https://www.accc.gov.au/publications/a-guide-to-testing-product-safety>

ACCC, 'Reinvigorating Australia's Competition Policy – ACCC Submission to the Competition Policy Review (Harper Enquiry)' (26 Nov 2014 accessed 8 Aug 2016) <  
<https://www.accc.gov.au/system/files/Competition-Policy-Review-ACCC-submission-to-Draft-Report-26-November-2014.pdf>>

ACCC, 'ACCC Submission in the draft revised Telecommunications Consumer Protections Industry Code' (Nov 2014 accessed 4 Jul 2016) <<https://www.accc.gov.au/about-us/consultations-submissions/accc-submissions>>

ACCC, 'ACCC takes action against LG for alleged false or misleading representations relating to consumer guarantees' Media release (15 Dec 2015 accessed 2 Feb 2016)  
<<https://www.accc.gov.au/media-release/accc-takes-action-against-lg-for-alleged-false-or-misleading-representations-relating-to-consumer-guarantees>>

ACCC, 'Product Safety Australia' (2016 accessed 17 Aug 2016) [www.recalls.gov.au](http://www.recalls.gov.au)

ACCC, 'Guidelines – Use of section 155 powers' (Sept 2016 accessed 5 Set 2016)  
[http://www.accc.gov.au/system/files/1119\\_ACCC%20Guidelines-use%20of%20section%20155%20powers\\_FA.PDF](http://www.accc.gov.au/system/files/1119_ACCC%20Guidelines-use%20of%20section%20155%20powers_FA.PDF)

ACCC, 'ACCC takes action against Volkswagen over diesel emission claims' Press Release (1 Sept 2016 accessed 4 Sept 2016) < <https://www.accc.gov.au/media-release/accc-takes-action-against-volkswagen-over-diesel-emission-claims>>

ACCC, 'ACCC and AER Corporate Plan 2015- 16' <<https://www.accc.gov.au/publications/corporate-plan-priorities/corporate-plan-priorities-2015-16>>

ACCC, '2016 ACCC Compliance and Enforcement Policy' (Feb 2016 accessed 3 Mar 2016) < [http://www.accc.gov.au/system/files/2016%20ACCC%20Compliance%20and%20Enforcement%20Policy\\_0.pdf](http://www.accc.gov.au/system/files/2016%20ACCC%20Compliance%20and%20Enforcement%20Policy_0.pdf)>

ACCC, 'Federal Court finds Valve made misleading representations about consumer guarantees' Media Release (29 Mar 2016 accessed 11 Apr 2016) < <http://www.accc.gov.au/media-release/federal-court-finds-valve-made-misleading-representations-about-consumer-guarantees>>

ACCC, 'ACCC appeals \$1.7m penalty against Reckitt Benckiser for misleading Nurofen representations' Media Release (23 May 2016 accessed 23 May 2016) < <https://www.accc.gov.au/media-release/accc-appeals-17m-penalty-against-reckitt-benckiser-for-misleading-nurofen-representations>>

ACCC, 'The Australian Competition and Consumer Commission's accountability framework for investigations' (2016 accessed 2 Jun 2016) <<https://foi.accc.gov.au/sites/foi.accc.gov.au/files/repository/ACCC%27s%20accountability%20framework%20for%20investigations.pdf>>

ACCC, 'Australian Consumer Law Review Interim Report' (Oct 2016 accessed 8 Oct 2016) <http://consumerlaw.gov.au/review-of-the-australian-consumer-law/have-your-say/>

ACCC, 'Unfair Terms On Small Business Contracts' (10 Nov 2016 accessed 10 Nov 2016) <[http://accc.gov.au/system/files/B2B%20UCT%20-%20Final%20-%20Unfair%20terms%20in%20small%20business%20contracts%20%20A%20review%20of%20selected%20industries\\_0.PDF](http://accc.gov.au/system/files/B2B%20UCT%20-%20Final%20-%20Unfair%20terms%20in%20small%20business%20contracts%20%20A%20review%20of%20selected%20industries_0.PDF)>

ACCC, 'ACCC welcomes Virgin Australia's move to stop pre-selecting travel insurance' Media release (1 Dec 2016 accessed 1 Dec 2016) <<http://www.accc.gov.au/media-release/accc-welcomes-virgin-australia-s-move-to-stop-pre-selecting-travel-insurance>>

ACCC, 'ACCC takes action against MSY alleging misrepresentation of consumer guarantees' Media release (1 Dec 2016 accessed 1 Dec 2016) < <http://www.accc.gov.au/media-release/accc-takes-action-against-msy-alleging-misrepresentation-of-consumer-guarantees>>

ACCC, 'Australian Consumer Law' (Jan 2017 accessed 2 Feb 2017) < <https://www.accc.gov.au/system/files/Copy%20of%20%28CD-17-49038%29%20-%20ACL%20Compliance%20%26%20Enforcement%20guide%20%28web%29.PDF>>

ACCC, 'ACCC cross-appeals Valve Federal Court judgment' *Media Release* (7 Mar 2017 accessed 8 Mar 2017) <<https://www.accc.gov.au/media-release/accc-cross-appeals-valve-federal-court-judgment>>

ACCC, 'Unfair contract terms under scrutiny' Media Release (28 Mar 2017 accessed 28 Mar 2017) <<http://www.accc.gov.au/media-release/unfair-contract-terms-under-scrutiny>>

ACCC, 'ACCC takes action against Apple over alleged misleading consumer guarantee representations' (6 Apr 2017 accessed 6 Apr 2017) < <https://www.accc.gov.au/media-release/accc-takes-action-against-apple-over-alleged-misleading-consumer-guarantee-representations>>

Australian Communications Consumer Action Network, 'Australian Consumer Law Review Submission by ACCAN' (May 2016 accessed 20 Aug 2016)  
<[http://consumerlaw.gov.au/files/2016/07/Australian\\_Communications\\_Consumer\\_Action\\_Network.pdf](http://consumerlaw.gov.au/files/2016/07/Australian_Communications_Consumer_Action_Network.pdf)>  
>Australian Cyber Security Centre (**ACSC**), '2015 Threat Report' (2015 accessed 9 Mar 2016)  
<[https://acsc.gov.au/publications/ACSC\\_Threat\\_Report\\_2015.pdf](https://acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf)>

Australian Federal Police, 'High Tech Crime' (n.d. accessed 2 Jun 2016) <https://www.afp.gov.au/what-we-do/crime-types/cybercrime/high-tech-crime#computer-intrusions>

Australian Government, 'Consumer Policy in Australia: A companion to the OECD consumer policy toolkit' (Mar 2011 accessed 2 Jan 2016)  
<[http://consumerlaw.gov.au/files/2015/09/Companion\\_to\\_OECD\\_Toolkit.pdf](http://consumerlaw.gov.au/files/2015/09/Companion_to_OECD_Toolkit.pdf)>

Australian Government, Attorney-General's Department, 'Departmental submission Inquiry into the comprehensive revision of the Telecommunications (Interception and Access) Act 1979', Senate Legal and Constitutional Affairs References Committee' (2016 accessed 5 Mar 2017)  
<[http://www.agps.gov.au/Parliamentary\\_Business/Committees/Senate/Legal\\_and\\_Constitutional\\_Affairs/Comprehensive\\_revision\\_of\\_TIA\\_Act](http://www.agps.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act)>

Australian Government Information Management Office, 'Negotiating the Cloud – Legal Issues in Cloud Computing Agreements Better Practice Guide' *Department of Finance and Deregulation* (Feb 2013 accessed 26 July 2014) [4] <<http://www.finance.gov.au/files/2013/02/negotiating-the-cloud-legal-issues-in-cloud-computing-agreements-v1.1.pdf>>

Australian Government, 'Regulator performance framework' (2014 accessed 29 Nov 2016)  
<[https://www.cuttingredtape.gov.au/sites/default/files/files/Regulator\\_Performance\\_Framework2.pdf](https://www.cuttingredtape.gov.au/sites/default/files/files/Regulator_Performance_Framework2.pdf)>

Australian Government and ACCC, 'Product Safety Australia' (n.d. accessed 6 Mar 2017)  
<<http://www.productsafety.gov.au/recalls?source=recalls>>

Australian Government Solicitor, 'Australian Consumer Law' *Fact Sheet No. 12* (March 2011 accessed 28 June 2014) <[http://www.agps.gov.au/publications/fact-sheets/Fact\\_sheet\\_No\\_12.pdf](http://www.agps.gov.au/publications/fact-sheets/Fact_sheet_No_12.pdf)>

Australian Government, 'Exposure Draft (30 Nov 2015) *Privacy Amendment (Notification of Serious Data Breaches Bill 2015*' <<https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Privacy-Amendment-Notification-of-Serious-Data-Breaches-Bill-2015-December-2015-exposure-draft.pdf>>

Australian Government, 'Serious data breach notification' *Consultation* (2015 accessed 2 Mar 2016)  
<<https://www.ag.gov.au/Consultations/Pages/serious-data-breach-notification.aspx>>

Australian Government, 'The Australian Government Guide to Regulation' *Dept. of Premier & Cabinet* (2015 accessed 2 Mar 2016) <  
[http://cuttingredtape.gov.au/sites/default/files/files/Australian\\_Government\\_Guide\\_to\\_Regulation.pdf](http://cuttingredtape.gov.au/sites/default/files/files/Australian_Government_Guide_to_Regulation.pdf)>

Australian Government, 'Australia's Cyber Security Strategy' (2016 accessed 22 Apr 2016) <<https://cybersecuritystrategy.dpmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf>>

Australian Government, 'Australian Consumer Survey 2011' Sweeney Research (2011 accessed 22 Oct 2015) [http://consumerlaw.gov.au/files/2015/09/Australian\\_Consumer\\_Survey\\_Report.pdf](http://consumerlaw.gov.au/files/2015/09/Australian_Consumer_Survey_Report.pdf)

Australian Government, 'Standard on Assurance Engagements ASAE 3001 *Compliance Engagements*', Auditing and Assurance Standards Board (Sept 2008 accessed 4 Jan 2015) <[www.auasb.gov.au/admin/file/content1023/c3/asae\\_3100\\_9-09-08.pdf](http://www.auasb.gov.au/admin/file/content1023/c3/asae_3100_9-09-08.pdf)>

Australian Government, 'Australian Government Public Data Policy Statement' (7 Dec 2015 accessed 30 May 2016) <<https://www.dpmc.gov.au/sites/default/files/publications/open-government-nap-consultation-print.pdf>>

Australian Government, Department of Communications and the Arts, 'Cloud Computing Regulatory Stock Take Report' (21 Jan 2014 accessed 2 Jan 2016) <<https://www.communications.gov.au/publications/cloud-computing-regulatory-stock-take-report%C2%A0>>

Australian Government, 'Review of whether there should be exceptions to the prohibition on civil litigant access to retained telecommunications data' (Apr 2017 accessed 2 May 2017) <<https://www.ag.gov.au/Consultations/Documents/Access-to-telecommunications-data/Review-civil-litigant-access-to-retained-telecommunications-data.pdf>>

Australian Human Rights Commission, 'A Quick Guide to Australian Discrimination Laws' (2014 accessed 8 Aug 2016) <https://www.humanrights.gov.au/employers/good-practice-good-business-factsheets/quick-guide-australian-discrimination-laws>

Australian IOT Alliance, 'IoT Security Guideline V1.0' (Feb 2017 accessed 2 Mar 2017): 17- 18 <<https://static1.squarespace.com/static/573853ed1d07c093e27aefd2/t/58ab9bf8ebbd1a2b74e2aa2d/1487641596432/IoTAA+Security+Guideline+V1.0.pdf>>

Australian Labor Party, 'National Information Policy' *Fact Sheet* (date accessed 4 Jun 2016) <[https://d3n8a8pro7vnmx.cloudfront.net/australianlaborparty/pages/4638/attachments/original/1449467663/NationalInformationPolicy\\_FINAL.pdf?1449467663](https://d3n8a8pro7vnmx.cloudfront.net/australianlaborparty/pages/4638/attachments/original/1449467663/NationalInformationPolicy_FINAL.pdf?1449467663)>

Australian Labor Party, 'Submission to the Productivity Commission ACL Review' (Oct 2016 accessed 12 Oct 2016) <[http://www.pc.gov.au/\\_\\_data/assets/pdf\\_file/0010/206938/sub001-consumer-law.pdf](http://www.pc.gov.au/__data/assets/pdf_file/0010/206938/sub001-consumer-law.pdf)>

### **Australian Law Reform Commission (ALRC)**

ALRC, 'For Your information: Australian Privacy Law and Practice Report' Volume 1 (2008 accessed 20 Nov 2015) <[http://www.alrc.gov.au/sites/default/files/pdfs/108\\_vol1.pdf](http://www.alrc.gov.au/sites/default/files/pdfs/108_vol1.pdf)>

ALRC, Serious Invasions of Privacy in the Digital Era, Discussion Paper No 80 (2014) <[http://www.alrc.gov.au/sites/default/files/pdfs/publications/whole\\_dp80.pdf](http://www.alrc.gov.au/sites/default/files/pdfs/publications/whole_dp80.pdf)>

ALRC, Serious Invasions of Privacy in the Digital Era, Discussion Paper No 80 (2014) <<http://www.alrc.gov.au/publications/serious-invasions-privacy-dp-80>>

ALRC, 'Serious Invasions of Privacy in the Digital Era' *ALRC Report No 123* (Mar 2014 accessed 10 Dec 2016) <https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123>

ALRC, 'Serious Invasions of Privacy in the Digital Era' *Final Report* (June 2014 accessed 3 Apr 2015) <<https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123>>

ALRC, 'Serious Invasions of Privacy in the Digital Era' *Summary Report No 123* (Mar 2014 accessed 10 Dec 2016) <https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123>>

ALRC, 'Executive Summary' ALRC Report 108 (2008 accessed 20 Apr 2015) <<http://www.alrc.gov.au/publications/Executive%20Summary/extensive-public-engagement#>>

Australian National Data Service, 'De-identification' *ANDS Guide* (11 Jan 2017 accessed 2 Feb 2017) <<http://www.ands.org.au/working-with-data/sensitive-data/de-identifying-data.>>

### **Australian Securities and Investments Commission (ASIC)**

ASIC, 'Senate enquiry into the performance of the Australian Securities and Investment Commission – Submission by ASIC on reforms to the credit industry and 'low doc' loans', (Oct 2013 accessed 20 Jan 2016) <<http://download.asic.gov.au/media/1311541/ASIC-Submission-on-credit-reform--to-Senate-inquiry.pdf>>

ASIC, 'Cyber Resilience: Health Check' *Report No. 429* (Mar 2015 accessed 4 Jan 2016) <<http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf>>

Australian Transport, 'National Road Safety Strategy 2011- 2020: Implementation Status Report 2015' (2011 accessed 22 Aug 2016) <[http://roadsafety.gov.au/performance/files/NRSS\\_Implementation\\_report\\_Nov2015.pdf](http://roadsafety.gov.au/performance/files/NRSS_Implementation_report_Nov2015.pdf)>

Austroroads, 'Governments told to be ready for start of driverless revolution by 2020' (24 August 2016 accessed 28 Aug 2016) <<http://www.austroroads.com.au/news-events/item/363-governments-told-to-be-ready-for-start-of-driverless-revolution-by-2020?tmpl=component&print=1>>

Auto Alliance, 'Statement before the Energy and Commerce Committee, Subcommittee on Commerce, Manufacturing and Trade, US House of Representatives' (21 Oct 2015 accessed 6 May 2016) <<http://www.energy.senate.gov/public/index.cfm/2016/1/hearing-is-to-examine-the-status-of-innovative-technologies-within-the-automotive-industry>>

Auto Alliance, 'Automakers Announce Initiative to Further Enhance Cyber-Security in Autos' (14 Jul 2015 accessed 6 May 2016) <<http://www.autoalliance.org/index.cfm?objectid=8D04F310-2A45-11E5-9002000C296BA163>>

Auto Alliance, 'Remarks from Vice President for Vehicle Safety at the Alliance of Automobile Manufacturers, Rob Strassburger', CyberAuto Press Conference Call (14 Jul 2015 accessed 6 May 2016) <<http://www.autoalliance.org/index.cfm?objectid=6AF42290-2A46-11E5-9002000C296BA163>>

Auto Alliance, 'Framework for Automotive Cybersecurity Best Practices' (19 Jan 2016 accessed 2 Mar 2016) <http://www.autoalliance.org/index.cfm?objectid=1E518FB0-BEC3-11E5-9500000C296BA163>

Auto Alliance, 'Comments of the Association of Global Automakers Concerning the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things', Docket No. 160331306-6306-01  
<[https://www.ntia.doc.gov/files/ntia/publications/comments\\_aga\\_on\\_ntia\\_iiot\\_request\\_for\\_comments.pdf](https://www.ntia.doc.gov/files/ntia/publications/comments_aga_on_ntia_iiot_request_for_comments.pdf)>

Autoblog, 'GM claims that it owns your car's software' (20 May 2015 accessed 12 Nov 2016)  
<<http://www.autoblog.com/2015/05/20/general-motors-says-owns-your-car-software/>>

Automotive Information Sharing and Analysis Center (**Auto-ISAC**), 'Automotive Cybersecurity Best Practices' *Executive Summary* (21 July 2016 accessed 2 Aug 2016) <  
<https://www.automotiveisac.com/best-practices/>>

## B

Baig, Edward C., 'Personal digital assistants are on the rise (and they want to talk)' *USA TODAY* (9 May 2016 accessed 22 May 2016)  
<<http://www.usatoday.com/story/tech/columnist/baig/2016/05/08/personal-digital-assistants-rise-and-they-want-talk/83715794/>>

Bailey, M. W., 'Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things' *Texas Law Review*, 2016 Apr, Vol.94(5), pp.1023-1054

Baker & McKenzie, 'Global Privacy Handbook' (2015 accessed 15 May 2016)  
[http://f.datasrvr.com/fr1/715/56640/2016\\_Global\\_Privacy\\_Handbook.pdf](http://f.datasrvr.com/fr1/715/56640/2016_Global_Privacy_Handbook.pdf)

Baker & McKenzie, 'Internet of Things: Some Legal and Regulatory Implications' (Feb 2016 accessed 16 Mar 2016)  
<[http://www.bakermckenzie.com/files/Uploads/Documents/Australia/ar\\_australia\\_internetofthings\\_feb16.pdf](http://www.bakermckenzie.com/files/Uploads/Documents/Australia/ar_australia_internetofthings_feb16.pdf)>

Banks, Timothy M. and Karl Schober, 'Data Security And Cybercrime In Canada' *Dentons* (25 Sept 2016 accessed 2 Oct 2016) <<http://www.lexology.com/library/detail.aspx?g=237135ad-df34-4e79-87fa-554b3dfdc7fa>>

Barber, C. Ryan, 'Tech Giants, Carmakers Rev Up Lobbying on Autonomous Vehicles' *The National Law Journal* (1 May 2017 accessed 1 May 2017) <  
[http://www.nationallawjournal.com/id=1202784940586/Tech-Giants-Carmakers-Rev-Up-Lobbying-on-Autonomous-Vehicles?cmp=share\\_twitter](http://www.nationallawjournal.com/id=1202784940586/Tech-Giants-Carmakers-Rev-Up-Lobbying-on-Autonomous-Vehicles?cmp=share_twitter)>

Barcena, M. B. & Candid Wueest, 'Insecurity in the Internet of Things' *Symantec* (12 Mar 2015 accessed 23 Mar 2016) <  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/insecurity-in-the-internet-of-things.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/insecurity-in-the-internet-of-things.pdf)>

Bar-Gill, Charles Oren, 'Seduction by Contract: Law, Economics, and Psychology in Consumer Markets', (2012)  
<<http://www.oxfordscholarship.com.ezproxy.bond.edu.au/view/10.1093/acprof:oso/9780199663361.001.0001/acprof-9780199663361>>

Barker, Colin, '25 billion connected devices by 2020 to build the Internet of Things' *ZDNet* (11 Nov 2014 accessed 5 Mar 2016) <<http://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-internet-of-things/>>

Barratt, James 'Why Stephen Hawking and Bill Gates Are Terrified of Artificial Intelligence' *Huffington Post* (9 Sept 2015 accessed 25 May 2016) <[http://www.huffingtonpost.com/james-barratt/hawking-gates-artificial-intelligence\\_b\\_7008706.html](http://www.huffingtonpost.com/james-barratt/hawking-gates-artificial-intelligence_b_7008706.html)>

Batchelor, Bill & Grant Murray, 'Internet of Things: Antitrust Concerns in The Pipeline?' *Kluwer Competition Law Blog* (12 May 2016 Accessed 2 Aug 2016) <http://kluwercompetitionlawblog.com/2016/05/12/internet-of-things-antitrust-concerns-in-the-pipeline/>>

Bauer, Harald, Mark Patel & Jan Veira, 'The Internet of Things: Sizing up the opportunity' *McKinsey & Company* (accessed 3 Apr 2016) <<http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity>>

BBC News, 'Fridge sends spam emails as attack hits smart gadgets' (17 Jan 2014 accessed 6 Apr 2016) <<http://www.bbc.com/news/technology-25780908>>

BBC, 'Apple stops selling Nest products in its US stores' (24 Jul 2015 accessed 2 Jun 2016) <http://www.bbc.com/news/technology-33655417>

BBC, 'Johnson & Johnson says insulin pump 'could be hacked"' (4 Oct 2016 accessed 6 Oct 2016) <<http://www.bbc.com/news/business-37551633>>

BBC News, 'Boy, 17, admits TalkTalk hacking offences' (15 Nov 2016 accessed 16 Nov 2016) <<http://www.bbc.com/news/uk-37990246>>

BBVA, 'Smart contracts: the ultimate automation of trust?' *Digital Economy Outlook* (Oct 2015 accessed 25 Apr 2016) <[https://www.bbvaesearch.com/wp-content/uploads/2015/10/Digital\\_Economy\\_Outlook\\_Oct15\\_Cap1.pdf](https://www.bbvaesearch.com/wp-content/uploads/2015/10/Digital_Economy_Outlook_Oct15_Cap1.pdf)>

Belay, Nick, 'Robot Ethics and Self-Driving Cars: How Ethical Determinations in Software Will Require a New Legal Framework' (2015) 40 *Journal of the Legal Profession* 119

Belle Isle, Jay W., 'Claybrook: DOT's "Proactive" Safety Principles Worthless' *Legal Reader* (18 Jan 2016 accessed 2 Jun 2016) <<http://www.legalreader.com/claybrook-dots-proactive-safety-principles-worthless/>>

Benady, David, 'Online marketplaces, Uberisation and business models of tomorrow' *Raconteur, The Times* (28 January 2016 accessed 1 Feb 2016) <<http://raconteur.net/business/online-marketplaces-uberisation-and-business-models-of-tomorrow>>

Benjamin, Alison, 'Tech innovations that could improve lives in 2015' *The Guardian (UK)* (7 Jan 2015 accessed 14 Jan 2016) <<http://www.theguardian.com/society/2015/jan/07/tech-innovations-improve-lives-social-impact>>

Bertoncella, Michele and Dominik Wee, 'Ten ways autonomous driving could redefine the automotive world' *McKinsey & Company* (June 2015 accessed 4 Apr 2016)

<<http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/ten-ways-autonomous-driving-could-redefine-the-automotive-world>>

Best, Jo, 'Who really owns your internet of things data?' *ZDNet* (11 Jan 2016 accessed 8 Apr 2016) <<http://www.zdnet.com/article/who-really-owns-your-internet-of-things-data/>>

BEUC, 'Consumer Programme 2014- 2020 Proposed Commission Regulation' (22 Mar 2012 accessed 6 Apr 2016) <<http://www.beuc.eu/publications/2012-00203-01-e.pdf>>

Bigelow, Pete, 'Nissan disables Leaf app due to hacking concerns' *autoblog* (25 Feb 2016 accessed 3 Apr 2016) <<http://www.autoblog.com/2016/02/25/nissanconnect-ev-leaf-app-hacking-followup/>>

Bigelow, Pete, 'Jeep in St. Louis hacked from Pittsburgh' *autoblog* (21 Jul 2016 accessed 3 Sept 2016) <<http://www.autoblog.com/2015/07/21/jeep-cherokee-hacked/>>

Bilton, Nick, 'Keeping Your Car Safe From Electronic Thieves', *The New York Times* (Apr. 15, 2015 accessed 4 Jun 2016) <<http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html>>

Bitdefender Channel, 'The Cloud Dilemma - Is Your Cloud Provider Secure?' (31 Mar 2016 accessed 4 Apr 2016) <<http://www.itbestofbreed.com/sponsors/bitdefender/best-tech/cloud-dilemma-your-cloud-provider-secure>>

Black, J., *Principles Based Regulation: Risks, Challenges and Opportunities* (2007) London School of Economics and Political Science, 10.

Blincoe, L. J., T.R. Miller, E. Zaloshnja & B.A. Lawrence, 'The Economic and Societal Impact of Motor Vehicle Crashes, 2010' *National Highway Traffic Safety Administration* (Revised May 2015) (Report No. DOT HS 812 013). Washington, DC <<https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812013>>

Blumenthal, Eli and Elizabeth Weise, 'Hacked home devices caused massive Internet outage', *USA TODAY* (21 Oct. 2016 accessed 22 Oct. 2016) <<https://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/>>

Bogost, Ian, 'The Internet of Things You Don't Really Need' *The Atlantic* (23 June 2015 accessed 2 Apr 2016) <<http://www.theatlantic.com/technology/archive/2015/06/the-internet-of-things-you-dont-really-need/396485/>>

Bojanova, Irena, 'Hacking IoT' *IEEE Computer Society* (12 Feb 2015 accessed 21 Mar 2016) <<https://www.computer.org/portal/web/sensing-iot/content?g=53926943&type=article&urlTitle=hacking-iot>>

Bojanova, Irena, 'Defining the Internet of Things' *IEEE Computer Society* (15 Mar 2015 accessed 21 Mar 2016) <<https://www.computer.org/web/sensing-iot/content?g=53926943&type=article&urlTitle=defining-the-internet-of-things>>

Bojanova, Irena, 'Defining the Internet of Things' *IEEE Computer Society* (16 Mar 2016 accessed 21 Mar 2016) <<https://www.computer.org/web/sensing-iot/content?g=53926943&type=article&urlTitle=defining-the-internet-of-things> >

Bojanova, Irena, 'Primitives and Elements of IOT Trustworthiness' *IEEE Computer Society* (16 Mar 2016 accessed 21 Mar 2016) <https://www.computer.org/portal/web/sensing-iot/content?g=53926943&type=article&urlTitle=primitives-and-elements-of-iot-trustworthiness>

Bojanova, Irena, 'What makes up the Internet of Things' *IEEE Computer Society* (31 Mar 2015 accessed 21 Mar 2016) <<https://www.computer.org/portal/web/sensing-iot/content?g=53926943&type=article&urlTitle=what-are-the-components-of-iot-> >

Bojanova, Irena, 'IoT and the ever-expanding web' *IEEE Computer Society* (14 Jul 2015 accessed 21 Mar 2016) <<https://www.computer.org/portal/web/sensing-iot/content?g=53926943&type=article&urlTitle=iot-and-the-ever-expanding-web->>

Bojanova, Irena, 'IoT Frameworks Products and Solutions' *IEEE Computer Society* (3 Dec 2015 accessed 21 Mar 2016) <<https://www.computer.org/portal/web/sensing-iot/content?g=53926943&type=article&urlTitle=iot-frameworks-products-and-solutions>>

Bojanova, Irena, 'IoT Standardisation It's a War' *IEEE Computer Society* (3 Dec 2015 accessed 21 Mar 2016) < <https://www.computer.org/portal/web/sensing-iot/content?g=53926943&type=article&urlTitle=iot-standardization-it-s-a-war>

Bonnington, Christina, 'Data from Wearables is Now Courtroom Fodder' *Wired* (12 Dec 2014 accessed 6 Apr 2016) <<http://www.wired.com/2014/12/wearables-in-court/>>

Booz Allen Hamilton, 'Submission to the National Telecommunications Administration and Information Administration' Response to Request for Comment (June 2, 2016 accessed 20 Jul 2016) <[https://www.boozallen.com/content/dam/boozallen/prod/internet-of-things/assets/booz\\_allen\\_hamilton\\_response\\_final.pdf](https://www.boozallen.com/content/dam/boozallen/prod/internet-of-things/assets/booz_allen_hamilton_response_final.pdf)>

Borowiec, Steven 'Google's AlphaGo AI defeats human in first game of Go contest', *The Guardian* (9 Mar 2016 accessed 9 Mar 2016) <<http://www.theguardian.com/technology/2016/mar/09/google-deepmind-alphago-ai-defeats-human-lee-sedol-first-game-go>>

Bose Australia, 'A message to our Bose Connect App customers' (20, 23 and 25 Apr 2016) <[https://www.bose.com.au/en\\_au/landing\\_pages/bose\\_corporation\\_updates.html](https://www.bose.com.au/en_au/landing_pages/bose_corporation_updates.html)>

Boston Consulting Group, 'The Value of our Digital Identity' *Liberty Global* (Nov 2012 accessed 2 Feb 2016) <[https://www.bcgperspectives.com/content/articles/digital\\_economy\\_consumer\\_insight\\_value\\_of\\_our\\_digital\\_identity/](https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/)>

Boston, William, 'Emissions Cases Against VW Heating Up Around the Globe' *Morningstar Dow Jones* (23 Aug 2016 accessed 10 Sept 2016) < <http://www.news.com.au/technology/innovation/motoring/volkswagen-back-in-federal-court-over-diesel-emissions-scandal/news-story/d6b4f88cb2502c896e715cc7a6daf0b9>>

Boudette, Neal, '5 Things That Give Self-Driving Cars Headaches' *The New York Times* (4 Jun 2016 Accessed 16 Oct 2016) < <http://www.nytimes.com/interactive/2016/06/06/automobiles/autonomous-cars-problems.html>>

Boudette, Neal E., 'Tesla Faults Brakes, but Not Autopilot, in Fatal Crash' *The New York Times* (29 Jul 2016 accessed 2 Aug 2016) < [http://www.nytimes.com/2016/07/30/business/tesla-faults-teslas-brakes-but-not-autopilot-in-fatal-crash.html?\\_r=0](http://www.nytimes.com/2016/07/30/business/tesla-faults-teslas-brakes-but-not-autopilot-in-fatal-crash.html?_r=0)>

Boudette, Neal, 'Autopilot Cited in Death of Chinese Tesla Driver' *The New York Times* (14 Sept 2016 accessed 16 Oct 2016) < [http://www.nytimes.com/2016/09/15/business/fatal-tesla-crash-in-china-involved-autopilot-government-tv-says.html?\\_r=0](http://www.nytimes.com/2016/09/15/business/fatal-tesla-crash-in-china-involved-autopilot-government-tv-says.html?_r=0)>

Bourne, Jason, 'One in three cloud services was susceptible to Heartbleed, research shows' *Cloudtech* (12 May 2014 accessed 7 June 2014) <http://www.cloudcomputing-news.net/news/2014/may/12/one-three-cloud-services-was-susceptible-heartbleed-research-shows/>

Bowles, Nellie 'Google self-driving car collides with bus in California, accident report says' *The Guardian* (1 Mar 2016 accessed 1 Mar 2016) <[http://www.theguardian.com/technology/2016/feb/29/google-self-driving-car-accident-california?utm\\_source=esp&utm\\_medium=Email&utm\\_campaign=GU+Today+main+NEW+H&utm\\_term=159420&subid=18035608&CMP=EMCNEWEML661912](http://www.theguardian.com/technology/2016/feb/29/google-self-driving-car-accident-california?utm_source=esp&utm_medium=Email&utm_campaign=GU+Today+main+NEW+H&utm_term=159420&subid=18035608&CMP=EMCNEWEML661912)>

Bowles, Nellie, 'Uber, Google and others form self-driving car lobby to shape US policy' *The Guardian* (27 Apr 2016 accessed 2 May 2016) < <https://www.theguardian.com/technology/2016/apr/26/uber-google-lyft-ford-volvo-self-driving-car-lobby>>

Brachman, Steve, 'John Deere, GM push back against consumer modifications of vehicle software' *IPWatchdog* (1 Jul 2015 accessed 3 Jul 2016) <<http://www.ipwatchdog.com/2015/07/01/john-deere-gm-push-back-against-vonsumer-modifications-on-vehicle-software>>

Bracy, Jedidiah, 'The IoT Zombies are already at your front door' *Privacy Tech* (29 Sept 2016 accessed 2 Oct 2016) <<https://iapp.org/news/a/how-poorly-secured-iot-devices-can-take-down-your-website/>>

Bracy, Jedidiah, 'On Building Consumer-Friendly Privacy Notices for the IoT' *Privacy Tech* (6 Nov 2015 accessed 29 Apr 2016) <<https://iapp.org/news/a/on-building-consumer-friendly-privacy-notices-for-the-iot/>>

Bradshaw, Stephen, 'Hacking for good- What is security testing?' *Australian Govt Digital Transformation Agency Blog* (2 Mar 2017 accessed 3 Mar 2017) <<https://www.dta.gov.au/blog/what-is-security-testing/>>

Branch, Phillip, 'How will data retention laws cope with the Internet of things?' *The Conversation* (2 Feb 2015 accessed 13 Apr 2016) <<https://theconversation.com/how-will-data-retention-laws-cope-with-the-internet-of-things-36885>>

Branch, Phillip, 'Are we ready for a world even more connected to the internet of things' *The Conversation* (20 Nov 2015 accessed 3 Mar 2016) <<http://theconversation.com/are-we-ready-for-a-world-even-more-connected-in-the-internet-of-things-50889>>

Brandis, Senator George, 'Amendment to the Privacy Act to Further Protect De-Identified Data' *Media Release* (28 Sept 2016 accessed 29 Sept 2016)  
<<https://www.attorneygeneral.gov.au/Mediareleases/Pages/2016/ThirdQuarter/Amendment-to-the-Privacy-Act-to-further-protect-de-identified-data.aspx>>

Brandom, Russell, 'Google backs off on previously announced Allo privacy feature' *THE VERGE* (21 Sept 2016 accessed 2 Nov 2016) <<http://www.theverge.com/2016/9/21/12994362/allo-privacy-message-logs-google>>

Breathometer, 'Privacy Policy' (11 Oct 2012 accessed 10 Mar 2016)  
<https://www.breathometer.com/legal/privacy-policy>

Breathometer, 'Terms & Conditions' (n.d. accessed 10 Mar 2016)  
<https://www.breathometer.com/legal/terms-of-use>

Briedis, Mark, Jane Webb & Michael Fraser, 'Improving the Communication of Privacy Information for Consumers' *ACCAN & UTS* (Feb 2016 accessed 2 Oct 2016)  
<http://accan.org.au/files/Grants/Improving%20Comm%20Privacy%20Info-full-accessible.pdf>

Brill, Julie 'The Internet of Things: From Regulators, Guidance and Enforcement', *The New York Times* (8 September 8, 2013 accessed 28 Feb 2016) <<https://www.ftc.gov/public-statements/2013/09/internet-things-regulators-guidance-enforcement>>

Brill, Julie, 'The Internet of Things: Building Trust and Maximizing Benefits through Consumer Control' *Fordham Law Review* (2014) 83: 1 205- 217 (26 Feb 2014 accessed 28 Feb 2016)  
<[https://www.ftc.gov/system/files/documents/public\\_statements/289531/140314fordhamprivacyspeech.pdf](https://www.ftc.gov/system/files/documents/public_statements/289531/140314fordhamprivacyspeech.pdf)>

Brill, Julie, 'Privacy and Data Security in the Age of Big Data and the Internet of Things' *Keynote Address at Washington Governor Jay Inslee's Cyber Security and Privacy Summit* (7 January 2016 accessed 28 Feb 2016) <<https://www.ftc.gov/public-statements/2016/01/privacy-data-security-age-big-data-internet-things>>

Brill, Julie, 'One Year Later: Privacy and Data Security in a World of Big Data, the Internet of Things, and Global Data Flows'  
*Keynote Address Before the USCIB/BIAC/OECD Conference on Promoting Inclusive Growth in the Digital Economy* (10 March 2015 accessed 28 Feb 2016)  
<[https://www.ftc.gov/system/files/documents/public\\_statements/629691/150310uscibremarks.pdf](https://www.ftc.gov/system/files/documents/public_statements/629691/150310uscibremarks.pdf)>

Brisbane, Alex, 'Tesla's Over-the-Air Fix: Best example Yet of the Internet of Things?' *WIRED* (Nov 2016 accessed Nov 2016) < <https://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things/>>

Briscoe, Bob, Andrew Odlyzko and Benjamin Tilly, 'Metcalfe's Law is Wrong', *IEEE Spectrum* (1 Jul 2016 accessed 4 Feb 2016) <http://spectrum.ieee.org/computing/networks/metcalfes-law-is-wrong>

Brody, Paul and Veena Pureswaran, 'Device Democracy Saving the Future of the Internet of things' *IBM Institute for Business Value, Executive Report* (2015 accessed 23 Mar 2016)  
<<http://iotbusinessnews.com/download/white-papers/IBM-Saving-the-future-of-IoT.pdf>>

Brookman, Justin, 'Statement Before the Senate Committee' (11 Feb 2015 accessed 7 Mar 2016) <<https://cdt.org/resource/statement-of-justin-brookman-before-the-us-senate-committee-on-commerce-science-and-transportation/>>

Brookman, Justin, 'Eroding Trust: How New Smart TV Lacks Privacy by Design and Transparency' *iapp privacy perspectives* (27 Nov 2013 accessed 26 Apr 2016) <<https://iapp.org/news/a/eroding-trust-how-new-smart-tv-lacks-privacy-by-design-and-transparency/>>

Brown, Jennifer, 'Data fit for the Courtroom?' *Canadian Lawyer* (2 Feb 2015 accessed 6 Apr 2016) <[www.canadianlawyermag.com/5450/Data-fit-for-the-courtroom.html](http://www.canadianlawyermag.com/5450/Data-fit-for-the-courtroom.html)>

Brown, Michael, 'Edyn smart garden probe review: A promising idea that needs time to blossom' *Techhive* (23 Jun 2015 accessed 13 Jun 2016) <http://www.techhive.com/article/2939022/edyn-smart-garden-probe-review-a-promising-idea-that-falls-short-on-delivery.html>

Buchanan, Matt, 'Can Smart Design Make You Love Your Smoke Detector' *The New Yorker* (8 Oct 2013 accessed 10 Apr 2016) <<http://www.newyorker.com/tech/elements/can-smart-design-make-you-love-your-smoke-detector>>

Buesnel, Guy, 'GPS Spoofing Is Now a Real Threat – Here's What Manufacturers of GPS Devices Need to Know' *Spirent* (14 Sept. 2015 accessed 4 Jun 2016) <[http://www.spirent.com/Blogs/Positioning/2015/September/GPS\\_Spoofing\\_Is\\_a\\_Real\\_Threat](http://www.spirent.com/Blogs/Positioning/2015/September/GPS_Spoofing_Is_a_Real_Threat)>

Bugcrowd, 'Bounty Programs' (n.d. accessed 2 Mar 2017) <<https://bugcrowd.com/list-of-bug-bounty-programs>>

BuildITSecurely, 'Our Goals for the Internet of things', (n.d. accessed 7 Apr 2016) <<https://builditsecure.ly/>>

Burdon, Mark and Paul Harpur, 'Re-conceptualising Privacy and Discrimination in an Age of Talent Analytics' (2014) 37 *UNSWLJ* 679 <<http://www.austlii.edu.au/au/journals/UNSWLawJl/2014/26.html#fn1>>

Burleigh, Kate. 'Australia needs to be in vanguard of Internet of Things' *The Sydney Morning Herald* (18 Oct 2015 accessed 5 Mar 2016) <<http://www.smh.com.au/comment/australia-needs-to-be-in-vanguard-of-internet-of-things-20151016-gkau1t.html>>

Burris, Daniel, 'The Internet of Things is far bigger than anyone realises' *Wired* (Nov 2014 accessed 1 April 2016) <<http://www.wired.com/insights/2014/11/the-internet-of-things-bigger/> and Part 2 <<http://www.wired.com/insights/2014/11/iot-bigger-than-anyone-realizes-part-2/>>

BusinessWire, 'IoT Will Drive Consumer Tech Industry to \$287 Billion in Revenues, an All-Time high, According to Consumer Technology Association' *BusinessWire* (4 Jan 2016 accessed 18 Apr 2016) <<http://www.businesswire.com/news/home/20160104006598/en/IoT-Drive-Consumer-Tech-Industry-287-Billion>>

Bussemer, Thymian, Christian Krell & Henning Meyer, 'Social Democratic Values in the Digital Society' *Friedrich Ebert Stiftung, Social Europe Occasional Paper No. 10* (10 Jan 2016 accessed 10 May 2016) <<https://www.socialeurope.eu/wp-content/uploads/2016/01/OccPap10.pdf>>

Bussing, Heather 'Can law keep up with technology?' *HRExaminer* (18 Aug 2012 accessed 28 Aug 2016) <<http://www.hrexaminer.com/can-law-keep-up-with-technoogy/>>

Butler, Des, 'The Dawn of the Age of Drones: An Australian Privacy Law Perspective' 37:2 (2014) *UNSWLJ* 434- 470 <[http://www.unswlawjournal.unsw.edu.au/sites/default/files/g2\\_butler.pdf](http://www.unswlawjournal.unsw.edu.au/sites/default/files/g2_butler.pdf)>

Buttarelli, Giovanni, 'Big data, big data protection: challenges and innovative solutions' *ERA Conference on Recent Developments in Data Protection Law Keynote Speech* (11 May 2015 accessed 8 Apr 2016) <[https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-05-11\\_ERA\\_speech\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-05-11_ERA_speech_EN.pdf)>

Buttarelli, Giovanni, 'Data protection as a bulwark for digital democracy' Keynote speech at the 6<sup>th</sup> International e-Democracy 2015 Conference on Citizen rights in the world of the new computing paradigms' (10 Dec 2015 accessed 8 Apr 2016) <[https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-12-10\\_eDemocracy\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-12-10_eDemocracy_EN.pdf)>

Buttarelli, Giovanni, "Ethics at the Root of Privacy and as the Future of Data Protection" *Presentation at Harvard & MIT* (19 April 2016 accessed 4 Sept 2016) <<https://Secure.Edps.Europa.Eu/Edpsweb/Edps/Cache/Ofonce/Edps/Ethics>>

## C

Cahill, Blake, 'Successful brands of the future are building trust capital now' *The Guardian* (24 April 2014 accessed 28 Mar 2015) <<http://www.theguardian.com/media-network/media-network-blog/2014/apr/24/brands-trust-future-internet-things>>

Cameron, David. 'CeBIT Trade Fair 2014: David Cameron's Speech' (9 January 2014 accessed 5 Mar 2016) <<https://www.gov.uk/government/speeches/cebit-2014-david-camerons-speech>>

Caon, Maurizio et al, 'Wearable technologies for Automotive User interfaces: danger or opportunity' *Conference: International Conference on Automotive User Interfaces and Interactive Vehicular Applications* (29 Sept 2014 accessed 16 Mar 2016) <[https://www.researchgate.net/publication/266174301\\_Wearable\\_Technologies\\_for\\_Automotive\\_User\\_Interfaces\\_Danger\\_or\\_Opportunity](https://www.researchgate.net/publication/266174301_Wearable_Technologies_for_Automotive_User_Interfaces_Danger_or_Opportunity)>

Carlton Fields, 'NIST IoT Framework Raises Interesting Cybersecurity and Data Privacy Challenges' (23 Dec 2015 accessed 2 Jan 2016) <<http://www.lexology.com/library/detail.aspx?g=6ddd0cc7-231c-42dc-ad1c-0c226aae5091>>

Caron, Xavier, Pachellos Bosua, Sean B. Maynard and Atif Ahmad, 'The Internet of things (IoT) and its impact on individual privacy: An Australian perspective' *Computer Law and Security Review* 32 (2016) 4- 14

Carrigan, Dean, John Gallagher and Yvonne Lam, 'Controversial mandatory data retention laws passed' *Clyde & Co LLP* (30 March 2015 accessed 31 Mar 2015) <<http://www.lexology.com/library/detail.aspx?g=ef4d20da-0bd0-4045-ae8d-07b14992d6d5>>

Carragio, Gullio, 'How the IoT will change with new European regulations?' *Gaming Tech Law* <<http://www.gamingtechlaw.com/2017/01/european-iot-regulations.html>>

Carroll, Rory, 'Goodbye Privacy, Hello 'Alexa': Amazon Echo, the home robot who hears it all' *The Guardian* (21 Nov 2015 accessed 4 Mar 2016) <<https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud>>

Carter, Jamie, 'Forget smart fridges: the Industrial Internet of Things is the real revolution' *techradar.pro* (10 Mar 2015 accessed 8 Apr 2016) <<http://www.techradar.com/au/news/world-of-tech/forget-smart-fridges-the-industrial-internet-of-things-is-the-real-revolution-1287276>>

Carter Newell, 'Cyber risk update: recent security breaches' (22 Mar 2016 accessed 26 Mar 2016) <[http://www.carternewell.com/page/Publications/Archive/Cyber\\_risk\\_update\\_recent\\_security\\_breaches/](http://www.carternewell.com/page/Publications/Archive/Cyber_risk_update_recent_security_breaches/)>

Caruana, Anthony, 'Privacy Commissioner releases new Privacy Regulatory Action policy' *CSO Online* (17 Nov 2014 accessed 8 Apr 2016) <http://www.cso.com.au/article/print/559758/privacy-commissioner-releases-new-privacy-regulatory-action-policy/>

Castro, Daniel, 'The Rise of Data Poverty in America' *Center for Data Innovation* (10 Sept 2014 accessed 6 Apr 2016) <[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00035-97829.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00035-97829.pdf)>

Castro, Daniel and Joshua New, '10 Policy Principles for Unlocking the Potential of the Internet of things' *Information technology and Innovation Foundation* (4 Dec 2014 accessed 2 Jan 2016) <<http://www2.datainnovation.org/2014-iot-policy-principles.pdf>>

Castro, Daniel & Alan McQuinn, 'The Privacy Panic Cycle: A Guide to Public Fears About New Technologies' *Information Technology & Innovation Foundation* (Sept 2015 accessed 6 Apr 2016) <[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00034-97826.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00034-97826.pdf)>

Cavoukian, Anna, 'A Regulator's Perspective on Privacy by Design' (n.d. accessed 10 May 2016) <<https://fpf.org/wp-content/uploads/A-Regulators-Perspective-on-Privacy-by-Design.doc>>

Cavoukian, Anna, 'Operationalizing Privacy by Design: From Rhetoric to Reality', *Office of the Information and Privacy Commissioner* (2012 accessed 4 Mar 2016) <<http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1254>>

CDT, 'Analysis of the Consumer Privacy Bill of Rights Act' (2 Mar 2015 accessed 2 Aug 2016) <<https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act/>>

CEDA, 'Australia's Future Workforce?' (2016 accessed 2 Feb 2016) <<http://www.ceda.com.au/research-and-policy/policy-priorities/workforce>>

Center for Data Innovation, 'Comment to NTIA' (13 Mar 2016 accessed 15 Jan 2017) <<https://www.ntia.doc.gov/files/ntia/publications/cdi-comments.pdf>>

Center for Democracy & Technology and Electronic Frontier Foundation, 'Brief of Amici Curiae' (12 Nov 2014 accessed 12 Apr 2016) <<https://cdt.org/files/2014/11/FILED-Amicus-Brief-of-CDT-and-EFF.pdf>>

Center for Digital Democracy, Consumers Federation of America, Consumer Watchdog, The Electronic Privacy Information Center and U.S. PIRG, 'Letter to the Federal Trade Commissioner' (15 Feb 2017 accessed 18 Feb 2017) <<https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15-2017.pdf>>

Central Intelligence Agency, 'CIA Statement on Claims by Wikileaks ' *Statement* (8 Mar 2017 accessed 12 Mar 2017) <https://www.cia.gov/news-information/press-releases-statements/2017-press-releases-statements/cia-statement-on-claims-by-wikileaks.html>

Cha, Bonnie, 'A Beginner's Guide to Understanding the Internet of Things' *Recode* (15 Jan 2017 accessed 20 Jan 2017) <<https://www.recode.net/2015/1/15/11557782/a-beginners-guide-to-understanding-the-internet-of-things>>

Chamberlain, Bill, 'Four Ways the Internet of Things will Innovate the Retail Industry' *Forbes* (28 Dec 2015 accessed 10 Apr 2016) <<http://www.forbes.com/sites/ibm/2015/12/28/four-ways-the-internet-of-things-will-innovate-the-retail-industry/print/>>

Chang, YaPing, Xuebing Dong & Wei Sun, 'Influence of characteristics of the Internet of things on Consumer Purchase Intention' *Social Behavior & Personality* (2014) 42: 2, 321- 330

Chatfield, Tom, 'How much should we fear the rise of artificial intelligence?' *The Guardian* (18 Mar 2016 accessed 18 Mar 2016) <<https://www.theguardian.com/commentisfree/2016/mar/18/artificial-intelligence-humans-computers>>

Chin, Ying & Derek Baigent, 'The Internet of Things: Smart Objects, Not-So-Smart Users?' *Griffith Hack* (16 May 2016 accessed 19 May 2016) <<http://griffithhack.com/ideas/insights/the-internet-of-things-smart-objects-not-so-smart-users/>>

CHOICE, 'Nine hours of 'conditions apply' *Media Release* (15 Mar 2017 accessed 15 Mar 2017) <<https://www.choice.com.au/about-us/media-releases/2017/march/nine-hours-of-conditions-apply>>

CHOICE, 'Nine hours of 'conditions apply' *Media Release* (15 Mar 2017 accessed 15 Mar 2017) <<https://www.choice.com.au/about-us/media-releases/2017/march/nine-hours-of-conditions-apply>>

Chou, James, 'Data Security Playing an increasing Role in Corporate Liability' National Security Law brief, America University Washington College of Law (24 Mar 2015 accessed 22 May 20-16) <<http://www.nationalsecuritylawbrief.com/data-security-playing-an-increasing-role-in-corporate-liability/>>

Christenson, Clayton M., *The Innovator's Dilemma: The Revolutionary Book that will Change the Way You Do Business* (Collins Business Essentials) 2003.

C-ISAC, 'Automotive Cybersecurity Best Practices' (2016) <<https://www.automotiveisac.com/best-practices/>>

Cisco, 'Internet of Everything: A \$4.6 trillion Public-Sector Opportunity' *White Paper* (2013 accessed 8 Apr 2016) <[http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe\\_public\\_sector\\_vas\\_white%20paper\\_121913final.pdf](http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf)>

Cisco, 'Embracing the Internet of Everything to Capture your Share of \$14.4 trillion' *White Paper* (2013 accessed 11 Apr 2016) <[http://www.cisco.com/c/dam/en\\_us/about/ac79/docs/innov/loE\\_Economy.pdf](http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/loE_Economy.pdf)>

Cisco, 'Connected Athlete' (2015 accessed 17 Apr 2016)  
[http://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/white\\_paper\\_c11-711705.html](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/white_paper_c11-711705.html)

Cisco Systems, 'Comment to NTIA', (13 Mar 2017 accessed 15 Mar 2017) <  
[https://www.ntia.doc.gov/files/ntia/publications/cisco\\_ntia\\_supplemental\\_iot\\_comments\\_03\\_13\\_2017\\_final.pdf](https://www.ntia.doc.gov/files/ntia/publications/cisco_ntia_supplemental_iot_comments_03_13_2017_final.pdf)>

Clabby, John E & Joseph W Swanson, 'A Firewall for the Boardroom: Best Practices to Insulate Directors and Officers from Derivative Lawsuits and Related Regulatory Actions regarding Data Breaches', Corporate Accountability Report, The Bureau of National Affairs, Inc. (14 Aug 2015 accessed 5 Oct 2016) <<http://www.bna.com>>

Clabby, John E., Joseph W. Swanson & Colton M. Petersen , 'A Look at Manufacturer Liability for the Internet of Things' *Carlton Fields* (4 Oct 2016 accessed 5 Oct 2016) <<https://www.carltonfields.com/a-look-at-manufacturer-liability-for-the-internet-of-things/>>

Clark, Patrick 'Connecting the Internet of Things' *Taylor Wessing* (Feb 2014 accessed 19 Nov 2015)  
<[http://united-kingdom.taylorwessing.com/download/article\\_connecting\\_iot.html](http://united-kingdom.taylorwessing.com/download/article_connecting_iot.html)>

Claybrook, Joan, Consumer Watchdog, The Center of Auto Safety & Consumers for Auto Reliability and Safety, 'Letter to President Obama' (13 Jul 2016 accessed 2 Aug 2016) <  
<http://www.consumerwatchdog.org/resources/ltrobamaav071316.pdf>>

Clayton Utz, 'Driving into the Future: Regulating Driverless Vehicles in Australia' (17 Aug 2016 accessed 20 Aug 2016) <<http://www.lexology.com/library/detail.aspx?g=08533855-ae66-405c-b5ff-0482b99e60be>>

Clearfield, Chris 'Why the FTC Can't Regulate the Internet of Things' *Forbes* (19 Sept 2013 accessed 3 Mar 2016) < <http://www.forbes.com/sites/chrisclearfield/2013/09/18/why-the-ftc-cant-regulate-the-internet-of-things/#6bdd868453ae>>

Clinton, President W. J., 'Memorandum for the Heads of Executive Departments and Agencies' *Presidential Directive* (1 Jul 1997 accessed 2 Feb 2016)  
<<http://clinton4.nara.gov/WH/New/Commerce/directive.html>>

Cole, Bernard, 'Namedropping: the many names of the Internet of Things' *EE Times* (20 Jan 2015 accessed 22 Mar 2016) [http://www.eetimes.com/author.asp?section\\_id=36&doc\\_id=1325245](http://www.eetimes.com/author.asp?section_id=36&doc_id=1325245)

Collett, Stacey 'How to recover after a cloud computing misstep' *Computerworld* (July 1, 2014 accessed 9 July 2014)  
[http://www.computerworld.com/s/article/9248619/How\\_to\\_recover\\_after\\_a\\_cloud\\_computing\\_misstep](http://www.computerworld.com/s/article/9248619/How_to_recover_after_a_cloud_computing_misstep)

Collingridge, David, **The Social Control of Technology** (Pinter, 1980)

Collins, Amy, Adam Fleisher, Reed Freeman & Alistair Maughan, 'The Internet of Things: The Old Problem Squared', *Morrison & Fleisher, Society for Computer & the Law* (24 Mar 2014 accessed 22 Apr 2016) < <http://www.scl.org/site.aspx?i=ed36578>>

Columbus, Louis, 'Roundup of Internet of Things Forecasts and Market Estimates, 2015' (3 Jan 2016 accessed 6 Mar 2016) <<https://www.enterpriseirregulars.com/104084/roundup-internet-things-forecasts-market-estimates-2015/>>

Comer, Stuart, 'Aussie IoT in the home spend tipped to top \$200m in 2020' (6 Nov 2015 accessed 14 Apr 2016) <<http://www.iotaustralia.org.au/2015/11/06/iot-facts-and-forecasts/aussie-iot-in-the-home-spend-tipped-to-top-200m-in-2020/>>

Comer, Stuart, 'Aussie IoT in the home spend tipped to top \$200m in 2020' (6 November 2015 accessed 2 Feb 2016) <<https://www.iotaustralia.org.au/2015/11/06/iot-facts-and-forecasts/aussie-iot-in-the-home-spend-tipped-to-top-200m-in-2020/>>

Comer, Stuart 'IoT tipped to drive US consumer tech market to record high' (6 January 2016 accessed 5 Mar 2016) <http://www.iotaustralia.org.au/2016/01/06/iot-facts-and-forecasts/iot-tipped-to-drive-us-consumer-tech-market-to-record-high/>

Comer, Stuart, 'Comms Alliance IoT Think Tank morphing into standalone IoT Alliance' (7 Jan 2016 accessed 5 Mar 2016) <http://www.iotaustralia.org.au/2016/01/07/iotnewanz/comms-alliance-iot-think-tank-morphing-into-stand-alone-iot-alliance/>

Comer, Stuart, 'In the 'internet of everyone' we will love Big Brother' (16 Mar 2016 accessed 19 Apr 2016) <http://www.iotaustralia.org.au/2016/03/16/jot-studies/internet-everyone-will-love-big-brother/>

Comer, Stuart, 'What is the Australian Government's Role in IoT?' (7 Apr 2016 accessed 11 May 2016) <<http://www.iotaustralia.org.au/2015/04/07/iotblog/whats-the-australian-governments-role-in-iot/#>>

Commercial Bar Association, 'Contract hampered by unfair term' (24 Nov 2016 accessed 29 Nov 2016) <http://www.commbarmatters.com.au/2016/11/24/contract-hampered-by-unfair-term/>

Commission for the Protection of Privacy, 'Own-initiative recommendation relating to 1) Facebook, 2) Internet and /or Facebook users as well as 3) users and providers of Facebook services, particularly plug-ins (CO-AR-2015-003)' *Recommendation No. 04/2015 of 13 May 2015* (13 May 2015 accessed 4 Jan 2016) <[www.privacycommission.be/sites/privacycommission/files/dopuments/recommendation\\_04\\_2015\\_0.pdf](http://www.privacycommission.be/sites/privacycommission/files/dopuments/recommendation_04_2015_0.pdf)>

Commonwealth Consumer Affairs Advisory Council, 'App purchases by Australian consumers on mobile or handheld devices' *Department of Treasury Inquiry Report* (July 2013 accessed 6 Apr 2016) <<http://ccaac.gov.au/2013/07/19/app-purchases-by-australian-consumers-on-mobile-and-handheld-devices/>>

Commonwealth Consumer Affairs Advisory Council, 'Sharing of Repair Information in the Automotive Industry' *Final Report* (27 Nov 2012 Accessed 30 Jun 2016) <<http://www.aaaa.com.au/data/Final-report-on-sharing-of-repair-information-in-the-automotive-industry.pdf>>

Commonwealth Parliament, House of Representatives, Explanatory Memorandum *Privacy Amendment (Notifiable Data Breaches) Bill 2016* (2016 accessed 2 Oct 2016) <[http://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/Bills\\_Search\\_Results/Result?bld=r5747](http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r5747)>

## Competition and Markets Authority UK (CMA)

CMA, 'Historic Annex A to unfair contract terms guidance' (Sept 2008)  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/450467/Unfair\\_terms\\_guidance\\_Annex\\_A.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450467/Unfair_terms_guidance_Annex_A.pdf)>

CMA, 'Unfair Contract Terms Guidance' (31 Jul 2015 accessed 2 Mar 2016) <  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/450440/Unfair\\_Terms\\_Main\\_Guidance.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450440/Unfair_Terms_Main_Guidance.pdf)>

CMA, 'Unfair contract terms flowcharts' (31 Jul 2015 accessed 2 Jun 2016) <  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/450429/Unfair\\_terms\\_flowchart.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450429/Unfair_terms_flowchart.pdf)>

CMA, 'Cloud storage consumer law compliance review – summary of undertakings provided to the CMA' (25 May 2017 accessed 2 Jun 2016 )  
<https://assets.publishing.service.gov.uk/media/57472472e5274a0378000009/Summary-of-undertakings-JCLDKH.pdf>>

CMA, 'Consumer law compliance review: cloud storage' *Findings Report* (27 May 2016 accessed 2 Jun 2016) < [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/526447/cloud-storage-findings-report.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/526447/cloud-storage-findings-report.pdf)>

Commonwealth of Australia, *Trade Practices Amendment (Australian Consumer Law) Bill 2009*  
<<https://www.legislation.gov.au/Details/C2009B00132/Explanatory%20Memorandum/Text>>

Commonwealth of Australia, House of Representatives, Explanatory Memorandum, Trade Practices Amendment (Australian Consumer Law) Bill (No 2) 2010 (Cth) [5.39]  
<http://www.austlii.edu.au/au/legis/cth/bill/tpaclb22010505/>

Communications Alliance, '*Enabling the Internet of things in Australia*' *Internet of Things Think Tank*, Geoff Heydon & Frank Zeichner (Oct 2015 accessed 3 Jan 2016)  
<[http://www.commsalliance.com.au/\\_\\_data/assets/pdf\\_file/0007/51991/Enabling-the-Internet-of-Things-for-Australia.pdf](http://www.commsalliance.com.au/__data/assets/pdf_file/0007/51991/Enabling-the-Internet-of-Things-for-Australia.pdf)>

Communications Alliance, 'Internet of Things Think-Tank highlights Need for National Strategy' *Media Release* (May 2015 accessed 5 Mar 2016) <<http://www.commsalliance.com.au/about-us/newsroom/Internet-of-Things-Think-Tank-Highlights-Need-for-National-Strategy>>

CompTIA, 'Comment to NTIA', (13 Mar 2017 accessed 15 Mar 2017)  
<[https://www.ntia.doc.gov/files/ntia/publications/comptia\\_green\\_paper\\_comment\\_final.pdf](https://www.ntia.doc.gov/files/ntia/publications/comptia_green_paper_comment_final.pdf)>

ComputerWorld, 'Pacemaker hacker says worm could possibly 'commit mass murder' *Computerworld* (17 Oct 2012 accessed 18 Apr 2016) IDG News Service <  
<http://www.computerworld.com/article/2473402/cybercrime-hacking/pacemaker-hacker-says-worm-could-possibly--commit-mass-murder-.html>>

ComputerWorld ANZ, 'CyberThreat looms large: is Australia doing enough to ensure cybersecurity?' (July 2016 accessed 11 Jul 2016)  
<[http://docs.media.bitpipe.com/io\\_13x/io\\_132733/item\\_1376580/ANZ\\_ISM\\_0716\\_ezine\\_FINAL.pdf](http://docs.media.bitpipe.com/io_13x/io_132733/item_1376580/ANZ_ISM_0716_ezine_FINAL.pdf)>

Comstock, Jonah, 'FTC: Shark Tank star Breathometer must offer full refunds for inaccurate smartphone breathalyzer' *mobihealthnews* (24 Jan 2017 accessed 22 Feb 2017) < <http://www.mobihealthnews.com/content/ftc-shark-tank-star-breathometer-must-offer-full-refunds-inaccurate-smartphone-breathalyzer>>

Condliffe, Jamie, 'Anonymised Credit Card Data Really Isn't Very Anonymous' *Gizmodo* (31 Jan 2015 accessed 15 Apr 2015) < <http://www.gizmodo.com.au/2015/01/anonymized-credit-card-data-really-isnt-very-anonymous/>>

Conger, Kate 'Uber begins background collection of rider location data' *TechCrunch* (29 Nov 2016 accessed 29 Nov 2016) <<https://techcrunch.com/2016/11/28/uber-background-location-data-collection/>>

Connolly, Kate, 'Angela Merkel: internet search engines are 'distorting perception'' *The Guardian* (28 Oct 2016 accessed 2 Nov 2016) <<https://www.theguardian.com/world/2016/oct/27/angela-merkel-internet-search-engines-are-distorting-our-perception>>

Connor, Steve, 'First self-driving cars will be unmarked so that other drivers don't try to bully them' *The Guardian* (30 Oct 2016 accessed 30 Oct 2016) <<https://www.theguardian.com/technology/2016/oct/30/volvo-self-driving-car-autonomous>>

Consultancy.uk, 'More digital adds 1.36 trillion to top 10 economies' (30 Mar 2015 accessed 23 Mar 2016) <<http://www.consultancy.uk/news/1694/more-digital-adds-136-trillion-to-top-10-economies>>

Consultancy.uk, 'Top 10 digital trends 2016 to watch for design thinking' (11 Jan 2016 accessed 23 Mar 2016) < <http://www.consultancy.uk/news/3162/top-10-digital-trends-2016-to-watch-for-design-thinking>>

Consumer Affairs Australia and New Zealand (**CAANZ**), 'Australian Consumer Law Review Final Report' (Apr 2017 accessed Apr 2017) <[https://cdn.tspace.gov.au/uploads/sites/86/2017/04/ACL\\_Review\\_Final\\_Report.pdf](https://cdn.tspace.gov.au/uploads/sites/86/2017/04/ACL_Review_Final_Report.pdf)>

Consumer Action Law Centre, 'Australian Consumer Law Review' (30 May 2016 accessed 3 Sept 2016) < <http://consumeraction.org.au/wp-content/uploads/2016/05/Consumer-Action-ACL-Review-Submission-FINAL.pdf>>

Consumer Action Law Centre, 'Submission to Productivity Issues Paper- Consumer Law Enforcement and Administration' (30 Aug 2016 accessed 4 Sept 2016) <<http://consumeraction.org.au/wp-content/uploads/2016/09/PC-ACL-Enforcement-and-Admin-Consumer-Action-Submission-FINAL.pdf>>

Consumer Affairs Victoria, 'Unfair Contract Terms in Victoria: Research into their Extent, Nature, Cost and Implications' *Research Paper No. 12* (October 2007 accessed 5 Aug 2014) [15] <<http://www.consumer.vic.gov.au/resources-and-education/research>>

Consumer Reports (US), 'Guide to Car Reliability' (20 Oct 2015 accessed 21 Apr 2016) [http://www.consumerreports.org/cro/cars/guide\\_to\\_car\\_reliability/index.htm](http://www.consumerreports.org/cro/cars/guide_to_car_reliability/index.htm)

Consumer Reports (US), 'Talking Cars on the Pros and Cons of Tesla Autopilot' (17 Nov 2015 accessed 2 Mar 2016) <<http://www.consumerreports.org/cars/talking-cars-video-podcast-takes-off-with-tesla-s-autopilot/>>

Consumer Reports (US), 'Safety Agency Wants Detailed Info on Tesla Autopilot After Fatal Crash: NHTSA releases letter to the automaker that includes list of requests' (12 Jul 2016 accessed 16 Jul 2016) <<http://www.consumerreports.org/tesla/safety-agency-wants-detailed-info-tesla-autopilot-after-fatal-crash/>>

Consumer Reports (US), 'Tesla's Autopilot: Too Much Autonomy Too Soon' (14 Jul 2016 accessed 16 Jul 2016) < <http://www.consumerreports.org/tesla/tesla-autopilot-too-much-autonomy-too-soon/>>

Consumers International, 'Connection and Protection in the Digital Age: the Internet of things and challenges for consumer protection' (11 Apr 2016 accessed 18 Apr 2016) <<http://www.consumersinternational.org/media/1657273/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf>>

Consumers International, 'Briefing: the Internet of things and challenges for consumer protection' (11 Apr 2016 accessed 18 Apr 2016) <<http://www.consumersinternational.org/media/1657279/briefing-connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf>>

Consumers International and Verbraucherzentrale Bundesverband, 'Proposed recommendations from the consumer movement to the G20 member states' (2017 accessed 22 Apr 2017) <<http://www.consumersinternational.org/media/1733750/g20-digital-recs-english-visual.pdf>>

Consumers Union, 'Comment to NTIA', (27 Feb 2017 accessed 30 Feb 2017) < [https://www.ntia.doc.gov/files/ntia/publications/consumer\\_union.pdf](https://www.ntia.doc.gov/files/ntia/publications/consumer_union.pdf)>

Control Engineering, 'Industrial Internet of Things (IIoT) benefits, examples' (3 June 2015 accessed 5 May 2016) <<http://www.controleng.com/single-article/industrial-internet-of-things-iiot-benefits-examples/a2fdb5aced1d779991d91ec3066cff40.html>>

Cooper, James C., 'Separation, Pooling and Predictive Privacy Harms from Big Data: Confusing Benefits for Costs' (7 Oct 2015 accessed 6 Apr 2016) <[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00028-97819.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00028-97819.pdf)>

Corfield, Gareth 'Internet of Things Security? Start with Who Owns the Data' *The Register* (28 Sept 2016 accessed 4 Dec 2016) < [http://www.theregister.co.uk/2016/09/28/cambridge\\_wireless\\_iiot\\_event\\_defence\\_sig/](http://www.theregister.co.uk/2016/09/28/cambridge_wireless_iiot_event_defence_sig/)>

Corones, Stephen, Sharon Christensen, Justin Malbon, Allan Asher & Jeannie Marie Paterson, 'Comparative analysis of Overseas Consumer Policy Frameworks' (April 2016 accessed 26 Jun 2016) <[http://consumerlaw.gov.au/files/2016/05/ACL\\_Comparative-analysis-overseas-consumer-policy-frameworks-1.pdf](http://consumerlaw.gov.au/files/2016/05/ACL_Comparative-analysis-overseas-consumer-policy-frameworks-1.pdf)>

Corrigan, Michael and Matthew Evans, 'Court clarifies when the ACCC can put your assets in the deep freeze in consumer harm cases' *Clayton Utz* (1 Sept 2016 accessed 3 Sept 2016) <<https://www.claytonutz.com/knowledge/2016/september/court-clarifies-when-the-acc-ccan-put-your-assets-in-the-deep-freeze-in-consumer-harm-cases>>

Cossetto, Michael & Michael Muratore, 'Less than 9 months to comply? That's unfair' *Bartier Perry* (10 Mar 2016 accessed 10 Mar 2016) <<https://www.bartier.com.au/insights/less-than-9-months-to-comply-with-the-unfair-contracts-regime-thats-unfair/>>

Coughlin, Joseph F., 'Trusting a Robot with Your Life: Can Self-Driving Cars Earn the Public's Trust?' (10 November 2016 accessed 10 Nov 2016) <<http://bigthink.com/disruptive-demographics/trusting-a-robot-with-your-life-can-self-driving-cars-earn-the-publics-trust>>

Counts, Reese, 'Hackers arrested after stealing more than 30 Jeeps in Texas' *autoblog* (4 Aug 2016 accessed 3 Sept 2016) <<http://www.autoblog.com/2016/08/04/hackers-steal-30-jeeps-houston-texas/>>

Cowan, Paris, 'Pilgrim to audit 21 Australian privacy policies' *itNews* (20 Feb 2015 accessed 2 Feb 2016) <https://www.itnews.com.au/news/pilgrim-to-audit-21-australian-privacy-policies-400708>

Cowan, Paris, 'Should Google be held liable when its driverless cars crash?' *itNews* (10 Jun 2016 accessed 10 Jun 2016) <<http://www.itnews.com.au/news/should-google-be-held-liable-when-its-driverless-cars-crash-420632>>

Cowan, Paris, 'Is data de-identification a myth?' *itNews* (16 Nov 2016 accessed 17 Nov 2016) [http://www.itnews.com.au/news/is-data-de-identification-a-myth-441572?utm\\_source=desktop&utm\\_medium=twitter&utm\\_campaign=share](http://www.itnews.com.au/news/is-data-de-identification-a-myth-441572?utm_source=desktop&utm_medium=twitter&utm_campaign=share)

Cowie, Tom, 'Car yards offering finance in most states have begun deploying the devices, which can track the movements of a car and even immobilise it if a payment is missed seat' *The Sydney Morning Herald* (5 Oct 2014 accessed 6 Feb 2016) <<http://www.smh.com.au/national/gps-trackers-put-repo-man-in-passenger-seat-20141001-10os1q.html>>

Craig, Amanda N., Scott J. Shackelford, Janine S. Hiller, 'Proactive cybersecurity: A Comparative Industry and Regulatory Analysis' *American Business Law Journal* 52: 4 (Winter 2015 accessed 2 Dec 2016) <<http://onlinelibrary.wiley.com.ezproxy.bond.edu.au/doi/10.1111/ablj.12055/epdf>>

Crist, Ry, 'Screwed by sex toy spying? You may get \$10k' *CNET* (15 Mar 2017 accessed 20 Mar 2017) <<https://www.cnet.com/au/news/app-enabled-sex-toy-users-get-10000-each-after-privacy-breach/>>

CSIRO, 'An open source platform for the Internet of Things' (n.d. accessed 18 Mar 2016) <<http://www.csiro.au/en/Research/D61/Areas/Robotics-and-autonomous-systems/Internet-of-Things/An-open-source-platform-for-the-Internet-of-Things>>

Cudmore, Justin and James True, 'Before you hit send: Complying with the Spam Act – the unsubscribe and identification requirements' *Marque Lawyers* (9 November 2014 accessed 25 Mar 2015) [http://www.marquelawyers.com.au/assets/marque-update\\_before-you-hit-send-complying-with-the-spam-act-has-the-recipient-consented-161014.pdf?utm\\_source=Mondaq&utm\\_medium=syndication&utm\\_campaign=inter-article-link](http://www.marquelawyers.com.au/assets/marque-update_before-you-hit-send-complying-with-the-spam-act-has-the-recipient-consented-161014.pdf?utm_source=Mondaq&utm_medium=syndication&utm_campaign=inter-article-link)

Culnane, C, Benjamin Rubenstein and Vanessa Teague, 'Understanding the maths crucial for protecting privacy' *Pursuit*, University of Melbourne Department of Engineering and Technology (29 Sept 2016 accessed 5 Oct 2016) <<https://pursuit.unimelb.edu.au/articles/understanding-the-maths-is-crucial-for-protecting-privacy>>

Cummings, M.L. & J.C. Ryan, 'Who is in Charge? Promises and Pitfalls of driverless Cars', *TR News* (May-June 2014 accessed 20 Mar 2016) <<http://hal.pratt.duke.edu/sites/hal.pratt.duke.edu/files/u7/TR%20news%20Cummings%20MAR14.pdf>>

Cummings, Dr Mary (Missy) Louise, 'Testimony Before the Senate Committee on Commerce, Science and Technology Hearing: "Hands Off: The Future of Self-Driving Cars' (15 Mar 2016 accessed 20 Mar 2016) <<https://governmentrelations.duke.edu/wp-content/uploads/Cummings-Senate-testimony-2016.pdf>> S

Currie, David, 'The new Competition and Markets Authority: how will it promote competition?' *Beesley Lecture* (7 Nov 2013 accessed 10 Dec 2016) <<https://www.gov.uk/government/speeches/the-new-competition-and-markets-authority-how-will-it-promote-competition>>

## D

Dadlich, Scott, 'Barack Obama, Neural Nets, Self-driving Cars, and the Future of the World' *WIRED* (Nov. 2016 accessed 12 Oct 2016) <[https://www.wired.com/2016/10/president-obama-mit-joi-ito-interview/?mbid=nl\\_101216\\_p3&CNDID=>](https://www.wired.com/2016/10/president-obama-mit-joi-ito-interview/?mbid=nl_101216_p3&CNDID=>)

Dalbey, Beth 'Volkswagen Agrees to \$4.3B Settlement in Emissions Cheating Scandal: Feds' (11 Jan 2017 accessed 20 Jan 2017) <<http://patch.com/michigan/detroit/vw-group-close-4-3b-settlement-feds-reports>>

Daniel, '30 best "Works with Nest" Devices – Smart Home on Steroids' *appcessories* (22 May 2016 accessed 12 June 2016) <http://www.appcessories.co.uk/works-with-nest-best-compatible-devices/>

Darrow, Barb, 'The Question of Who Owns the Data Is About to Get a Lot trickier' *Fortune* (6 Apr 2016 accessed 7 Apr 2016) <<http://fortune.com/2016/04/06/who-owns-the-data/>>

Data Protection Commissioner (Ireland), 'Anonymisation and pseudonymisation' (n.d. accessed 2 Aug 2016) <<https://dataprotection.ie/viewdoc.asp?DocID=1594&ad=1>>

Data Protection Commissioner (Ireland), 'Guidance Note for Data Controllers on Location Data' (October 2016 accessed 2 Nov 2016) <<https://www.dataprotection.ie/docs/Guidance-Note-for-Data-Controllers-on-Location-Data/g/1587.htm>>

Datta, Amit, M.C. Tschantz & A. Datta, 'Automated Experiments on Ad Privacy Settings' *Proceedings on Privacy Enhancing Technologies* 2015 (1) 92- 112 Submitted to *FTC PrivacyCon 2016* <[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00067-98112.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00067-98112.pdf)>

Davenport, Tom 'Why are most "targeted marketing offers so bad?"' *Deloitte University Press* (7 Jul 2015 accessed 4 Jan 2016) <[dupress.com/articles/why-re-most-targetted-marketing-offers-so-bad/?id=us:2sm:3tw:dup945:awa:dup:072114:deloitteba:essay](http://dupress.com/articles/why-re-most-targetted-marketing-offers-so-bad/?id=us:2sm:3tw:dup945:awa:dup:072114:deloitteba:essay)>

Davenport, Thomas H. and John Lucker, 'Running on Data: activity trackers and the internet of things' *Deloitte Review* (26 Jan 2015 accessed 2 Apr 2016) <<https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-16/internet-of-things-wearable-technology.html>>

Davies, Alex, 'Obviously drivers are already abusing Tesla's Autopilot' (Oct 2015 accessed 20 Nov 2016) <<https://www.wired.com/2015/10/obviously-drivers-are-already-abusing-teslas-autopilot/>>

Davies, Alex, 'Self-driving cars are legal but road rules would be nice' (15 May 2015 accessed 20 Dec 2015) <<https://www.wired.com/2015/05/self-driving-cars-legal-real-rules-nice/>>

Davies, Alex, 'The Startup that could help GM beat Google to the Self-driving car' *WIRED* (11 Aug 2015 accessed 13 Aug 2016) <<https://www.wired.com/2016/08/gm-cruise-automation-self-driving-vogt/>>

Davies, Alex, 'Apple better be ready for the mad world of Car Regulations' *WIRED* (21 Sept 2015 accessed 2 Aug 2016) <<https://www.wired.com/2015/09/apple-better-ready-mad-world-car-regulations/>>

Davies, Alex, 'Ford say's it'll have a fleet of fully autonomous cars in just 5 years' *WIRED* (16 Aug 2016 accessed 20 Aug 2016) <https://www.wired.com/2016/08/ford-autonomous-vehicles-2021/>

Davies, Alex, 'Climb Inside Uber's Self-Driving Car—Its Next Big Disruption' *WIRED*, (14 Sept 2016 accessed 2 Oct 2016) <<https://www.wired.com/video/2016/09/inside-uber-s-self-driving-car/>>

Davies, Alex, 'Uber's self-driving truck makes its first delivery: 50,000 beers' *WIRED* (25 Oct 2016 accessed 29 Oct 2016) <https://www.wired.com/2016/10/ubers-self-driving-truck-makes-first-delivery-50000-beers/>

Davies, Alex, 'Detroit is stopping Silicon Valley in the self-driving car race' *WIRED* (3 Apr 2017 accessed 4 Apr 2017) <[https://www.wired.com/2017/04/detroit-stopping-silicon-valley-self-driving-car-race/?mbid=nl\\_4317\\_p2&CNDID=>](https://www.wired.com/2017/04/detroit-stopping-silicon-valley-self-driving-car-race/?mbid=nl_4317_p2&CNDID=>)>

Davies Collison Cave, 'Take a look to the future: driverless vehicles pose privacy and other regulatory challenges' *Lexology* (18 Mar 2016) <<http://www.lexology.com/library/detail.aspx?g=3aba2ef2-5c7f-4eec-9b0d-b3a55f1686a4>>

Davies, Michael, 'The perfect Storm: Five forces of Innovation' *Endeavour Partners* (Jul 2014 accessed 26 Mar 2016) <<http://endeavourpartners.net/perfect-storm-five-forces-innovation/>>

Davies, Rob, 'Driverless cars to dent insurance industry, warns Volvo chief' *The Guardian* (2 May 2016 accessed 10 May 2016) <<https://www.theguardian.com/business/2016/may/03/driverless-cars-dent-motor-insurers-volvo>>

Davis, Douglas, 'Prepared Statement for the Record of Intel Corporation' *Transportation 'The Connected World: Examining the Internet of Things' Full Committee Hearing* (11 Feb 2015 accessed 7 Mar 2016) (11 Feb 2015 accessed 7 Mar 2016) <<<http://www.commerce.senate.gov/public/index.cfm/2015/2/the-connected-world-examining-the-internet-of-things>>>

Davis, Hazel, 'Customers are core to any digital strategy' *Raconteur, The Times* (28 January 2016 accessed 1st February 2016) <<http://raconteur.net/business/customers-are-core-to-any-digital-strategy>>

De Bruin, Roland, 'Autonomous Intelligent Cars on the European intersection of liability and privacy' Working Paper (23 Mar 2015 accessed 2 Aug 2-16) < <http://www.cier.nl/?p=4279>>

Deloitte, 'Privacy by Design: setting a new standard for privacy certification' (n.d. accessed 4 May 2016)< <https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF>>

Deloitte, 'The Internet of Things ecosystem: unlocking the Business Value of Connected Devices' (2014 accessed 8 Mar 2016) <[www2.deloitte.com/global/en/./internet-of-things-ecosystem.html](http://www2.deloitte.com/global/en/./internet-of-things-ecosystem.html)>

Deloitte, 'Driving sensible solutions: Deloitte puts the internet of things to work for motorists' (2014 accessed 8 Mar 2016) < <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-gr15-driving-sensible-solutions.pdf>>

Deloitte, 'Anticipate, sense, and respond Connected Government and the Internet of things' A *GovLab Report* (2015 accessed 6 Mar 2016) [http://d27n205i7rookf.cloudfront.net/wp-content/uploads/2015/08/DUP\\_1268\\_IoT-Public-sector\\_vFINAL\\_8.31.pdf](http://d27n205i7rookf.cloudfront.net/wp-content/uploads/2015/08/DUP_1268_IoT-Public-sector_vFINAL_8.31.pdf)>

Deloitte, 'The internet of things really is things, not people' *TMT Predictions 2015* <<http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-pred15-iot-is-things.pdf>>

Deloitte, 'Navigating the Digital Divide: Digital influence in Australian Retail 2015' (14 Jul 2015 accessed 5 may 2016) < <https://www2.deloitte.com/au/en/pages/technology/articles/digital-divide.html>>

Deloitte, 'Global Mobile Consumer Survey: Southeast Asia Survey' (Dec 2015 accessed 8 Mar 2016) <<https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-2015-global-mobile-consumer-survey-southeast-asia-edition.pdf>>

Deloitte, 'A Crisis of Confidence' (7 Mar 2016 accessed 8 Mar 2016) <<https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-global-cm-survey-report.pdf>>

Deloitte, 'Virtual Reality: a billion dollar niche' (2016 accessed 8 Mar 2016) <<http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-prediction-virtual-reality-hardware-sales.pdf>>

Deloitte, 'Digital Democracy Survey' (10<sup>th</sup> edition) *Deloitte Development LLC* (2016 accessed 30 Mar 2016) <http://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-deloitte-digital-democracy-executive-summary.pdf>>

Deloitte, 'Technology trends 2016: Innovating in the digital era: A Public-Sector Perspective' (May 2016 accessed 15 may 2016) <<http://www2.deloitte.com/us/en/pages/public-sector/articles/tech-trends-public-sector.html?id=us:2em:3na:pstt2016:awa:cons:051716>>

Deloitte, 'Internet of things: From Sensing to Doing' *CIO, Wall Street Journal* (11 May 2016 accessed 31 May 2016) <<http://deloitte.wsj.com/cio/2016/05/11/internet-of-things-from-sensing-to-doing/tab/print/>>

Deloitte, 'Navigating the New Digital divide: A global summary of findings from nine countries on digital influence in retail' (2016 accessed 5 May 2016)  
<<http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Consumer-Business/gx-cb-global-digital-divide.pdf>>

Deloitte, 'Digital Democracy Survey' (2016 accessed 30 May 2016)  
<http://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-deloitte-digital-democracy-executive-summary.pdf>

Deloitte, 'Deloitte Australian Privacy Index 2016: Trust without Borders' (2016 accessed Jun 2016)  
<<http://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index-2016.html>>

Deloitte, 'Switch on to the connected home' *The Deloitte Consumer Review* (May 2016 accessed 10 Oct 2017) <<https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-16.pdf>>

Dennis, Sarah and Grace Ness 'Is your B2B sale of goods really B2C? Yes, when a business is actually "acquiring as a consumer"' *Clayton Utz* (1 Sept 2016 accessed 2 Sept 2016) <  
<https://www.claytonutz.com/knowledge/2016/september/is-your-b2b-sale-of-goods-really-b2c-yes-when-a-business-is-actually-acquiring-as-a-consumer>>

Department of Business, Innovation and Skills (UK), 'Consumer Engagement and Detriment Survey 2014' *TNS* (2014 accessed 26 Nov 2015) <https://www.gov.uk/government/publications/consumer-engagement-and-detriment-survey-2014>

Department of Commerce (US), 'EU- US Privacy Shield Principles' (2016 accessed 28 Feb 2016)  
<[https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu\\_us\\_privacy\\_shield\\_full\\_text.pdf](https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf)>

Department of Finance, Office of Best Practice Regulation, 'Best practice regulation handbook'  
<<http://finance.gov.au/obpr/ptproposal/handbook/appendix-A-five-yearly-reviews.html>>

Department of Innovation and Science, 'Innovation Policy Report' (monthly, accessed 17 Apr 2016)  
<<http://www.industry.gov.au/innovation/reportsandstudies/Pages/InnovationPolicyReport.aspx>>

Department of Transport (US), 'Proactive Safety Principles' (2016 accessed 7 Jun 2016) <  
<https://www.transportation.gov/briefing-room/proactive-safety-principles-2016>>

Department of Transportation, 'Letter to Tesla Motors' (8 July 2016 accessed 16 Jul 2016)  
<[http://static2.consumerreportscdn.org/content/dam/cro/news\\_articles/cars/NHTSA-letter-to-Tesla-autopilot.pdf](http://static2.consumerreportscdn.org/content/dam/cro/news_articles/cars/NHTSA-letter-to-Tesla-autopilot.pdf)>

Derene, Glenn, 'Tesla Model S Update Improves Safety of Its Summon Feature' (9 Mar 2016 accessed 2 Jun 2016) <  
<http://www.consumerreports.org/hybrids-evs/video-tesla-model-s-update-improves-safety-of-its-summon-feature/>>

De Zwart, M., Sal Humphreys and Beatrix van Dissel, 'Surveillance, Big data and democracy: Lessons for Australia from the US and UK', *UNSWLJ* 37:2 (2014) 713-747 (accessed 09 Aug 2016) <<http://search.informit.com.au.ezproxy.bond.edu.au/documentSummary;dn=613351331512035;res=IELAPA>> ISSN: 0313-0096>

Dickson, Ben 'Why IoT security is so critical' *Techcrunch* (24 Oct 2015 accessed 2 Mar 2015) <<https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/>>

DLA Piper, Arbitration Update on Arbitration Clauses in Standard Form Consumer Contracts (April 2016 accessed 15 May 2016) <<https://www.dlapiper.com/~media/Files/Insights/Publications/2016/04/Avoiding%20the%20void.pdf>>

DLA Piper, 'A Guide to the General Data Protection Regulation' (Nov 2016 accessed 12 Feb 2017) <<https://www.dlapiper.com/~media/Files/Insights/Publications/2016/12/General%20Data%20Protection%20Regulation%20Brochure.PDF>>

DLA Piper, 'Data Protection Laws of the World' (2016 accessed 15 May 2016) <<https://www.dlapiperdataprotection.com/>>

DLA Piper, 'Data Protection Laws of the World' (2017 accessed 2 Apr 2017) <<https://www.dlapiperdataprotection.com/>>

DLA Piper, 'Global Data Privacy Snapshot' (2017 accessed 2 Feb 2017) <<https://www.dlapiper.com/~media/Files/Insights/Publications/2017/01/DLA%20Piper%20Whitepaper.pdf>>

D-Link, 'D-Link Systems Inc. Enlists Cause of Action Institute to Defend Corporate & Consumer Rights' *Media Release* (10 Jan 2017 accessed 2 Feb 2017) <<http://us.dlink.com/press-centre/press-releases/d-link-systems-inc-enlists-cause-of-action-institute-to-defend-corporate-consumer-rights/>>

Dobbs, Richard, James Manyika & Jonathan Woetzel 'The Internet of Things: Mapping the Value Beyond the Hype' *McKinsey & Co* (June 2015 accessed 26 Nov 2015) <[http://www.mckinsey.com/insights/business\\_technology/The\\_Internet\\_of\\_Things\\_The\\_value\\_of\\_digitizing\\_the\\_physical\\_world?cid=other-eml-alt-mgi-mck-oth-1506](http://www.mckinsey.com/insights/business_technology/The_Internet_of_Things_The_value_of_digitizing_the_physical_world?cid=other-eml-alt-mgi-mck-oth-1506)>

Dolan, Matthew 'Why experts worry about the Tesla crash' *Detroit Free Press* (2 Jul 2016 accessed 6 Jul 2016) <<http://www.freep.com/story/money/cars/2016/07/01/experts-worry-tesla-crash/86611662/>>

Donato, Christine, 'The Big Data Revolution: Who Owns our Information?' *SAPVoice Forbes* (11 Apr 2016 accessed 11 Apr 2016) <<http://www.forbes.com/sites/sap/2016/04/11/the-bigdata-revolution-who-owns-our-data/>>

Donny, Lance, 'US Senate Testimony', 'Donny QFRs for IoT Hearing' and "Lance Donny Written response' *Transportation 'The Connected World: Examining the Internet of Things' Full Committee Hearing* (11 Feb 2015 accessed 7 Mar 2016) <<http://www.commerce.senate.gov/public/index.cfm/2015/2/the-connected-world-examining-the-internet-of-things>>

Dowling, Joshua, 'Why there is a record number of car safety recalls: 2.5 million and counting' *news.com.au* (10 Jul 2016 accessed 20 Jul 2016) <

<http://www.news.com.au/finance/business/manufacturing/why-there-is-a-record-number-of-car-safety-recalls-25-million-and-counting/news-story/78d643cd42b7e3cbf7c4ac020429f555>>

Downey, Colin, 'Florida State Highway Patrol Clears Tesla' *Consumers' Research* (2 Feb 2017 accessed 3 Feb 2017) <<http://consumersresearch.org/florida-state-highway-patrol-clears-tesla/>>

Duffy, Sophia H. and Jamie Patrick Hopkins, 'Sit, Stay, Drive: The Future of Autonomous Car Liability' (2013) 16 *SMU Science and Technology Law Review* 453

Duhig, Charles, 'Campaigns mine personal lives to get out vote' *The New York Times* (14 Oct 2012 accessed 15 Mar 2014):1 <[http://www.nytimes.com/2012/10/14/us/politics/campaigns-mine-personal-lives-to-get-out-vote.html?\\_r=0](http://www.nytimes.com/2012/10/14/us/politics/campaigns-mine-personal-lives-to-get-out-vote.html?_r=0)>

Dull, Tamara, 'Big Data and the Internet of things: Two sides of the same coin?' *SAS Best Practice* (2014 accessed 12 Apr 2016) <[http://www.sas.com/en\\_us/insights/articles/big-data/big-data-and-iot-two-sides-of-the-same-coin.html](http://www.sas.com/en_us/insights/articles/big-data/big-data-and-iot-two-sides-of-the-same-coin.html)>

Dutton, William H. 'Putting things to work: Social and policy challenges for the Internet of things' *Info* (May 2014 accessed 18 Apr 2016) Vol.16(3), pp.1-21 <<http://www.emeraldinsight.com.ezproxy.bond.edu.au/doi/pdfplus/10.1108/info-09-2013-0047>>

## E

Eckerson, Olivia 'Internal report on Target data breach reveals glaring security holes' (22 Sept 2015 accessed 19 Nov 2015) <http://searchsecurity.techtarget.com/news/4500253983/Internal-report-on-Target-data-breach-reveals-glaring-security-holes>

Eckerson, Olivia, 'FBI CISO warns of IoT data breaches' *TechTarget* (23 Sept 2015 accessed 19 Nov 2015) <<http://searchsecurity.techtarget.com/news/4500254067/FBI-CISO-warns-of-IoT-data-breaches>>

Editor, 'Shaking up the wearables' *The Economist* (26 Aug 2014 accessed 5 Jan 2016) <<http://www.economist.com/news/business-and-finance/21613925-potential-market-personal-fitness-tracking-devices-over-hyped-shedding-wearables>>

Editorial, 'The Guardian view on robots and humanity: Passing Go Editorial' *The Guardian* (10 Mar 2016 accessed 10 Mar 2016) <<http://www.theguardian.com/commentisfree/2016/mar/09/the-guardian-view-on-robots-and-humanity-passing-go>>

Editorial, 'The Guardian view on self-driving cars: attention needed' Editorial (2 Jul 2016 accessed 2 Jul 2016) < <https://www.theguardian.com/commentisfree/2016/jul/01/the-guardian-view-on-self-driving-cars-attention-needed>

Egan, Matt, 'What is the Internet of things?' *Techworld* (4 Dec 2015 accessed 8 Apr 2016) < <http://www.techworld.com/picture-gallery/cloud/internet-of-things-vs-things-on-internet-what-is-internet-of-things-3631177/#7>>

Egelman, Serge, Julia Bernd et al, 'The Teaching Privacy Curriculum', *Submission to FTC PrivacyCon 2016* (2015 accessed 6 Apr 2016) < [https://www.ftc.gov/system/files/documents/public\\_comments/2015/09/00014-97596.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/09/00014-97596.pdf)>

## Electronic Privacy Information Center (EPIC)

EPIC, 'Comments of the Electronic Privacy Information Center to the Federal Trade Commission on the Privacy and Security Implications of the Internet of Things' (1 Jun 2013 accessed 2 Feb 2016) <https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf>

EPIC, 'Google Plans Advertising on Appliances, Including Nest Thermostat' (22 May 2014 accessed 5 Mar 2016) <https://epic.org/2014/05/google-plans-advertising-on-ap.html>

EPIC, 'Brief of Amicus Curiae Electronic Privacy Information Center (Epic) And Thirty-Three Technical Experts and Legal Scholars in Support of Respondent, *Federal Trade Commission, v. Wyndham Hotels & Resorts, LLC, et al.*, Case No. 14-3514' (12 Nov 2014 Accessed 2 Feb 2016) <<https://epic.org/amicus/ftc/wyndham/Wyndham-Amicus-EPIC.pdf>>

EPIC, 'Samsung Smart TV Complaint' (24 Feb 2015 accessed 11 Aug 2016) <<https://www.epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf>> and Commentary <<https://epic.org/privacy/internet/ftc/samsung/>>

EPIC, 'Request for Workshop and Investigation of 'Always On' Consumer Devices', Letter to US Department of Justice and the FTC (10 Jul 2015 accessed 4 Feb 2016) <<https://epic.org/2015/07/epic-urges-investigation-of-al.html>>

EPIC, 'Brief of Amicus Curiae FTC v. Wyndham' (2016 accessed 8 Mar 2016) <<https://epic.org/amicus/ftc/wyndham/#interest>>

EPIC, 'Communications Privacy Rulemaking' *Letter to the FCC* (20 Jan 2016 accessed 2 Jun 2016) <<https://epic.org/privacy/consumer/EPIC-to-FCC-on-Communications-Privacy.pdf>>

EPIC, "Comments of the Electronic Privacy Information Center to the National Telecommunications and Information Administration, US Department of Commerce On the Benefits, Challenges and Potential Roles for the Government in Fostering the Advancement of the Internet of Things" (2 June 2016 accessed 26 Jun 2016) <https://www.ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things>

EPIC, 'Cahen v. Toyota Motor Corporation' *Epic.org* (2016 accessed 8 Aug 2016) <https://epic.org/amicus/cahen/#EPIC>

EPIC, 'Comments of the Electronic Privacy Information Center to the National Highway Traffic Safety Administration/Department of Transportation Request for Comment on "Federal Automated Vehicles Policy" *Docket No. 2016-22993* (22 November 2016 accessed 1 Dec 2016) <https://www.epic.org/privacy/internet/iot/EPIC-NHTSA-AV-Policy-Comments-11-22-16.pdf>

EPIC, 'Testimony to 'The Promises and Perils of Emerging Technologies for Cybersecurity, 115th Cong.', *U.S. Senate Committee on Commerce, Science, & Transportation* (22 Mar 2017 accessed 28 Mar 2017) <<https://epic.org/testimony/congress/EPIC-SCOM-IoTandAI-Mar2017.pdf>>

Elias, Jennifer, 'Wearables are Missing a Crucial Aspect: Community' (17 Nov 2015 accessed 10 Mar 2016) < <http://www.forbes.com/sites/jenniferelias/2015/11/17/wearables-are-missing-a-crucial-aspect-community/#4f89f4fc6417>>

Elias, Jennifer, '6 Ways to Protect Your Data in the Age of Wearables' 1.0' (15 Dec 2015 accessed 10 Apr 2016) < <http://www.forbes.com/sites/jenniferelias/2015/12/15/6-ways-to-protect-your-data-in-the-age-of-wearables-1-0/#3c10b0b74405>>

Elvy, Stacy A., 'Contracting in the Age of the Internet of Things: Article 2 Of the UCC and Beyond' [2016] *Hofstra Law Review* 44: 839

Endeavour Partners, 'The Future of Activity Trackers (Part 3): The Secret to Long Term Engagement' (Jan 2014 accessed 26 Mar 2016) <http://endeavourpartners.net/the-future-of-activity-trackers-part-3-the-secret-to-long-term-engagement/>

Endeavour Partners, 'Wearables abandonment rates are not improving materially' (May 2015 accessed 26 Mar 2016) < <http://endeavourpartners.net/wearables-abandonment-rates-are-not-improving-materially/>>

Enigma Software, 'Cyber Attacks Aimed at Data Brokers D&B, Altegrity and LexisNexis Claim Theft of Important Data' (2013 accessed 9 Apr 2015) <<http://www.enigmasoftware.com/cyber-attacks-data-brokers-db-altegrity-lexisnexis-theft-important-data/>>

Equinix, 'Fulfilling the Promise of Big Data: A New Paradigm for Connecting Data within the Enterprise. Why Latency is holding back the Promise of Big Data" *Techworld White Paper* (8 Mar 2016 accessed 10 Mar 2016) <<http://www.techworld.com/resources/white-paper/analytics-big-data/fulfilling-promise-big-data-new-paradigm-connecting-data-within-enterprise-3636351/>>

Eskens, Sarah Johanna, 'Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It?' (February 29, 2016). Available at SSRN: <http://ssrn.com/abstract=2752010> < [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2752010](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2752010)>

Etherington, Daniel, 'Google Reveals 'The Physical Web,' A Project to Make Internet of Things Interaction App-Less' *TechCrunch* (2 Oct 2014 accessed 11 Apr 2016) <http://techcrunch.com/2014/10/02/google-the-physical-web/>

Etlinger, Susana and Jessica Groopman, 'The Trust Imperative: A Framework for Ethical Data Use' *Altimeter* (25 Jun 2015 accessed 2 Aug 2016) <http://www.altimetergroup.com/pdf/reports/The-Trust-Imperative-Altimeter-Group.pdf>

Etlinger, Susan, "AI" *Altimeter* (Jan 2017 accessed 3 Feb 2017) <http://www.altimetergroup.com/pdf/reports/The-Age-of-Artificial-Intelligence-Altimeter.pdf>

## **European Commission (EC)**

EC, 'Options for and Effectiveness of Internet Self- and Co-Regulation' (Jonathan Cave, Chris Marsden and Steve Simmons) *Rand Corporation* (2008 accessed 12 Jun 2016) < [http://www.rand.org/content/dam/rand/pubs/technical\\_reports/2008/RAND\\_TR566.pdf](http://www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR566.pdf)>

EC, 'Europe's policy options for a dynamic and trustworthy development of the Internet of things' *Rand Europe* (SMART 2012/0053 accessed 2 Jan 2016) <[http://www.rand.org/content/dam/rand/pubs/research\\_reports/RR300/RR356/RAND\\_RR356.pdf](http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR356/RAND_RR356.pdf)>

EC, 'C-ITS Platform Final Report' (Jan 2016 accessed 20 Dec 2016)  
<https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf>

EC, AIOTA, 'Report AIOTI Working Group 4 – Policy' (15 Oct 2015 accessed 3 Mar 2016) <https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf>

EC, 'Commission Staff Working Document: Advancing the Internet of Things in Europe accompanying the document "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitising European Industry - Reaping the full benefits of a Digital Single Market COM(2016) 180' (19 Apr 2016 accessed 3 Jun 2016) <<https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe>>

EC, Digital Single Market, Research and Innovation (9 Jun 2016 accessed 2 Mar 2017)  
<https://ec.europa.eu/digital-single-market/en/research-innovation-iot>

EC, Commission Staff Working Document 'Preliminary Report on the E-commerce Sector Inquiry' (15 Sept 2016 accessed 2 Oct 2016)  
[http://ec.europa.eu/competition/antitrust/sector\\_inquiry\\_preliminary\\_report\\_en.pdf](http://ec.europa.eu/competition/antitrust/sector_inquiry_preliminary_report_en.pdf)

EC, 'Study on consumers' attitudes towards Terms and Conditions (T&Cs) Final Report (2016 accessed 2 Dec 2016)  
<[http://ec.europa.eu/consumers/consumer\\_evidence/behavioural\\_research/docs/terms\\_and\\_conditions\\_final\\_report\\_en.pdf](http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/terms_and_conditions_final_report_en.pdf)>

EC, 'IOT Security and Privacy Workshop' AIOTA (13 Jan 2017 accessed 20 Feb 2017)  
<<[https://europa.eu/newsroom/events/internet-things-%E2%80%93-privacy-and-security-workshop\\_en](https://europa.eu/newsroom/events/internet-things-%E2%80%93-privacy-and-security-workshop_en)>

EC, 'Internet of Things Privacy & Security Workshop's Report' (10 Apr 2017 accessed 15 Apr 2017)  
<<https://ec.europa.eu/digital-single-market/en/news/internet-things-privacy-security-workshops-report>>

European Court of Human Rights, 'Personal Data Protection' *Factsheet* (Feb 2016 accessed 8 Apr 2016) < [http://www.echr.coe.int/Documents/Handbook\\_data\\_protection\\_ENG.pdf](http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf)>

### **European Data Protection Supervisor (EDPS)**

EDPS, 'Executive Summary of the Preliminary Opinion of the European Data Protection Supervisor on privacy and competitiveness in the age of big data' (26 Mar 2014 accessed 6 Dec 2016) [http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014XX0716\(01\)&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014XX0716(01)&from=EN)>

EDPS, 'Privacy and competitiveness in the age of big data: The Interplay between Data Protection, Competition and Consumer Protection in the Digital Economy' (*Preliminary Opinion of the European Data Protection Supervisor*) (Mar 2014 accessed 2 Jan 2016) <  
[https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26\\_competition\\_law\\_big\\_data\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competition_law_big_data_EN.pdf)>

EDPS, 'Opinion 5/2016 Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC)' (26 Jul 2016 accessed 10 Aug 2016)

<[https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-07-22\\_Opinion\\_ePrivacy\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-07-22_Opinion_ePrivacy_EN.pdf)>

EDPS, 'Opinion 4/2015 Towards a new digital ethics' (11 Sept 2015 accessed 8 Feb 2016) <[https://edps.europa.eu/sites/edp/files/publication/15-09-11\\_data\\_ethics\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf)>

EDPS, 'Towards a New Digital Ethics' (1 Feb 2016 accessed 8 Apr 2016)  
<<https://www.youtube.com/watch?v=HGN5WfUJR90>>

EDPS, 'Assessing the necessity measures that limit the fundamental right to the protection of personal data: A Toolkit' (11 Apr 2017 accessed 13 Apr 2017)  
[https://edps.europa.eu/sites/edp/files/publication/17-04-11\\_necessity\\_toolkit\\_en\\_0.pdf](https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf)

## **European Union (EU)**

EU, Commission Staff Working Document, 'Future Networks and the Internet- Early Challenges regarding the Internet of things' (2010)  
[http://ec.europa.eu/information\\_society/eeurope/i2010/docs/future\\_internet/swp\\_internet\\_things.pdf](http://ec.europa.eu/information_society/eeurope/i2010/docs/future_internet/swp_internet_things.pdf)

EU, 'Internet of Things – Architecture' IoT-A (30 Nov 2013 accessed 10 Mar 2016) <http://www.ietf.org/public/front-page>>

EU, 'Background document: Open Consultation on Geo-Blocking and Other Geographically-Based Restrictions When Shopping and Accessing Information in the EU (2015 accessed 26 Nov 2015)  
<<https://ec.europa.eu/eusurvey/files/0a9debaa-2d76-4877-b75a-f987812ebe74>>

EU, 'Regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy' (2015 accessed 26 Nov 2015)  
<<https://ec.europa.eu/eusurvey/runner/Platforms/#>>

EU, 'Research for TRAN Committee – Self-piloted cars: the future of road transport', Director-General for Internal Policies Policy Department B (2016 accessed 2 Jul 2016)  
[http://www.europarl.europa.eu/RegData/etudes/STUD/2016/573434/IPOL\\_STU\(2016\)573434\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/573434/IPOL_STU(2016)573434_EN.pdf)

EU, 'The Precautionary Principle' (21 Sept 2015 accessed 3 Feb 2016) <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3A132042>

EU, Art 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation services on smart mobile services' (2011 accessed 2 Aug 2016) <  
[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf)>

EU, Art 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices' (adopted 27 Feb 2013 accessed 2 Feb 2016) < [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf)>

EU, Article 29 Data Protection Working Party, 'Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)' (19 Jul 2016 accessed 20 Aug 2016) <  
[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf)>

EU, Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (10 Apr 2014 accessed 2 Jan 2016) < [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)>

EU, Article 29 Data Protection Working Party, 'Opinion 1/2008 on data protection issues related to search engines' (Adopted 4 Apr 2008 accessed 2 Aug 2016) < [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf)>

EU, Article 29 Data Protection Working Party, 'Opinion 8/2014 on Recent Developments on the Internet of Things' *Article 29 of Directive 95/46/EC* (16 Sept 2014 accessed 16 Mar 2016) <[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf)>

EU, Open Consultation on Geo-Blocking and Other Geographically-Based Restrictions When Shopping and Accessing Information in the EU (2015 accessed 26 Nov 2015) <<https://ec.europa.eu/eusurvey/runner/geoblocksurvey2015/>>

EuroActiv.com, 'Economist editor: Big data is a goldmine for companies' (6 May 2014 accessed 10 Apr 2015) < <http://www.euractiv.com/sections/eskills-growth/economist-editor-big-data-goldmine-companies-301933>>

### **European Union Agency for Network and Information Security (ENISA)**

ENISA, 'Privacy and data protection by design – from policy to engineering', (2014 accessed 14 Jun 2016) <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design>;

ENISA, 'Threat Landscape for Smart Home and Media Convergence' (9 Feb 2015 accessed 2 Nov 2015) < <https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence>>

ENISA, 'Online privacy tools for the general public' (17 Dec 2015 accessed 14 Jun 2016) <https://www.enisa.europa.eu/publications/privacy-tools-for-the-general-public>

ENISA, 'Security and Resilience of Smart Home Environments: Good practices and recommendations' (Dec 2015 accessed 2 Apr 2016) <https://www.enisa.europa.eu/publications/security-resilience-good.../at.../fullReport>

ENISA, 'Big Data Threat Landscape and Good Practice Guide' (2016 accessed 20 Mar 2016) <<https://www.enisa.europa.eu/publications/bigdata-threat-landscape>>

ENISA, 'PETs controls matrix - A systematic approach for assessing online and mobile privacy tools' (20 Dec 2016 accessed 10 Feb 2016) <https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools>

ENISA, 'Privacy Enhancing Technologies: Evolution and State of the Art' (9 Mar 2017 accessed 20 Mar 2017) <https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art>

Europe Economics, 'An Analysis of the issue of Consumer Detriment and the most appropriate methodologies to estimate it' (2007 accessed 4 Jan 2016)

<[http://ec.europa.eu/consumers/consumer\\_evidence/market\\_studies/docs/study\\_consumer\\_detriment.pdf](http://ec.europa.eu/consumers/consumer_evidence/market_studies/docs/study_consumer_detriment.pdf)>

Europe Economics, 'Assessing the Impact of Policy on Consumer Detriment' (2007 accessed 4 Jan 2016) <

[http://ec.europa.eu/consumers/consumer\\_evidence/market\\_studies/docs/handbook\\_consumer-detriment.pdf](http://ec.europa.eu/consumers/consumer_evidence/market_studies/docs/handbook_consumer-detriment.pdf)>

European Parliament, 'Challenges for Competition policy in a Digitalised economy' *Study for the ECON Committee* (July 2015 accessed 2 Aug 2016)

[http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL\\_STU%282015%29542235](http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282015%29542235)

European Parliament, 'Consumer protection in the EU: Policy overview' (Sept 2015 accessed 6 Apr 2016) <

[http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/565904/EPRS\\_IDA\(2015\)565904\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/565904/EPRS_IDA(2015)565904_EN.pdf)>

European Parliamentary Research Service, 'The Internet of things: opportunities and challenges' (May 2015 accessed 2 Jan 2016)

[http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS\\_BRI\(2015\)557012\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf)>

### **European Research Cluster on the Internet of Things (IERC)**

IERC, 'Internet of Things' (2013 accessed 2 Jan 2016) [http://www.internet-of-things-research.eu/about\\_iot.htm](http://www.internet-of-things-research.eu/about_iot.htm)

IERC, 'Internet of Things – IoT Governance, Privacy and Security' (Jan 2015 accessed 12 Apr 2016) <  
<http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf>>

IERC, 'Internet of Things beyond the Hype: Research, Innovation and Deployment' (2015 accessed 13 Apr 2016) <  
[http://www.internet-of-things-research.eu/pdf/Internet%20of%20Things%20beyond%20the%20Hype%20-%20Chapter%203%20-%20SRIA%20-%20IERC%202015\\_Cluster\\_%20eBook\\_978-87-93237-98-8\\_P\\_Web.pdf](http://www.internet-of-things-research.eu/pdf/Internet%20of%20Things%20beyond%20the%20Hype%20-%20Chapter%203%20-%20SRIA%20-%20IERC%202015_Cluster_%20eBook_978-87-93237-98-8_P_Web.pdf)>

Europol, 'The Internet Organised Crime Threat Assessment (IOCTA) 2015' (30 Sept 2015 accessed 2 Jan 2016) <  
<https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015>>

Evans, Dave 'The Internet of Things: Connected in Four Dimensions' *Huffington Post* (24 Sept 2014 accessed 2 Mar 2016) <  
[http://www.huffingtonpost.com/dave-evans/cisco-beyond-things-the-interne\\_b\\_3976104.html](http://www.huffingtonpost.com/dave-evans/cisco-beyond-things-the-interne_b_3976104.html)>

Evans, Dave, 'We Need to get the Internet of Things right' *TechCrunch* (19 Apr 2015 accessed 11 Apr 2016) <http://techcrunch.com/2015/04/19/we-need-to-get-the-internet-of-things-right/>>

Evans, Jeff, 'The Opt-Out Challenge' Black & Veatch (March/April 2012 accessed 3 Nov 2016) *Electric Light & Power* <  
<http://bv.com/docs/articles/the-opt-out-challenge.pdf>>

## Executive Office of the President (EOP)

EOP, 'Big Data: Seizing Opportunities, Preserving Values' Interim progress report (May 2014 accessed 10 May 2016) <

[https://www.whitehouse.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_may\\_1\\_2014.pdf](https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf)>

EOP, 'Big Data and Differential Pricing' Feb 2015 accessed 10 May 2016)

[https://obamawhitehouse.archives.gov/sites/default/files/whitehouse\\_files/docs/Big\\_Data\\_Report\\_None\\_mbargo\\_v2.pdf](https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_None_mbargo_v2.pdf)

EOP, 'Big Data: a Report on Algorithmic Systems, Opportunity, and Civil Rights' (May 2016 accessed 10 May 2016)

[https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016\\_0504\\_data\\_discrimination.pdf](https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf)>

EOP, National Science and Technology Council Committee of Technology, 'Preparing for the Future of Artificial Intelligence' (Oct 2016 accessed Oct 2016)

[https://www.whitehouse.gov/sites/default/files/whitehouse\\_files/microsites/ostp/NSTC/preparing\\_for\\_the\\_future\\_of\\_ai.pdf](https://www.whitehouse.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf)

EY, Gigatronic and Code White, 'Automotive Cybersecurity' (2016 accessed 2 Jul 2016)

<[http://www.ey.com/Publication/vwLUAssets/ey-automotive-cybersecurity/\\$FILE/ey-automotive-cybersecurity.pdf](http://www.ey.com/Publication/vwLUAssets/ey-automotive-cybersecurity/$FILE/ey-automotive-cybersecurity.pdf)>

## F

Fadilpašić, Sead, 'Consumers do not Trust Internet of Things' *betanews* (April 2016 accessed 11 May 2016) <<http://betanews.com/2016/04/08/internet-of-things-consumer-trust/>>

Fair, Lesley 'Dealing in Personal Data? Let the seller beware' *FTC Blog* (18 Feb 2016 accessed 23 Feb 2016) <https://www.ftc.gov/news-events/blogs/business-blog/2016/02/dealing-personal-data-seller-beware>>

Fair, Lesley, 'ASUS case suggests 6 things to watch for in the Internet of Things' (23 Feb 2016 accessed 23 Feb 2016) < <https://www.ftc.gov/news-events/blogs/business-blog/2016/02/asus-case-suggests-6-things-watch-internet-things>>

Fair, Lesley, 'FTC challenges claims for smartphone breathalyzer pitched on "Shark Tank"' (23 Jan 2017 accessed 22 Feb 2017) <<https://www.ftc.gov/news-events/blogs/business-blog/2017/01/ftc-challenges-claims-smartphone-breathalyzer-pitched-shark>>

Farrell, Paul and Oliver Laughland, 'Asylum-seeker data breach to be investigated by Privacy Commissioner' *The Guardian* (19 Feb 2014 accessed 9 Apr 2015)

<<http://www.theguardian.com/world/2014/feb/19/asylum-seeker-data-breach-to-be-investigated-by-privacy-commissioner>>

Farrell, Scott 'How to use humans to make "smart contracts" truly smart' (30 June 2016 accessed 5 July 2016) *King & Wood Mallesons* <<http://www.kwm.com/en/au/knowledge/insights/smart-contracts-open-source-model-dna-digital-analogue-human-20160630>>

Faure, Michael G. & Hanneke A. Luth, 'Behavioural Economics in Unfair Contract Terms: Cautions and Considerations' *J Consum Policy* (2011) 34:337-358  
<<http://web.b.ebscohost.com.ezproxy.bond.edu.au/ehost/pdfviewer/pdfviewer?sid=2248341d-ca16-422e-950b-56853adeb34a%40sessionmgr102&vid=1&hid=116>>

FDA, "General Wellness: Policy for Low Risk Devices," on January 20, 2015' U.S. Department of Health and Human Services Food and Drug Administration (29 Jul 2016 accessed 20 Oct 2016)  
<<https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429674.pdf>>

FDA, 'Postmarket Management of Cybersecurity in Medical Devices', *Nonbinding recommendations*, U.S. Department of Health and Human Services Food and Drug Administration (28 Dec 2016 accessed 22 Jan 2017)  
<<https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf>>

**Federal Bureau of Investigation (FBI)**, 'Cyber Tip: Be Vigilant with your Internet of things (IoT) devices' *Alert Number I-031716-PSA* (13 Oct 2015 accessed 2 Mar 2016) < <https://www.fbi.gov/news/stories/cyber-tip-be-vigilant-with-your-internet-of-things-iot-devices>>

FBI 'Cyber Tip: Be Vigilant with Your Internet of Things (IoT Devices)' (13 Oct 2015 accessed 14 Jul 2016) < <https://www.fbi.gov/news/stories/cyber-tip-be-vigilant-with-your-internet-of-things-iot-devices>>

FBI, 'Motor vehicles increasingly vulnerable to remote exploits' (17 Mar 2016 accessed 11 May 2016) < <https://www.ic3.gov/media/2016/160317.aspx>>

FBI, Risks of Internet of Things Devices' Podcast (3 Jul 2016 accessed 13 Jul 2016)  
<<https://www.fbi.gov/audio-repository/news-podcasts-thisweek-risks-of-internet-of-things-devices.mp3>>

### **Federal Chamber of Automotive Industries (FCAI),**

FCAI, 'FCAI Submission to the Qld Parliamentary Inquiry into Lemon Laws' (8 Oct 2015 accessed 6 May 2016) < <http://www.fcai.com.au/news/publication/index/year/all/month/all/publication/73>>

FCAI, 'FCAI Submission to NTC Issues Paper: Regulatory barriers to more automated road and rail vehicles' (11 Apr 2016 accessed 11 Apr 2016)  
<<http://www.fcai.com.au/news/publication/index/year/all/month/all/publication/77>>

FCAI, 'Submission to the ACL Review' (Jun 2016 accessed 20 Aug 2016) < [http://consumerlaw.gov.au/files/2016/07/Federal\\_Chamber\\_of\\_Automotive\\_Industries.pdf](http://consumerlaw.gov.au/files/2016/07/Federal_Chamber_of_Automotive_Industries.pdf)>

FCAI, 'FCAI Submission to NTC Issues Paper: Regulatory Barriers to More Automated Road and Rail Vehicles' < [http://www.ntc.gov.au/Media/Reports/\(2B3F8B5D-51EB-4104-8D0C-4CF9CB10C9D2\).pdf](http://www.ntc.gov.au/Media/Reports/(2B3F8B5D-51EB-4104-8D0C-4CF9CB10C9D2).pdf)>

Federal Communications Commission (FCC), 'In the Matter of Protecting the Privacy of Customer of broadband and Other Telecommunications Services' Notice of Proposed Rulemaking (1 Apr 2016 accessed 2 Aug 2016) (WC Docket No. 16-106) < <https://www.fcc.gov/document/fcc-releases-proposed-rules-protect-broadband-consumer-privacy>>

## Federal Trade Commission

FTC, 'Mobile apps for kids: Disclosures still not making the grade' *Text of the Commission Staff Report* (2012 accessed 8 Mar 2016) <https://www.ftc.gov/reports/mobile-apps-kids-disclosures-still-not-making-grade>

FTC, 'How to keep Your Personal Information Secure' (Jul 2012 accessed 8 Mar 2016) <https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure>

FTC, 'Mobile Privacy Disclosures: Building Trust Through Transparency: A Federal Trade Commission Staff Report' (Feb 2013 accessed 23 Feb 2016) <<https://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission>>

FTC 'Mobile App Developers: Start with Security' (Feb 2013 accessed 23 Feb 2016) <<https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security>>

FTC, 'Consumer Fraud in the United States, 2011: The Third FTC Survey' *Staff Report of the Bureau of Economics* (April 2013 accessed 26 Mar 2016) [https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey\\_0.pdf](https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf)

FTC, 'Advertising and Privacy Disclosures in a Digital World' (30 May 2013 accessed 16 Mar 2016) <[https://www.ftc.gov/sites/default/files/documents/public\\_events/short-advertising-privacy-disclosures-digital-world/finalworkshoptranscriptaugust72012.pdf](https://www.ftc.gov/sites/default/files/documents/public_events/short-advertising-privacy-disclosures-digital-world/finalworkshoptranscriptaugust72012.pdf)>

FTC, 'Internet of Things Privacy and Security in a Connected World (19 Nov 2013 accessed 26 Nov 2015) Public Workshop' <<https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>>

FTC, 'FTC Approves Final Order Settling Charges Against TRENDnet, Inc.' (7 Feb 2014 accessed 16 Mar 2016) <<https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc>>

FTC, 'Comment of the Federal Trade Commission, In the Matter of Advance Notice of Proposed Rulemaking Regarding Federal Motor Vehicle Safety' Docket No. NHTSA-2014-0022 (20 Oct 2014 accessed 4 Jan 2016) <[https://www.ftc.gov/system/files/documents/advocacy\\_documents/federal-trade-commission-comment-national-highway-traffic-safety-administration-regarding-nhtsa/141020nhtsa-2014-0022.pdf](https://www.ftc.gov/system/files/documents/advocacy_documents/federal-trade-commission-comment-national-highway-traffic-safety-administration-regarding-nhtsa/141020nhtsa-2014-0022.pdf)>

FTC, 'Start with Security: A Guide for Business' (Jan 2015 accessed 4 Jan 2016) <[https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business?utm\\_source=govdelivery](https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business?utm_source=govdelivery)>

FTC, 'Careful Connections: Building Security in the Internet of Things' (Jan 2015 accessed 23 Feb 2016) <<https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things>>

FTC, Internet of Things Privacy and Security in a Connected World, *Staff Report* (Jan 2015 accessed 26 Nov 2015) <<https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>>

FTC, 'Opening remarks of Edith Ramirez to the International Consumer Electronics Show', (6 Jan 2015 accessed 5 Jan 2016) < <https://www.ftc.gov/public-statements/2015/01/privacy-iot-navigating-policy-issues-opening-remarks-ftc-chairwoman-edith>>

FTC, 'FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks', *Press Release* (27 Jan 2015 accessed 26 Nov 2015) <<https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices>>

FTC, 'Internet of Things Workshop Report: Separate Statement of Commissioner Maureen K. Ohlhausen' (27 Jan 2015 accessed 26 Nov 2015) <[https://www.ftc.gov/system/files/documents/public\\_statements/620691/150127iotmkostmt.pdf](https://www.ftc.gov/system/files/documents/public_statements/620691/150127iotmkostmt.pdf)>

FTC, 'Dissenting Statement of Commissioner Joshua D. Wright Issuance of The Internet of Things: Privacy and Security in a Connected World Staff Report January 27, 2015 (27 Jan 2015 accessed 26 Nov 2015) <[https://www.ftc.gov/system/files/documents/public\\_statements/620701/150127iotjdwstmt.pdf](https://www.ftc.gov/system/files/documents/public_statements/620701/150127iotjdwstmt.pdf)>

FTC, 'Consumer complaints to the FTC increased in 2015' *Consumer Information Blog* (1 Mar 2015 accessed 9 Mar 2016) < [https://www.consumer.ftc.gov/blog/consumer-complaints-ftc-increased-2015?utm\\_source=govdelivery](https://www.consumer.ftc.gov/blog/consumer-complaints-ftc-increased-2015?utm_source=govdelivery)

FTC, 'How to Regulate the Internet of Things Without Harming its Future: Some Do's and Don'ts', Remarks of Joshua D Wright, Commissioner FTC at the US Chamber of Commerce (21 May 2015 accessed 2 Jan 2015) < [https://www.ftc.gov/system/files/documents/public\\_statements/644381/150521iotchamber.pdf](https://www.ftc.gov/system/files/documents/public_statements/644381/150521iotchamber.pdf)>

FTC, 'FTC Charges Data Brokers with Helping Scammer Take More Than \$7 Million from Consumers' Accounts' (12 Aug 2015 accessed 7 Mar 2016) <<https://www.ftc.gov/news-events/press-releases/2015/08/ftc-charges-data-brokers-helping-scammer-take-more-7-million>>

FTC, 'Who's Brokering your Data?' *FTC Consumer Information Blog* (12 Aug 2015 accessed 8 Mar 2016) < <https://www.consumer.ftc.gov/blog/whos-brokering-your-data>>

FTC, Prepared Statement of the Federal Trade Commission on Examining Ways to Improve Vehicle and Roadway Safety Before the Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, United States House of Representatives, Washington, D.C. (21 October 2015 accessed 25 May 2016) [https://www.ftc.gov/system/files/documents/public\\_statements/826551/151021vehiclesafetytestimony.pdf](https://www.ftc.gov/system/files/documents/public_statements/826551/151021vehiclesafetytestimony.pdf)

FTC, 'Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers: Court Also Enters \$4.1M Default Judgment Against Additional Defendant' Press Release (18 Feb 2016 accessed 23 Feb 2016) [https://www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive?utm\\_source=govdelivery](https://www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive?utm_source=govdelivery)>

FTC, 'United States Dept. of Commerce Letter to Vera Jourova, Commissioner for Justice, Consumers and Gender Equality', 23 Feb 2016 accessed 28 Feb 2016)  
<[https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu\\_us\\_privacy\\_shield\\_full\\_text.pdf](https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf)>

FTC 'ASUS settles FTC charges that insecure home routers and "cloud" services put consumer's privacy at risk' (23 February 2016 accessed 5 Apr 2016) <<https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-homerouters-cloud-services-put>>

FTC, 'ASUS Settles FTC Charges that Insecure Home Routers and "Cloud" Services put Consumers' Privacy at Risk' (23 Feb 2016 accessed 23 Feb 2016) <[https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put?utm\\_source=govdelivery](https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put?utm_source=govdelivery)>

FTC, 'Mobile Privacy Disclosures: Building Trust Through Transparency: A Federal Trade Commission Staff Report' (Feb 2013 accessed 17 Mar 2016) <  
<https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf>>

FTC, 'Statement of FTC Chairwoman Edith Ramirez on EU-U.S. Privacy Shield Framework' *Press Release* (29 Feb 2016 accessed 2 Mar 2016) <[https://www.ftc.gov/news-events/press-releases/2016/02/statement-ftc-chairwoman-edith-ramirez-eu-us-privacy-shield-0?utm\\_source=govdelivery](https://www.ftc.gov/news-events/press-releases/2016/02/statement-ftc-chairwoman-edith-ramirez-eu-us-privacy-shield-0?utm_source=govdelivery)>

FTC, 'FTC Releases Annual Summary of Consumer Complaints Press Release' (1 Mar 2016 accessed 2 Mar 2016) <[https://www.ftc.gov/news-events/press-releases/2016/03/ftc-releases-annual-summary-consumer-complaints?utm\\_source=govdelivery](https://www.ftc.gov/news-events/press-releases/2016/03/ftc-releases-annual-summary-consumer-complaints?utm_source=govdelivery)>

FTC, 'Prepared Statement of the Federal Trade Commission on *Opportunities and Challenges in Advancing Health Information Technology* Before the House Oversight and Government Reform Subcommittees on Information Technology and Health, Benefits and Administrative Rules' Washington DC (22 Mar 2016 accessed 24 Mar 2016)  
<[https://www.ftc.gov/system/files/documents/public\\_statements/941063/160322commtestimonyhealthinfo.pdf?utm\\_source=govdelivery](https://www.ftc.gov/system/files/documents/public_statements/941063/160322commtestimonyhealthinfo.pdf?utm_source=govdelivery)>

FTC, 'MOU between the US Federal Trade Commission and the Canadian Radio-television and Telecommunications Commission on Mutual Assistance in the Enforcement of Laws on Commercial Email and Telemarketing' (24 Mar 2016 accessed 26 Mar 2016)  
[https://www.ftc.gov/system/files/documents/cooperation\\_agreements/032416crtc mou2.pdf](https://www.ftc.gov/system/files/documents/cooperation_agreements/032416crtc mou2.pdf)

FTC, 'FTC Approves Final Order in Oracle Java Security Case' (29 Mar 2016 accessed 1 Apr 2016)  
<[https://www.ftc.gov/news-events/press-releases/2016/03/ftc-approves-final-order-oracle-java-security-case?utm\\_source=govdelivery](https://www.ftc.gov/news-events/press-releases/2016/03/ftc-approves-final-order-oracle-java-security-case?utm_source=govdelivery)>

FTC, 'Order to File a Special Report' *FTC Matter No P165402* (6 May 2016 accessed 6 May 2016) <  
<https://www.ftc.gov/system/files/attachments/press-releases/ftc-study-mobile-device-industrys-security-update-practices/160509mobilesecuritymodelorder.pdf>>

FTC, 'FTC to Study Mobile Device Industry's Security Update Practices' (9 May 2016 accessed 20 Sept 2016) <<https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices>>

FTC, 'Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission Before the Federal Communications Commission: In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services' (27 May 2016 accessed 30 Jun 2016) <https://www.ftc.gov/policy/policy-actions/advocacy-filings/2016/05/comment-staff-bureau-consumer-protection-federal>

FTC, 'Comment of the Staff of the Bureau of Consumer Protection and the Office of Policy Planning Before the NTIA: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things' (2 June 2016 accessed 2 June 2016) <[https://www.ftc.gov/system/files/documents/advocacy\\_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf](https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf)>

FTC, 'Commission Finds *LabMD* Liable for Unfair Data Security Practices' (29 Jul 2016 accessed 1 Aug 2016) <<https://www.ftc.gov/news-events/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices>>

FTC, 'Prepared Statement on Oversight of the Federal Trade Commission' *United States Senate* (27 Sept 2016 accessed 2 Oct 2016) [https://www.ftc.gov/system/files/documents/public\\_statements/986433/commission\\_testimony\\_oversight\\_senate\\_09272016.pdf](https://www.ftc.gov/system/files/documents/public_statements/986433/commission_testimony_oversight_senate_09272016.pdf)

FTC, 'RE Request for Comment on "Federal Automated Vehicles Policy," Docket No. NHTSA-2016-0090, Comment of the Director of the Bureau of Consumer Protection of the Federal Trade Commission' (21 Nov 2016 accessed 22 Nov 2016) <[https://www.ftc.gov/system/files/documents/advocacy\\_documents/comment-jessica-l-rich-director-bureau-consumer-protection-ftc-national-highway-traffic-safety/ntsb\\_letter\\_comment112116.pdf?utm\\_source=govdelivery](https://www.ftc.gov/system/files/documents/advocacy_documents/comment-jessica-l-rich-director-bureau-consumer-protection-ftc-national-highway-traffic-safety/ntsb_letter_comment112116.pdf?utm_source=govdelivery)>

FTC, 'IoT Home Inspector Challenge' (4 Jan 2017 accessed 15 Feb 2017) <<https://federalregister.gov/d/2016-31731>>

Federation Internationale de L'Automobile (FIA)

FIA, 'What Europeans think about Connected Cars' (Jan 2016 accessed 21 Apr 2016) <[http://www.fiaregion1.com/download/20160129\\_fia\\_survey\\_brochure\\_2016\\_web\\_fin\\_fin.PDF](http://www.fiaregion1.com/download/20160129_fia_survey_brochure_2016_web_fin_fin.PDF)>

FIA, 'What Europeans think about Connected Cars' (Jan 2016 accessed 2 Mar 2016) <[http://www.fiaregion1.com/download/myarmydata/fia\\_survey\\_brochure\\_2016\\_web.pdf](http://www.fiaregion1.com/download/myarmydata/fia_survey_brochure_2016_web.pdf)>

Feibus, Mike, 'Face It, You're Bored of the Smartwatch You Got last Christmas' *Fortune* (10 Apr 2016 accessed 11 Apr 2016) <<http://fortune.com/2016/04/10/wearables-smartwatch/>>

Ferguson, Adele, 'Cominsure exposed' *Sydney Morning Herald* (8 Mar 2016 accessed 2 Dec 2016) <<http://www.smh.com.au/interactive/2016/cominsure-exposed/heart-attack/>>

Fernandes, Clinton & Vijay Sivaraman, 'It's only the beginning: Metadata Retention laws and the Internet of Things' *Australian Journal of Telecommunications and the Digital Economy* 3(3) (2015) <http://telsoc.org/ajtde/index.php/ajtde/article/view/21>

Fernandes, Earlence, Jaeyeon Jung and Atul Prakash, 'Security Analysis of Emerging Smart Home Applications' in *Proceedings of 37th IEEE Symposium on Security and Privacy* (May 2016 accessed 5 May 2016) <<https://iotsecurity.eecs.umich.edu/>>

Ferrier Hodgson, 'Australian retail 20915: Welcome to The Hunger Games!' (Feb 2015 accessed 26 Apr 2016) <  
[http://www.ferrierhodgson.com/~media/Ferrier/Files/Documents/Publications/Retail/2015/AustralianRetail\\_2015\\_Welcome%20to%20the%20Hunger%20Games.pdf](http://www.ferrierhodgson.com/~media/Ferrier/Files/Documents/Publications/Retail/2015/AustralianRetail_2015_Welcome%20to%20the%20Hunger%20Games.pdf)>

Field, Emily, 'CPSC Chair Kaye Eyes Safety Risks in New Technologies' *LAW360* (8 Aug 2016 accessed 9 Aug 2016) < <http://www.law360.com/articles/824104/print?section=consumerprotection>>

Field, Sean, 'Six cyber security standards you need to know about if you're a Company Director or Board Member' *Maddocks* (8 Mar 2016 accessed 9 Mar 2016) <https://www.maddocks.com.au/six-cyber-security-standards-need-know-youre-company-director-board-member/>

Field, Sean, 'NIST Cybersecurity Framework Workshop - Day 1' *Maddocks* (17 May 2017 accessed 18 May 2017) <<https://www.maddocks.com.au/blog/nist-workshop/>>

Field, Sean, 'NIST Cybersecurity Framework Workshop - Day 2' *Maddocks* (23 May 2017 accessed 25 May 2017) <<https://www.maddocks.com.au/blog/nist-workshop-day2/>>

Finley, Klint, 'Tim Berners Lee, 'Inventor of the web', plots a radical overhaul of his creation' *WIRED* (4 Apr 2017 accessed 4 Apr 2017) [https://www.wired.com/2017/04/tim-berners-lee-inventor-web-plots-radical-overhaul-creation/?mbid=nl\\_4417\\_p2&CNDID=](https://www.wired.com/2017/04/tim-berners-lee-inventor-web-plots-radical-overhaul-creation/?mbid=nl_4417_p2&CNDID=)

Fisher Jake, 'Tesla Responds to Potential for its Cars to Unintentionally Drive Away in Self-Parking Mode' *ConsumerReports* (18 May 2016 accessed 2 Jun 2016) <http://www.consumerreports.org/car-safety/tesla-model-s-summon-self-parking-can-be-activated-unintentionally/>>

Fisher, Eli, 'Developments in Data Driven Law: A Discussion with Peter Leonard' *G+T* (23 Sept 2016 accessed 30 Sept 2016) <<https://www.gtlaw.com.au/?q=developments-data-driven-law-discussion-peter-leonard>>

Fisher, Jake 'Tesla to Fix Self-Parking Feature After Consumer Reports Raises Safety Concern' *Consumer Reports* (10 Feb 2016 accessed 2 Jun 2016) <<http://www.consumerreports.org/car-safety/tesla-fixes-self-parking-feature-after-consumer-reports-raises-safety-concern/>>

Fisher, Jake, 'Tesla to Fix Self-Parking Feature After Consumer Reports Raises Safety Concern: Summon mode now to come with additional protections' (10 February 2016 accessed 16 Jul 2016) <<http://www.consumerreports.org/car-safety/tesla-fixes-self-parking-feature-after-consumer-reports-raises-safety-concern/>>

Fisher, Senator Deb, 'Senators introduce Bipartisan Internet of Things Bill' *Press release* (1 Mar 2016 accessed 7 Mar 2016) <http://www.fischer.senate.gov/public/index.cfm/2016/3/senators-introduce-bipartisan-internet-of-things-bill>

Fitbit, 'Can someone take over my account?' Fitbit Help (n.d. accessed 10 Nov 2016) <[https://help.fitbit.com/articles/en\\_US/Help\\_article/1969](https://help.fitbit.com/articles/en_US/Help_article/1969)>

Fitbit, 'Is my Fitbit data secure' (n.d. accessed 10 Nov 2016) <[https://help.fitbit.com/articles/en\\_US/Help\\_article/1758/?l=en\\_US&fs=RelatedArticle](https://help.fitbit.com/articles/en_US/Help_article/1758/?l=en_US&fs=RelatedArticle)>

Fitzgerald, Michael, 'What the Internet of Things Could mean to consumers' *MIT Sloan Management Review* (10 Feb 2016 accessed 4 Apr 2016) <http://sloanreview.mit.edu/article/what-the-internet-of-things-could-mean-to-consumers/>

Forbath, Theodore, 'The third wave of computing' *Forbes* (3 Oct 2015 accessed 25 Apr 2016) <http://fortune.com/2013/13/1003/the-third-wave-of-computing/>>

Foley, 'IoT – it's all about the data, right?' (25 Feb 2015 accessed 2 Jan 2016) <<http://www.lexology.com/library/detail.aspx?g=35530642-c249-46fd-bebf-d295529d71a6>>

Forder, Jay & Dan Svantesson, *Internet & Ecommerce Law* (Oxford University Press, 2010)  
Fortinet, 'Fortinet Reveals Internet of Things: Connected Home' Survey Results (23 Jun 2014 accessed 2 Jun 2016) < <http://investor.fortinet.com/releasedetail.cfm?releaseid=855992>>

Fox2Now, 'The FCC just gave you a little more control over your online privacy' CNN Wires (28 Oct 2016 accessed 2 Nov 2016) <http://fox2now.com/2016/10/28/the-fcc-just-gave-you-a-little-more-control-over-your-online-privacy/>

Franceschi-Bicchierai, Lorenzo, 'When the Internet of Things Starts to Feel Like the Internet of Shit' *Motherboard* (17 Dec 2015 accessed 3 Jun 2016) <<https://motherboard.vice.com/read/when-the-internet-of-things-starts-to-feel-like-the-internet-of-shit>>

Franceschi-Bicchierai, Lorenzo, 'Hackers Stole 65 Million Passwords from Tumblr, New Analysis Reveals' *Motherboard* (30 May 2016 accessed 3 Jun 2016) < <http://motherboard.vice.com/read/hackers-stole-68-million-passwords-from-tumblr-new-analysis-reveals>>

Frerichs, Sabine, 'False promises? A Sociological Critique of the Behavioural Turn in Law and Economics' *J Consum Policy* (2011) 34: 289 - 314  
<<http://web.b.ebscohost.com.ezproxy.bond.edu.au/ehost/pdfviewer/pdfviewer?sid=2248341d-ca16-422e-950b-56853adeb34a%40sessionmgr102&vid=1&hid=116>>

Frew, James, 'The Internet of Things: 10 useful Products you must Try in 2016' *makeuseof* <<http://www.makeuseof.com/tag/internet-things-10-useful-products-must-try-2016/>>

Fung, Brian, 'Here's the scariest part about the Internet of Things' *The Washington Post* (19 Nov 2013 accessed 2 Jan 2016) <https://www.washingtonpost.com/news/the-switch/wp/2013/11/19/heres-the-scariest-part-about-the-internet-of-things/>

Future of Life Institute, 'Asilomar AI Principles' (2017 accessed 20 Feb 2017) <<https://futureoflife.org/ai-principles/>>

Future of Life, 'AI Open Letter' citing Stuart Russell, Daniel Dewey and Max Tegmark, 'Research priorities for Robust and Beneficial Artificial Intelligence' *Association for the Advancement of Artificial Intelligence* (Winter 2015 accessed 25 May 2016) <<http://futureoflife.org/ai-open-letter>>

## G

Gamer, Noah, 'Your IoT device: How much data should it collect?' *ECN Magazine* (31 Mar 2015 accessed 4 Apr 2016) <<https://www.ecnmag.com/blog/2015/03/your-iot-device-how-much-data-should-it-collect>>

Gao, Lingling & Xuesong Bai 'A unified perspective of internet of things technology' *Asia pacific journal of marketing and logistics* 26(2) (2014 accesses 6 Mar 2016) <http://www.emeraldinsight.com.ezproxy.bond.edu.au/doi/pdfplus/10.1108/APJML-06-2013-0061>

Garber, Megan, 'When Algorithms Take the Stand' *The Atlantic* (30 Jun 2016 accessed 10 Feb 2017) <<https://www.theatlantic.com/technology/archive/2016/06/when-algorithms-take-the-stand/489566/>>

Garcia, Flavia D., David Oswald, Timo Kasper and Pierre Pavlides, 'Lock It and Still Lose It – On the (In)Security of Automotive Remote Keyless Entry Systems' *Proceedings of the 25th USENIX Security Symposium August 10–12, 2016 Austin, TX* <<https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia>>

Gardner, Stephen, 'World's Data Protection Leaders Highlight Internet of Things, Big Data Privacy Risks' *Bloomberg Law* (20 Oct 2014 accessed 7 Feb 2016) <<http://www.bna.com/worlds-data-protection-n17179897174/>>

Gartner, 'Forecast: The Internet of Things, Worldwide, 2013' (2013 accessed 19 Nov 2015) <<http://www.gartner.com/document/2625419?ref=QuickSearch&sthkw=G00259115>>

Gartner, 'Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020' (12 December 2013 accessed 3 Mar 2016) <<http://www.gartner.com/newsroom/id/2636073>>

Gartner, 'Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015' *Press Release* (11 Nov 2014 accessed 5 Mar 2016) <<http://www.gartner.com/newsroom/id/2905717>>

Gartner, '2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organisations Should Monitor' *Press Release* (18 Aug 2015 accessed 4 Mar 2016) <http://www.gartner.com/newsroom/id/3114217>

Gartner, "Gartner Says Worldwide Wearable Devices Sales to Grow 18.4 Percent in 2016' *Press Release* (2 Feb 2016 accessed 29 Mar 2016) <<http://www.gartner.com/newsroom/id/3198018>>

Gartner, 'Gartner Says Worldwide IoT Security Spending to Reach \$348 Million in 2016' (25 Apr 2016 accessed 30 Apr 2016) <<http://www.gartner.com/newsroom/id/3291817>>

Genser, Nalani, 'A New experience model for the smart home and consumer IoT' *Endeavour Partners* (Jan 2016 accessed 26 Mar 2016) <http://endeavourpartners.net/assets/Endeavour-Partners-A-New-Experience-Model-for-Consumer-IoT-Jan-2016.pdf>

Georgia Tech, 'Comment to NTIA' (13 Mar 2017 accessed 15 Mar 2017)  
<[https://www.ntia.doc.gov/files/ntia/publications/wireless\\_erc\\_cacp\\_-\\_final.pdf](https://www.ntia.doc.gov/files/ntia/publications/wireless_erc_cacp_-_final.pdf)>

Gerbis, Nicholas, '10 Nightmare Scenarios from the Internet of Things' *Tech*  
<<http://computer.howstuffworks.com/10-nightmare-scenarios-from-internet-of-things.htm/printable>>

Gershman, Jacob, 'Prosecutors say Fitbit Device Exposed Fibbing in Rape Case' *The Wall Street Journal Law Blog* (21 Apr 2016 accessed 2 May 2016) <  
<http://blogs.wsj.com/law/2016/04/21/prosecutors-say-fitbit-device-exposed-fibbing-in-rape-case/>>

Gibbs, Samuel, 'Privacy fears over 'smart' Barbie that can listen to your kids' *The Guardian* (13 Mar 2015 accessed 10 May 2016) < <https://www.theguardian.com/technology/2015/mar/13/smart-barbie-that-can-listen-to-your-kids-privacy-fears-mattel>>

Gibbs, Samuel, 'Hackers can hijack Wi-Fi Hello Barbie to spy on your children' *The Guardian* (26 Nov 2015 accessed 10 May 2016) < <https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children>>

Gibbs, Samuel, 'Samsung's voice-recording smart TVs breach privacy law, campaigners claim' (28 Feb 2015 accessed 10 May 2016) < <https://www.theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim>>

Gibbs, Samuel, 'Jeep owners urged to update their cars after hackers take remote control' *The Guardian* (22 Jul 2015 accessed 16 Mar 2016) <  
<http://www.theguardian.com/technology/2015/jul/21/jeep-owners-urged-update-car-software-hackers-remote-control>>

Gibbs, Samuel, 'What happens when Tesla's AutoPilot goes wrong: owners post swerving videos' 21 Oct 2015 accessed 16 Mar 2016) *The Guardian*  
<https://www.theguardian.com/technology/2015/oct/21/tesla-autopilot-goes-wrong-videos>

Gibbs, Samuel, 'Samsung SmartThings Hub review: an Internet of Things to rule them all?' *The Guardian* (8 Feb 2016 accessed 20 Mar 2016)  
<https://www.theguardian.com/technology/2016/feb/08/samsung-smarthings-hub-review-internet-of-things>

Gibbs, Samuel, 'Amazon Echo review: the best combined speaker and voice assistant in the UK' (21 Nov 2016 accessed 21 Nov 2016) <https://www.theguardian.com/technology/2016/nov/21/amazon-echo-review-the-best-combined-speaker-and-voice-assistant-in-the-uk>

Gibbs, Samuel, 'Self-driving cars: who's building them and how do they work?' *The Guardian* (16 May 2016 accessed 27 May 2016) < <https://www.theguardian.com/technology/2016/may/26/self-driving-cars-whos-building-them-and-how-do-they-work>>

Gibbs, Samuel, 'Tesla model X glitches lock owners out of cars' *The Guardian* (21 Apr 2016 accessed 21 Apr 2016) [https://www.theguardian.com/technology/2016/apr/21/tesla-model-x-glitches-lock-owners-out-of-cars-suv?utm\\_source=esp&utm\\_medium=Email&utm\\_campaign=GU+Today+USA+-+Version+CB+header&utm\\_term=168344&subid=18035608&CMP=ema\\_565](https://www.theguardian.com/technology/2016/apr/21/tesla-model-x-glitches-lock-owners-out-of-cars-suv?utm_source=esp&utm_medium=Email&utm_campaign=GU+Today+USA+-+Version+CB+header&utm_term=168344&subid=18035608&CMP=ema_565)

Gibbs, Samuel, 'What is the internet of things and how does ARM fit in?' *The Guardian* (18 Jul 2016 accessed 18 Jul 2016) <<https://www.theguardian.com/technology/2016/jul/18/what-is-the-internet-of-things-arm-holdings-softbank>>

Gibbs, Samuel, 'Uber riders to be able to hail self-driving cars for the first time' *The Guardian* (19 Aug 2016 accessed 21 Aug 2016) <<https://www.theguardian.com/technology/2016/aug/18/uber-riders-self-driving-cars>>

Giffi, Craig A., Joe Vitale, Ryan Robinson, Gina Pingitore, 'The race to autonomous driving, Winning American consumers' trust' *Deloitte Review* (23 Jan 2017 accessed 2 Feb 2017) <[https://dupress.deloitte.com/content/dam/dup-us-en/articles/3565\\_Race-to-autonomous-driving/DR20\\_The%20race%20to%20autonomous%20driving\\_reprint.pdf](https://dupress.deloitte.com/content/dam/dup-us-en/articles/3565_Race-to-autonomous-driving/DR20_The%20race%20to%20autonomous%20driving_reprint.pdf)>

Gilbert & Tobin, 'Singtel Optus Pty Ltd v ACCC' (27 Apr 2012 accessed 20 Apr 2015) <<http://www.lexology.com/library/detail.aspx?g=46cac7c5-c732-4001-b553-98f620b75935>>

Gilbert, Arlo 'The time that Tony Fadell sold me a container of hummus' *Blog* (3 Apr 2016 accessed 2 Sept 2016) <<https://arlogilbert.com/the-time-that-tony-fadell-sold-me-a-container-of-hummus-cb0941c762c1#.3r06trom>>

Glance, David, 'New Ways your smartwatch (and phone) may be spying on you. How worried should you be?' *The Conversation* (6 Jan 2016 accessed 6 Jan 2016) <<http://theconversation.com/new-ways-your-smartwatch-and-phone-may-be-spying-on-you-how-worried-should-you-be-52781>>

Glancy, Dorothy J., 'Autonomous and Automated and Connected Cars - Oh My: First Generation Autonomous Cars in the Legal Ecosystem' (2015) 16 *Minnesota Journal of Law, Science and Technology* 619

Glancy, D.J., R. W. Petersen & K. F. Graham, 'A Look at the Legal Environment for Driverless Vehicles' *National Cooperative Highway Research Program* (Feb 2016 accessed 6 May 2016) <[http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp\\_lrd\\_069.pdf](http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_lrd_069.pdf)>

Gogarty, Brendan and Meredith Hagger, 'The Laws of Man Over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air' (2008) 19 *Journal of Law, Information and Science* 124–32

Golding, Paul, 'Apportioning Security Risk and the GDPR' *The IT Law Community* (19 Jan 2016 accessed 22 Apr 2016) <<http://www.scl.org/site.aspx?i=ed46195>>

Golle, Philippe and Kurt Partridge 'Your Morning Commute Is Unique: On The Anonymity Of Home/Work Location Pairs' (13 May 2009 accessed 3 Aug 2016) <<https://33bits.org/2009/05/13/your-morning-commute-is-unique-on-the-anonymity-of-homework-location-pairs/>>

Golle, Philippe and Kurt Partridge, 'On the anonymity of Home/ Work Location pairs' Stanford University (n.d. accessed 3 Aug 2016) <<http://crypto.stanford.edu/~pgolle/papers/commute.pdf>>;

Golson, Jordan, 'Read the Florida Highway patrol's full investigation into the fatal Tesla crash' *The Verge* (1 Feb 2017 accessed 20 Feb 2017) <<http://www.theverge.com/2017/2/1/14458662/tesla-autopilot-crash-accident-florida-fatal-highway-patrol-report>>

Goodman, Bryce & Seth Flaxman 'EU regulations on algorithmic decision-making and a 'right to explanation' 2016 ICML Workshop on Human Interpretability in Machine Learning (WHI 2016), New York, NY, USA <http://arxiv.org/pdf/1606.08813v1.pdf>

Goodwin, Matt, 'Toothless Tiger...Now with Teeth' *Pigott Stinson* (3 Sept 2013 accessed 20 Apr 2015) <<http://pigott.com.au/publications/toothless-tigernow-with-teeth/>>

Google, 'Self-Driving Car Project Monthly Report' (Jan 2016 accessed 8 Apr 2016) <<https://www.google.com/selfdrivingcar/reports/>>

Google, 'Google Self-Driving Car Project Monthly Report' (Feb 2016 accessed 8 Apr 2016) <http://static.googleusercontent.com/media/www.google.com/en//selfdrivingcar/files/reports/report-0216.pdf>

Google, 'Self-Driving Car Project Monthly Report July 216' (31 Jul 2016 accessed 12 Aug 2016) <<https://static.googleusercontent.com/media/www.google.com/en//selfdrivingcar/files/reports/report-0716.pdf>>

Gray, Anthony, 'Unfair Contract Terms: Termination for Convenience' (2013) *University of Western Australia Law Review* 229 [http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/UWALawRw/2013/12.html?stem=0&synonyms=0&query="australian%20consumer%20law"%20section%2023](http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/UWALawRw/2013/12.html?stem=0&synonyms=0&query=)

Green, Leslie D., 'Surfing the Internet of Things: Industry still sorting out complex network' *Crains Detroit Business* (13 March 13, 2016 accessed 13 Mar 2016) <<http://www.crainsdetroit.com/article/20160313/NEWS/303139993/surfing-the-internet-of-things-industry-still-sorting-out-complex>>

Greenberg, Andy 'Hackers reveal Nasty New Car Attacks – with me behind the Wheel' *Forbes* (24 Jul 2013 accessed 3 Mar 2016) < <http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#6741c6765bf2>>

Greenberg, Andy, 'Radio Attack Lets Hackers Steal 24 Different Car Models', *WIRED* (21 Mar 2016 accessed 12 Aug 2016) < <https://www.wired.com/2016/03/study-finds-24-car-models-open-unlockingignition-hack/>>

Greenberg, Andy, 'Flaws in Samsung's 'Smart' Home let hackers unlock doors and set off fire alarms' *WIRED* (5 May 2016 accessed 12 Aug 2016) <<https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlock-doors-set-off-fire-alarms/>>

Greenberg, Andy, 'The Jeep Hackers are back to prove car hacking can get much worse' *WIRED* (1 Aug 2016 accessed 2 Aug 2016) < <https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/>>

Greenberg, Andy, 'A New Wireless Hack Can Unlock 100 Million Volkswagens' *WIRED* (10 Aug 2016 accessed 12 Aug 2016) <https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/>>

Greenberg, Andy, 'Chrysler launches Detroit's First Bug Bounty for Hackers' *WIRED* (13 Sept 2016 accessed 20 Oct 2016) <https://www.wired.com/2016/07/chrysler-launches-detroits-first-bug-bounty-hackers/>

Greenberg, Andy, 'It's finally legal to hack your own devices (even your car)' *WIRED* (31 Oct 2016 accessed 2 Nov 2016) <[https://www.wired.com/2016/10/hacking-car-pacemaker-toaster-just-became-legal/?mbid=nl\\_11116\\_p3&CNDID=>](https://www.wired.com/2016/10/hacking-car-pacemaker-toaster-just-became-legal/?mbid=nl_11116_p3&CNDID=>)

Greenberg, Andy, 'Android Phone hacks could unlock Millions of Cars' *WIRED* (16 Feb 2017 accessed 16 Feb 2017) <[https://www.wired.com/2017/02/hacked-android-phones-unlock-millions-cars/?mbid=nl\\_21717\\_p8&CNDID=>](https://www.wired.com/2017/02/hacked-android-phones-unlock-millions-cars/?mbid=nl_21717_p8&CNDID=>)

Greenberg, Andy, 'Securing driverless cars from hackers is hard. Ask the ex-Uber guy who protects them' ' *WIRED* (12 Apr 2017 accessed 13 Apr 2017) <https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/>

Greenberg, DM, S Baron-Cohen, DJ Stillwell, M Kosinski and PJ Rentfrow, 'Musical Preferences are Linked to Cognitive Styles' (2015) *PLoS ONE* 10(7): e0131151 <<https://doi.org/10.1371/journal.pone.0131151>>

Greenfield, Rebecca, 'Elon Musk's Data Doesn't Back Up His Claims of New York Times Fakery' *The Atlantic Wire* (14 Feb 2013 accessed 16 Mar 2016) <<http://www.theatlanticwire.com/technology/2013/02/elon-musks-data-doesnt-back-his-claims-new-york-times-fakery/62149/>>

Greenleaf, Graham 'Is it too late to protect privacy? Pessimism reigns over big data and the law' *UNSW* (15 Sept 2014 accessed 8 Aug 2016) <http://newsroom.unsw.edu.au/news/law/it-too-late-protect-privacy-pessimism-reigns-over-big-data-and-law>

Greenleaf, Graham, 'Foreword: Abandon all Hope?' 37(2) (2014) UNSWLJ 636- 642 <<http://www.unswlawjournal.unsw.edu.au/sites/default/files/foreword.pdf>>

Griffith Hack, 'Parking app perils show value of privacy impact assessments' (18 May 2016 accessed 19 May 2016) <<http://www.lexology.com/library/detail.aspx?g=f6369b47-25fc-47a2-8297-d4f009a1fce9>>

Griffith, Chris 'Malware cripples Australian Apple iCloud accounts' *The Australian* (29 May 2014 accessed 29 July 2014) <<http://www.theaustralian.com.au/technology/malware-cripples-australian-apple-icloud-accounts/story-e6frgakx-1226935680356>>

Griffith, Erin 'Fixing Twitter' *Fortune* (8 Mar 2016 accessed 8 Mar 2016) <<http://fortune.com/fixing-twitter-jack-dorsey/>>

Griffith, Gabriella, 'Encouraging clicks with moment marketing' *Raconteur, The Times* (28 January 2016 accessed 1st February 2016) <<http://raconteur.net/business/encouraging-clicks-with-moment-marketing>>

Griffith, Gabriella, 'Top 5 Digital marketing tips' *Raconteur, The Times* (28 January 2016 accessed 1st February 2016) <<http://raconteur.net/business/top-5-digital-marketing-tips>>

Groopman, J & Susan Etlinger, 'Consumer Perceptions of Privacy in the Internet of Things' *Altimeter* (June 2015 accessed 12 Apr 2016) < <http://www.altimetergroup.com/pdf/reports/Consumer-Perceptions-Privacy-IoT-Altimeter-Group.pdf>>

Gross, Grant 'Privacy groups want investigation of big data acquisitions' *CIO* (7 Feb 2015 accessed 22 Nov 2016) < <http://www.cio.com.au/article/565755/privacy-groups-want-investigation-big-data-acquisitions/>>

Grosse, Neil, '21 Ideas for the twentieth-first century' *Businessweek Online* (30 Aug 1999 accessed 16 Mar 2016) [http://www.businessweek.com/1999/99\\_35/b3644024.htm](http://www.businessweek.com/1999/99_35/b3644024.htm) LINK BROKESN

Grosse, Neil, 'Q&A: An Internet Pioneer Moves toward Nomadic Computing' *Businessweek Online* (30 Aug 1999 accessed 16 Mar 2016) < [http://www.businessweek.com/1999/99\\_35/b3644024.htm](http://www.businessweek.com/1999/99_35/b3644024.htm)> LINK BROKEN

Grossman, Lev, 'Here's the Full Transcript of TIME's Interview with Apple CEO Tim Cook' *Time Magazine* (17 Mar 2016 accessed 18 Mar 2016) < <http://time.com/4261796/tim-cook-transcript/>>

Grossman, Lev, 'Inside Apple CEO Tim Cook's Fight With the FBI' *Time Magazine* (17 Mar 2016 accessed 18 Mar 2016) < <http://time.com/4262480/tim-cook-apple-fbi-2/>>

Gutierrez, Peter, 'IoTAA releases IoT security guidelines' *IoT Hub* (28 Feb 2017 accessed 4 Mar 2017) <<https://www.iothub.com.au/news/iotaa-releases-iot-security-guidelines-452893>>

### **Groupe Spécial Mobile Association (GSMA)**

GSMA, 'Connected Car Forecast: Global Connected Car Market to Grow Threefold Within Five Years' (3 Feb 2013 accessed 10 Dec 2015) <[https://www.gsma.com/iot/wp-content/uploads/2013/06/cl\\_ma\\_forecast\\_06\\_13.pdf](https://www.gsma.com/iot/wp-content/uploads/2013/06/cl_ma_forecast_06_13.pdf)>

GSMA, 'The Impact of the Internet of Things' *KRC Research* (2015 accessed 2 Sept 2016) <<http://www.gsma.com/newsroom/wp-content/uploads/15625-Connected-Living-Report.pdf>>

GSMA, 'IoT Privacy by Design Decision Tree' (8 May 2015 accessed 8 Mar 2016) <<http://www.gsma.com/iot/iot-knowledgebase/iot-privacy-design-decision-tree/>>

GSMA, 'Competition policy in the Digital Age: A Practical handbook' (Oct 2015 accessed 2 Aug 2016) <http://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/Competition-Policy-Handbook.pdf>

GSMA, 'Unlocking the Value of IoT Through Big Data' (11 December 2015 accessed 2 Apr 2016) < [http://www.gsma.com/connectedliving/wp-content/uploads/2015/12/cl\\_iot\\_bigdata\\_11\\_15-004.pdf](http://www.gsma.com/connectedliving/wp-content/uploads/2015/12/cl_iot_bigdata_11_15-004.pdf)>

GSMA, 'IoT Security Guidelines Overview Document' (Feb 2016 accessed 2 Apr 2016) <<http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.11-v1.1.pdf>>

GSMA, 'Automotive IoT Security: Countering the Most Common Forms of Attack' (22 March 2016 accessed 2 Apr 2016) < <http://www.gsma.com/connectedliving/automotive-iot-security-countering-the-most-common-forms-of-attack/>>

Gunning, Patrick, 'All Steamed Up About Consumer Guarantees' *King & Wood Mallesons InCompetition* (9 Sept 2014 accessed 11 Apr 2016) <http://incompetition.com.au/2014/09/steamed/>

## H

Hackett, Robert, 'Linkedin Lost 167 Million Account Credentials in Data Breach' *Fortune* (18 May 2016 accessed 4 Jun 2016) <<http://fortune.com/2016/05/18/linkedin-data-breach-email-password/>>

Hackett, Robert 'Google Found Disastrous Symantec and Norton Vulnerabilities That Are 'As Bad as It Gets' *Fortune* (29 Jun 2016 accessed 3 Jul 2016) <<http://fortune.com/2016/06/29/symantec-norton-vulnerability/>>

Hackett, Robert, 'Why you should care about Microsoft's latest legal battle' *Fortune* (8 Sept 2015 accessed 16 Jul 2016) <<http://fortune.com/2015/09/08/microsoft-legal-battle-why-care/>>

Hales, Lydia, 'Technology that can help you improve your sleep' *ABC News* (22 Oct 2016) <<http://www.abc.net.au/news/health/technology-that-can-help-you-improve-your-sleep/7944228>>

Halliday, James & Rebecca Lam, 'Internet of Things: Some Legal and Regulatory Implications' (26 Feb 2016 accessed 7 Apr 2016) <<http://www.lexology.com/library/detail.aspx?g=988064c6-0bc2-4657-90d6-f9bf85fa0adc>>

Halliday, James & Rebekah Lam, 'Internet of Things - Just Hype or the Next Big Thing?' (2015) 34(3) *Communications Law Bulletin* 7 <[http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/CommsLawB/2015/14.html?stem=0&synonyms=0&query="internet%20of%20things](http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/CommsLawB/2015/14.html?stem=0&synonyms=0&query=)>

Halliday, James; Lam, Rebekah, 'Internet of Things - Is it Hype or the Next Big Thing? - Part II' (2016) 34(4) *Communications Law Bulletin* 4 <[http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/CommsLawB/2016/2.html?stem=0&synonyms=0&query="internet%20of%20things](http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/CommsLawB/2016/2.html?stem=0&synonyms=0&query=)>

Hamblen, Matt, 'After DDOS attack, senator seeks industry-led security standards for IoT devices' *Computerworld* (28 Oct 2016 accessed 5 Nov 2016) <<http://www.computerworld.com/article/3136650/security/after-ddos-attack-senator-seeks-industry-led-security-standards-for-iot-devices.html>>

Hamilton, David, 'The Four Internet of Things Connectivity Models Explained' (29 Apr 2016 accessed 2 Mar 2016) <<http://www.thewhir.com/web-hosting-news/the-four-internet-of-things-connectivity-models-explained>>

Hann, Graham 'There's spam in my fridge!' *Taylor Wessing* (Feb 2014 accessed 19 Nov 2015) <[http://united-kingdom.taylorwessing.com/download/article\\_spam\\_fridge.html](http://united-kingdom.taylorwessing.com/download/article_spam_fridge.html)>

Harris, Mark, 'California lawmaker pushes for driver-free robot car testing on public roads' *The Guardian* (26 Mar 2016 accessed 10 Mar 2016) <<https://www.theguardian.com/technology/2016/mar/25/california-self-driving-car-bill-google>>

Harris, Mark, 'Google reports self-driving car mistakes: 272 failures and 13 near misses' *The Guardian* (13 Jan 2016 accessed 12 Apr 2016) <<https://www.theguardian.com/technology/2016/jan/12/google-self-driving-cars-mistakes-data-reports>>

Harris, Tristan, 'How technology Hijacks People's Minds – from a Magician and Google's Design Ethicist' *Blog* (18 May 2016 accessed 25 May 2016) <https://medium.com/@tristanharris/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3#.7r7htsyyz>

Havens, John C., 'The ethics of AI: how to stop your robot cooking your cat' *The Guardian* (23 Jun 2015 accessed 21 Apr 2016) <<http://www.theguardian.com/sustainable-business/2015/jun/23/the-ethics-of-ai-how-to-stop-your-robot-cooking-your-cat>>

Hawking, Stephen, Stuart Russell, Max Tegmark, Frank Wilczek, 'Stephen Hawking: 'Transcendence looks at the implications of artificial intelligence - but are we taking AI seriously enough?' *The Independent* (2 May 2014 accessed 26 May 2016) <<http://www.independent.co.uk/news/science/stephen-hawking-transcendence-looks-at-the-implications-of-artificial-intelligence-but-are-we-taking-9313474.html>>

Hawkins, Andrew J., 'Delphi and Mobileye are teaming up to build a self-driving system by 2019' *The VERGE* (23 Aug 2016 accessed 15 Aug 2016) <<http://www.theverge.com/2016/8/23/12603624/delphi-mobileye-self-driving-autonomous-car-2019>>

Hawkins, Andrew J., 'Self-driving cars will have to pry the steering wheel from our cold, dead hands, poll says' *THE VERGE* (28 Sept 2016 accessed 2 Oct 2016) <<http://www.theverge.com/2016/9/28/13076948/self-driving-car-poll-autonomy-kelley-blue-book>>

Hawkins, Andrew J., 'Fatal Tesla Autopilot accident investigation ends with no recall ordered' *THE VERGE* (19 Jan 2017 accessed 25 Jan 2017) <<https://www.theverge.com/2017/1/19/14323990/tesla-autopilot-fatal-accident-nhtsa-investigation-ends>>

Heath, Nick 'I know what you ate last supper: What home sensors will reveal about your life' *Techrepublic* (5 Feb 2-014 accessed 4 Mar 2-16) <<http://www.techrepublic.com/blog/european-technology/i-know-what-you-ate-last-supper-what-home-sensors-will-reveal-about-your-life/>>

Helberger, Natalie, 'Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law' *University of Amsterdam - Institute for Information Law (IViR)* (6 February 6, 2016 accessed 3 Jun 2016) <<http://ssrn.com/abstract=2728717>>

Hepworth, Annabel, 'ACCC: 'rogues don't care about penalties' *The Australian* (16 Apr 2016 accessed 2 Aug 2016) <<http://www.theaustralian.com.au/business/accc-rogues-dont-care-about-penalties/news-story/0bbdf40e76bd23c3ae273f54455b0a60>>

Herbert Smith Freehills, 'Unfair Contract Terms Checklist' (October 2016 accessed 12 Oct 2016) <https://www.herbertsmithfreehills.com/latest-thinking/imminent-changes-to-unfair-contract-terms-regime>

Hern, Alex, 'Samsung rejects concern over 'Orwellian' privacy policy' *The Guardian* (9 Feb 2015 accessed 10 May 2016) <<https://www.theguardian.com/technology/2015/feb/09/samsung-rejects-concern-over-orwellian-privacy-policy>>

Hern, Alex, 'Facebook's 'ethnic affinity' advertising sparks concerns of racial profiling' *The Guardian* (22 Mar 2016 accessed 22 Mar 2016) <<https://www.theguardian.com/technology/2016/mar/22/facebooks-ethnic-affinity-advertising-concerns-racial-profiling>>

Hern, Alex, 'Germany calls on Tesla to drop 'Autopilot' branding' *The Guardian* (17 Oct 2016 accessed 17 Oct 2016) <<https://www.theguardian.com/technology/2016/oct/17/germany-calls-on-tesla-to-drop-autopilot-branding>>

Hern, Alex, 'Is Apple's next product an electric car?' *The Guardian* (21 Apr 2016 accessed 21 Apr 2016) <<https://www.theguardian.com/technology/2016/apr/21/is-apple-next-product-an-electric-car-telsa>>

Hern, Alex, 'QuadRooter Android bug could affect almost 1bn phones, researchers claim' *The guardian* (8 Aug 2016 accessed 9 Aug 2016) <<https://www.theguardian.com/technology/2016/aug/08/quadrooter-android-bug-phones-hackers-smartphone>>

Hern, Alex, 'CloudPets stuffed toys leak details of half a million users' *The Guardian* (1 Mar 2017 accessed 14 Mar 2017) <<https://www.theguardian.com/technology/2017/feb/28/cloudpets-data-breach-leaks-details-of-500000-children-and-adults>>

Herridge, Catherine and Pamela K. Browne, 'Romanian Hacker Guccifer: I breached Clinton server, "it was easy"' *news.com.au* (5 May 2016 accessed 5 May 2016) <<http://www.news.com.au/finance/work/leaders/romanian-hacker-guccifer-i-breached-clinton-server-it-was-easy/news-story/f69b0f7537158cdef16fb0454b873932>>

Hewlett Packard, 'How safe are home security systems? An HPE study on IoT security' (Nov 2015 accessed 6 Apr 2016) <<http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-7342ENW.pdf>>

Hewlett Packard, 'Internet of things research study 2015 report' (2015 accessed 6 Apr 2016) <<http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf>>

Hewlett Packard, 'Internet of Things Security Study: Smartwatches' *Submission to FTC PrivacyCon 2016* (2016 accessed 6 Apr 2016) <[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00050-98093.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00050-98093.pdf)>

Heydon, Geoff & Frank Zeichner, 'Enabling the Internet of Things for Australia', *Communications Alliance Internet of Things Think Tank* (Oct 2015 accessed 5 Mar 2016) <[http://www.commsalliance.com.au/\\_\\_data/assets/pdf\\_file/0007/51991/Enabling-the-Internet-of-Things-for-Australia.pdf](http://www.commsalliance.com.au/__data/assets/pdf_file/0007/51991/Enabling-the-Internet-of-Things-for-Australia.pdf)>

Higgins, Tim, 'Tesla narrowly misses 2016 sales goal' *The Australian Business Review* (4 Jan 2017 accessed 22 Jan 2017) <<http://www.theaustralian.com.au/business/technology/tesla-narrowly-misses-2016-sales-goal/news-story/93b478343e30c55bb4fc738ace637b04?nk=e5744dc39742255a723213b360602648-1491343062>>

High, Peter, 'A Conversation with the Most Influential Cybersecurity Guru to the US Government' *Forbes* (7 Dec 2015 accessed 7 Apr 2016) <<http://www.forbes.com/sites/peterhigh/2015/12/07/a-conversation-with-the-most-influential-cybersecurity-guru-to-the-u-s-government/print/>>

Hill, Kashmir, 'How Your Security System Could Be Used to Spy on You' *Forbes* (23 Jul. 2014 accessed 18 Jan 2016) [www.forbes.com/sites/kashmirhill/2014/07/23/how-your-security-system-could-be-used-to-spy-on-you](http://www.forbes.com/sites/kashmirhill/2014/07/23/how-your-security-system-could-be-used-to-spy-on-you)

Hill, Kashmir, 'Facebook Added 'Research' To User Agreement 4 Months After Emotion Manipulation Study', *Forbes* (30 June 2014 accessed 30 July 2014) <<http://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-usersafter-emotion-manipulation-study/>>

Hill, Simona, 'Who's tracking your fitness tracker? We asked an expert' *Digital Trends* (19 March 2016 accessed 6 Apr 2016) < <http://www.digitaltrends.com/wearables/whos-tracking-your-fitness-tracker/>>

Hilton, Anthony, 'UK is hot target for Cybercrime' *Raconteur, The Times* (28 January 2016 28 January 2016 accessed 1st February 2016) <<http://raconteur.net/business/uk-is-hot-target-for-cybercrime>>

Hilts, Andrew, Christopher Parsons & Jeffrey Knockel, 'Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security', Open Effect & Citizen Lab, (2 Feb 2-016 accessed 16 Aug 2016) <[apo.org.au/files/Resource/every\\_step\\_you\\_fake.pdf](http://apo.org.au/files/Resource/every_step_you_fake.pdf)>

Hines, Nikolaus, 'Is Tesla the Netflix of Cars? Data Scientists Say Probably Not' *Inverse* (2016 accessed 20 Nov 2016) <https://www.inverse.com/article/13908-tesla-not-netflix-of-cars>

Hogan Lovell, 'Innovation and Regulation: An Uncomfortable Relationship?' (12 Oct 2016 accessed 13 Oct 2016) <<http://www.lexology.com/library/detail.aspx?g=e88ff74b-cdce-4680-a2b7-aba9239e38c1>>

Holdowsky, Jonathan, Monika Mahto, Michael E. Raynor and Mark Cotteleer, 'Inside the IOT: a primer on the technologies building the IoT' *Deloitte* (21 Aug 2015 accessed 5 Feb 2016) <https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-primer-iot-technologies-applications.html>

Holt, Alison 'Voluntary Code: Guidance for Sharing Data' *Oxford Internet Institute* \*Dec 2015 accessed 2 Aug 2017) < <https://www.oii.ox.ac.uk/blog/new-voluntary-code-guidance-for-sharing-data-between-organisations/>>

Hon, Kuan, 'Killing Cloud Quickly, with GDPR' *The IT Law Community* (4 Feb 2016 accessed 22 Apr 2-16) <<http://www.scl.org/site.aspx?i=ed46375>>

Hong, Nicole, 'For Consumers, Injury Is Hard to Prove in Data-Breach Cases', *The Wall Street Journal* (26 June 2016 accessed 5 Jul 2016) < <http://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988>>

Hong, W.P., 'Samsung shows that the internet of things is now "in sync with real life' *Samsung Newsroom* (8 Jan 2016 accessed 11 May 2016) <<https://www.news.samsung.com/global/Samsung-shows-that-the-internet-of-things-is-now-in-sync-with-real-life>>

Hoofnagle, Chris and Jan Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price' 61 *UCLA L. Rev.* 606 (2013-2014 accessed 10 Apr 2015) <<http://www.uclalawreview.org/pdf/61-3-2.pdf>>

Hoofnagle, Chris & Jennifer M Urban, 'Alan Westin's Privacy Homo Economicus' (1 Jun 2014 accessed 5 Apr 2016) 49 *Wake Forest L. Rev.* 261  
<[https://www.ftc.gov/system/files/documents/public\\_comments/2015/09/00003-97143.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/09/00003-97143.pdf)>

Hosain, Syed Zaeem, 'Reality Check: 50B IoT devices connected by 2020 – beyond the hype and into reality' *RCR Wireless News* (28 Jun 2016 accessed 2 Aug 2016)  
<<http://www.rcrwireless.com/20160628/opinion/reality-check-50b-iot-devices-connected-2020-beyond-hype-reality-tag10>>

Howard, Jeremy 'The wonderful and terrifying implications of computers that can learn' *TEDX Brussels* (Dec 2014 accessed 4 Jan 2016) <<https://youtu.be/xx310zm3tls>>

Hughes, Gordon and Lisa Di Marco, 'Online privacy policies – it's not just about the Privacy Act' *Internet Law Bulletin* (April 2015 accessed 2 May 2015) 38- 40.

Hughes, Gordon, and Andrew Sutherland, 'Enforcement problems with online contacts: an Uber case study' *Davies Collison Cave* (5 Oct 2016 accessed 10 Oct 2016) <<http://www.davies.com.au/ip-news/enforcement-problems-with-online-contacts-an-uber-case-study>>

Hull, Dana, 'Tesla owner in Autopilot crash won't sue, but car insurer might' *Automotive News, Bloomberg* (2016 accessed 28 Aug 2016)  
<<http://www.autonews.com/article/20160819/OEM06/160819822/tesla-owner-in-autopilot-crash-wont-sue-but-car-insurer-might>>

Hull, Dana, 'Tesla Breakup with Mobileye Turns Ugly' *Bloomberg* (16 Sept 2016 accessed 20 Sept 2016)  
<<https://www.bloomberg.com/news/articles/2016-09-16/tesla-says-mobileye-tried-to-block-its-auto-vision-capability>>

Hutchinson, Terry and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' *Deakin Law Review* 17: 1 (2012) <<https://ojs.deakin.edu.au/index.php/dlr/article/view/70>>

Hynd, David & Mike McCarthy, 'Study on the benefits resulting from the installation of Event Data Recorders: Final Report' *Transport Research Laboratory Published Project Report PPR707 2014*, prepared for the European Commission (2014 accessed 18 Mar 2016)  
[http://ec.europa.eu/transport/road\\_safety/pdf/vehicles/study\\_edr\\_2014.pdf](http://ec.europa.eu/transport/road_safety/pdf/vehicles/study_edr_2014.pdf)

I

IAB (US), 'Privacy and Tracking in a Post CookieWorld' *White Paper* (Jan 2014 accessed 9 Apr 2015) [7] <[http://www.iabaustralia.com.au/uploads/uploads/2014-11/1415289600\\_3ee3de01b67c04945704bce1e7964095.pdf](http://www.iabaustralia.com.au/uploads/uploads/2014-11/1415289600_3ee3de01b67c04945704bce1e7964095.pdf)>

I Am the Cavalry, 'Five Star Automotive Cyber Safety Framework' (2015 accessed 2 Sept 2016)  
<<https://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf>>

I Am The Cavalry, 'Hippocratic Oath for Connected Medical Devices', (19 Jan 2016 accessed 2 Sept 2016) <<https://www.iamthecavalry.org/wp-content/uploads/2016/01/I-Am-The-Cavalry-Hippocratic-Oath-for-Connected-Medical-Devices.pdf>>

IAPP-EY, 'Annual Privacy Governance Report 2015' (2015 accessed 6 Apr 2016) <[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00029-97820.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00029-97820.pdf)>

Ibrahim, Tony, 'Flatlining Monitors' 'testing fitness trackers with heart rate monitors – what we found' CHOICE (8 Sept 2016 accessed 20 Sept 2016) < <https://www.choice.com.au/health-and-body/diet-and-fitness/sportswear-and-shoes/articles/fitness-trackers-with-heart-rate-monitors-what-we-found>>

Icontrol Networks, '2015 State of the smart home report' (2015 accessed 20 Jul 2016) < file:///C:/Users/fudge\_000.ONCOMING-STORM/AppData/Local/Microsoft/Windows/INetCache/IE/U5AUANBP/Smart\_Home\_Report\_2015.pdf>

IDC, 'The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things' *EMC Digital Universe with Research & Analysis by IDC* (April 2014 accessed 29 Apr 2016) <http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm>

IDC Italia S.r.L and TXT e-solutions S.P.A. 'Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination' (13 May 2015 accessed 21 Apr 2017) < <https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination>>

IDC & TXT, 'Definition of a Research and innovation Policy Leveraging Cloud Computing and IoT Combination' European Commission (13 May 2015 accessed 10 Feb 2016): 9 <https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination>>

IDC, 'The Worldwide Wearables Market Leaps 126.9% in the Fourth Quarter and 171.6% in 2015, according to IDC' (23 Feb 2016 accessed 3 Apr 2016) < <http://www.idc.com/getdoc.jsp?containerId=prUS41037416>>

IDG UK, '15 Most Powerful Internet of Things Companies 2016' *Computerworld UK* (16 Dec 2015 accessed 10 Mar 2016) <<http://www.computerworlduk.com/galleries/data/12-most-powerful-internet-of-things-companies-3521713/#7>>

IEEE, 'Towards a definition of the Internet of things (IoT)' (27 May 2015 accessed 22 Mar 2016) < <http://iotbusinessnews.com/download/white-papers/IEEE-IoT-Towards-Definition-Internet-Of-Things.pdf>>

IEEE, 'Wearfit: Security Design Analysis of a Wearable Fitness Tracker' (2016 accessed 29 Apr 2016) <<http://www.computer.org/cms/CYBSI/docs/Wearfit.pdf>>

Independent Security Evaluators, 'Exploiting SOHO Routers: Case Studies' (2015 accessed 3 Dec 2016) <[http://securityevaluators.com/knowledge/case\\_studies/routers/soho\\_router\\_hacks.php](http://securityevaluators.com/knowledge/case_studies/routers/soho_router_hacks.php)>

Independent Security Evaluators, 'Technical Report' (2016 accessed 3 Mar 2016) <[http://securityevaluators.com/knowledge/case\\_studies/routers/soho\\_techreport.pdf](http://securityevaluators.com/knowledge/case_studies/routers/soho_techreport.pdf)>

InfoBright, 'Will the owner of the data please stand up?' (18 Jun 2014 accessed 3 Mar 2016) < <https://infobright.com/blog/will-owner-data-please-stand-up/>>

Information Accountability Foundation, 'Unified Ethical Frame for Big Data Analysis' *Draft* (March 2015 accessed 6 Apr 2016) < [https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00049-98091.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00049-98091.pdf)> and [https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00049-98092.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00049-98092.pdf)

Information & Privacy Commissioner of Ontario, 'Privacy by Design' (2013 accessed 5 Jan 2016) <<https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf>>

### **Information Commissioner's Office UK (ICO)**

ICO, 'Conducting privacy impact assessments code of practice' (Feb 2014 accessed 5 Mar 2016) <<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>>

ICO, 'Response to Ofcom consultation: 'Promoting investment and innovation in the Internet of Things'' (1 Oct 2014 accessed 2 Feb 2016) <<https://ico.org.uk/about-the-ico/consultations/ofcom-consultation-promoting-investment-and-innovation-in-the-internet-of-things/>>

ICO, 'Data sharing code of practice' (2016 accessed 20 Apr 2016) <[https://ico.org.uk/media/for-organisations/documents/1068/data\\_sharing\\_code\\_of\\_practice.pdf](https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf)>

ICO, 'Privacy notices, transparency and control – a code of practice on communicating privacy information to individuals' (24 Mar 2016 accessed 20 Apr 2016) <https://ico.org.uk/media/about-the-ico/privacy-notices-transparency-and-control-0-0.pdf>

ICO, 'Privacy notices, transparency and control' (7 Oct 2016 accessed 20 Oct 2016) < <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/>>

ICO, 'Privacy impact assessments' (7 Oct 2016 accessed 20 Oct 2016) <<https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/>>

ICO, 'Anonymisation Code of Practice' (accessed 8 Aug 2016 <<https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>>

ICO, 'Data sharing code of practice' (accessed 8 Aug 2016) <[https://ico.org.uk/media/for-organisations/documents/1068/data\\_sharing\\_code\\_of\\_practice.pdf](https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf)>

ICO, TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack ' (5 Oct 2016 accessed 20 Oct 2016) < <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/>>

Information is Beautiful, 'World's Biggest Data Breaches: selected losses greater than 30,000 records' (updated 30th Mar 2015 accessed 18 Apr 2015) <<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>>

Insurance Box, 'Journey data privacy policy' (n.d. accessed 2 Apr 2017) <<http://insurancebox.com.au/documents/privacy-promise.pdf>>

Insurance Council of Australia, 'Driverless Vehicles and Road Safety (inquiry)' *Submission* (8 Apr 2016 accessed 2 June 2016) <

<http://www.insurancecouncil.com.au/assets/submission/2016/Driverless%20Cars%20Submission%20to%20NSW%20Parliament.pdf>>

Insurance Council of Australia, 'Submission to the Australian Consumer Law review' *Submission* (27 May 2016 accessed 2 June 2016)

<[http://www.insurancecouncil.com.au/assets/submission/2016/2016\\_05\\_27\\_ICA\\_Submission\\_Australian\\_Consumer\\_Law\\_Review.pdf](http://www.insurancecouncil.com.au/assets/submission/2016/2016_05_27_ICA_Submission_Australian_Consumer_Law_Review.pdf)>

Insurance Council of Australia, Productivity Commission Inquiry into Data Availability and Use 'Submission (29 Jul 2016 accessed 4 Sept 2016)

<[http://www.insurancecouncil.com.au/assets/submission/2016/2016\\_07\\_29\\_Submission\\_PC\\_Data%20Access%20and%20Use.pdf](http://www.insurancecouncil.com.au/assets/submission/2016/2016_07_29_Submission_PC_Data%20Access%20and%20Use.pdf)>

Intel, 'Policy framework for the Internet of things (IoT)' (2014 accessed 2 Jan 2016) <

<http://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-iot-framework.pdf>>

Intel, 'A Guide to the Internet of Things Infographic' (2014 accessed 11 Apr 2016) <

<http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html>>

Intel, 'The Internet of things (IoT) and Automotive and Transport Policy Principles' (2014 accessed 2 Jan 2016) < <http://www.intel.com/content/www/us/en/policy/policy-iot-automotive-transportation.html>>

Intel, 'Internet of Things (IoT) Policy (n.d. accessed 2 Sept 2016)

<<http://www.intel.com/content/www/us/en/policy/policy-internet-of-things-iot.html>>

Intel, 'The Internet of things and healthcare policy principles' (n.d. accessed 2 Sept 2016)

<<http://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-iot-healthcare.pdf>>

### **International Consumer Protection and Enforcement Network (ICPEN)**

ICPEN, 'Mauritius Declaration on the Internet of Things' *International Conference of Data Protection and Privacy Commissioners*, (14 Oct 2014 accessed 12 Apr 2015) <

<http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf>>

ICPEN, 'Mauritius Declaration Resolution on Big Data' (15 Oct 2015 accessed 7 Feb 2016)

<<http://www.privacyconference2014.org/media/16427/Resolution-Big-Data.pdf>>

International Federation on Aging, 'Report on good practices in e-inclusion, ethical guidance and designing a dialogue roadmap' *The Senior Project* (2009 accessed 13 Apr 2016) <[http://www.ifa-fiv.org/wp-content/uploads/2012/12/059\\_Report-on-good-practices-ethical-guidance-15-Nov-09.pdf](http://www.ifa-fiv.org/wp-content/uploads/2012/12/059_Report-on-good-practices-ethical-guidance-15-Nov-09.pdf)>

Internet Society, 'The Internet of Things: An Overview Understanding the issues and challenges of a more connected World' (Oct 2015 accessed 18 Mar 2016)

<[https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014\\_0.pdf](https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf)> (authors Karen Rose, Scott Eldrige, Lyman Chapin)

Internet Society, 'Global Internet Report 2015' (2015) and 2016 (2016 accessed 2 Sept 2016) <  
<https://www.internetsociety.org/globalinternetreport/2016/>> and  
[http://www.internetsociety.org/globalinternetreport/2015/assets/download/IS\\_web.pdf](http://www.internetsociety.org/globalinternetreport/2015/assets/download/IS_web.pdf)>

Internet Society, 'Comment to NTIA' (13 Mar 2017 accessed 15 Mar 2017)  
<[https://www.ntia.doc.gov/files/ntia/publications/internet\\_society\\_20170307.pdf](https://www.ntia.doc.gov/files/ntia/publications/internet_society_20170307.pdf)>

IOT Alliance Australia (IOTAA), 'Internet of Things Security Guideline' v 1.0 (Feb 2017 accessed Feb 2017)  
<<https://static1.squarespace.com/static/573853ed1d07c093e27aefd2/t/58ad2133e4fcb594b8f4fd73/1487741239672/loTAA+Security+Guideline+V1.0.pdf> >

IoTUK and BCS, 'Accelerating the Internet of Things in the UK: Using Policy to Support Practice' *Rand Corporation* (9 May 2016 accessed 10 Jun 2016)  
<<http://www.rand.org/randeurope/research/projects/accelerating-internet-of-things-uk.html>>

Iqbal, Muhammad Usman and Samsung Lim, 'Privacy Implications of Automated GPS Tracking and Profiling' (2010) 29 *Technology and Society Magazine* 39

ISACA, '2015 ISACA IT Risk/ Reward Barometer – Australian Consumer results' *Global Report* (Oct 2015 accessed 29 Apr 2016) < [http://www.isaca.org/SiteCollectionDocuments/2015-risk-reward-survey/2015-isaca-risk-reward-consumer-summary-australia\\_res\\_eng\\_1015.pdf](http://www.isaca.org/SiteCollectionDocuments/2015-risk-reward-survey/2015-isaca-risk-reward-consumer-summary-australia_res_eng_1015.pdf)>

ISACA, 'ISACA Survey: Wide Gap between Australian Consumers and Global IT Professionals on Internet of Things Security' *Press Release* (14 Oct 2015 accessed 3 Jan 2016) <  
<http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/ISACA-Survey-Wide-Gap-between-Australian-Consumers-and-Global-IT-Professionals-on-Internet-of-Things-Security.aspx>>

International Transport Forum, 'Automated and Autonomous Driving: Regulation Under Uncertainty' (2016 accessed 2 Aug 2016)  
<[http://cyberlaw.stanford.edu/files/publication/files/15CPB\\_AutonomousDriving.pdf](http://cyberlaw.stanford.edu/files/publication/files/15CPB_AutonomousDriving.pdf)>

International Telecommunications Union, 'Overview of the Internet of Things' (15 Jun 2012 accessed 3 Mar 2016) <<http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060>>

Ivan, 'Things You Need to Know about Internet of Things' *The Cloud Infographic* (7 Jan 2016)  
<<http://www.thecloudinfographic.com/2016/01/07/things-you-need-to-know-about-internet-of-things.html>>

## J

Jaffe, Mark 'IoT Won't Work Without Artificial intelligence' *WIRED* (n.d. accessed 3 Mar 2016)  
<<http://www.wired.com/insights/2014/11/iot-wont-work-without-artificial-intelligence/>>

Jain, Neha, James O'Reilly & Nicholas Silk, 'Driverless Cars: Insurers Cannot be Asleep at the Wheel' *Bank Underground* (19 Jun 2015 accessed 2 Aug 2016)  
<<https://bankunderground.co.uk/2015/06/19/driverless-cars-insurers-cannot-be-asleep-at-the-wheel/>>

Janakiram, MSV, '5 Companies that will Dominate Consumer IoT Market- Parts 1 and 2' *Forbes* (26 May 2015 accessed 3 Apr 2016) <<http://www.forbes.com/sites/janakirammsv/2015/05/26/5-companies-that-will-dominate-consumer-iot-market-part-2/#6d22440c1930>>

Jaruzelski, Barry, Kevin Schwartz and Volker Staack, 'Innovation's New World Order' *Strategy & Business* (27 Oct 2015 accessed 6 Mar 2-016) < <http://www.strategy-business.com/feature/00370?gko=e606a>>

Jawbone, 'AliphCom UP Privacy Policy' (effective 16 Dec 2014 accessed 2 Feb 2-016) <<https://jawbone.com/up/privacy>>

Jawbone, 'AliphCom UP Terms of Use' (effective 16 Dec 2014 accessed 2 Feb 2-016) <<https://jawbone.com/legal/up/terms>>

Jetstar Airways Pty Limited, 'Undertakings to the Commerce Commission under s46A of the Fair Trading Act 1986 (NZ)' (16 Mar 2016 accessed 5 Dec 2016) <<http://www.comcom.govt.nz/fair-trading/enforcement-response-register/detail/928>>

John, Leslie K., Allesandro Acquisti and George Loewenstein, 'Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information', *Journal of Consumer Research* (2011 accessed 6 Jun 2016) 37(5):858-873

Johnston, Anna, 'Mobiles, metadata and the meaning of 'personal information'', *SalingerPrivacy Blog* (19 Jan 2017 accessed 3 Feb 2017) <<https://www.salingerprivacy.com.au/2017/01/19/federalcourtdecision/>>

Johnston, Anna, 'What's in the bag: data analytics or social surveillance?' *SalingerPrivacy Blog* (20 Jun 2016 accessed 3 Aug 2016) <http://www.salingerprivacy.com.au/2016/06/20/data-analytics/>>

Johnston, Chris, 'Digital is Fuelling the UK Economy' *The Times* (28 January 2016 accessed 1st February 2016) <<http://raconteur.net/business/digital-is-fuelling-the-uk-economy>>

Jones Day, 'Global privacy & data security update' (12 Sept 2016 accessed 12 Sept 2016) <<http://www.jonesday.com/global-privacy-cybersecurity-update-vol-12-11-18-2016/>>

Joyner, Tony, Matthew O'Leary & Alex Drake-Brockman, 'Unfair contract terms checklist' *Herbert Smith Freehills LLP* (18 Mar 2016 accessed 19 Mar 2016) <<http://www.herbertsmithfreehills.com/insights/legal-briefings/unfair-contract-terms-checklist> >

Juniper Research, 'Consumer Cloud – There's No Limit' *White Paper* (2014 accessed 6 July 2014) < [http://www.juniperresearch.com/shop/download\\_whitepaper.php?whitepaper=261](http://www.juniperresearch.com/shop/download_whitepaper.php?whitepaper=261)>

Juniper, 'IOT – Internet of Transformation' (Jul 2015 accessed Oct 2016) < <https://www.juniperresearch.com/document-library/white-papers/iot-internet-of-transformation>>

Juniper, 'Connected Homes Getting Smarter' (Oct 2015 accessed Oct 2016) <<https://www.juniperresearch.com/document-library/white-papers/connected-homes-getting-smarter>>

Juniper, 'On track with Connected and Self-driving Vehicles' (Dec 2015 accessed Oct 2016) <<https://www.juniperresearch.com/document-library/white-papers/on-track-with-connected-and-self-driving-vehicles>>

Juniper, 'Fitness Wearables – Time To Step Up' (Jan 2016 accessed Oct 2016)  
<https://www.juniperresearch.com/document-library/white-papers/fitness-wearables--time-to-step-up>

Juniper, 'Smart Glasses seeing through the Hype' (Feb 2016 accessed Oct 2016)  
<https://www.juniperresearch.com/resources/whitepapers?page=5>

Juniper, 'Connected Couture' (Mar 2016 accessed Oct 2016)  
<<https://www.juniperresearch.com/document-library/white-papers/connected-couture>>

## K

K&L Gates, 'Privacy concerns over Westfield's ticketless parking system' (5 February 2016 accessed 19 May 2016) <<http://www.lexology.com/library/detail.aspx?g=c78228f7-2123-465d-b678-5583cbb8e787>>

Kalia, Amul, 'With Windows 10, Microsoft Blatantly Disregards User Choice and Privacy: A Deep dive' *Electronic Frontier Foundation* (17 Aug 2016 accessed 20 Aug 2016) <  
<https://www.eff.org/deeplinks/2016/08/windows-10-microsoft-blatantly-disregards-user-choice-and-privacy-deep-dive>>

Kam, Richard, 'Time to Get Security Smart About the Internet of Things' *IAPP* (24 Nov 2015 accessed 26 Apr 2016) <https://iapp.org/news/a/time-to-get-security-smart-about-the-internet-of-things/>

Kam, Richard, 'The security of IoT: Is your Fitbit a key for criminals?' *The Privacy Advisor* (22 Jan 2016 accessed 29 Apr 2016) < <https://iapp.org/news/a/the-security-of-iot-is-your-fitbit-a-key-for-criminals/>>

Kam, Richard, 'Connected cars: security and privacy risks on wheels' *IAPP* (22 Feb 2016 accessed 26 Apr 2016) <https://iapp.org/news/a/connected-cars-security-and-privacy-risks-on-wheels/>

Kam, Richard, 'State of Siege: Infrastructure and Industrial Security and Privacy on the IoT' *IAPP* (21 Mar 2016 accessed 26 Apr 2016) <<https://iapp.org/news/a/state-of-siege-infrastructure-and-industrial-security-and-privacy-on-the-iot/>>

Kam, Richard, 'Internet of Things makes big data even bigger (and riskier)' *IAPP* (25 Apr 2016 accessed 27 Apr 2016) <<https://iapp.org/news/a/internet-of-things-makes-big-data-even-bigger-and-riskier/>>

Kang, Cecelia, 'Consumers to Gain Control Over Data That Internet Firms Cull' *The New York Times* (27 Oct 2016 accessed 28 Oct 2016) <[http://www.nytimes.com/2016/10/28/technology/fcc-tightens-privacy-rules-for-broadband-providers.html?\\_r=0](http://www.nytimes.com/2016/10/28/technology/fcc-tightens-privacy-rules-for-broadband-providers.html?_r=0)>

Kelley Blue Book, 'Future Autonomous Driver Study' (Sept 2016 accessed 25 Sept 2016)  
<<http://mediaroom.kbb.com/future-autonomous-vehicle-driver-study>>

Kelley, Patrick Gage, 'Privacy as Iconography' Submission to FTC *privacyCom* 2016 <[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00073-98121.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00073-98121.pdf)>

Kelly, Samantha Murphy, 'Facebook Changes its 'Move Fast and Break Things' Motto (1 May 2014 accessed 26 May 2016) <http://mashable.com/2014/04/30/facebooks-new-mantra-move-fast-with-stability/#PoyW43b6UsqdIn> 2014

Kelly, Will, '7 steps to IoT data security' *InfoWorld* (26 Oct 2015 accessed 5 Feb 2016) <http://www.infoworld.com/article/2997264/internet-of-things/7-steps-to-iot-data-security.html>

Kerr, Orin, 'Second Circuit: Warrants cannot be used to compel disclosure of emails stored outside the United States' *The Washington Post* (14 Jul 2016 Accessed 16 Jul 2016) <<https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/14/second-circuit-warrants-cannot-be-used-to-compel-disclosure-of-emails-stored-outside-the-united-states/>>

Kessler Topaz Meltzer Check LLP., 'Shareholder Class Action Filed Against Fitbit Inc' <<https://www.ktmc.com/new-cases/fitbit-inc>>

Kevin, 'Things You Need to Know about Internet of Things' *The Cloud Infographic* (7 Jan 2016 accessed 23 Feb 2016) < [http://www.thecloudinfographic.com/2016/01/07/things-you-need-to-know-about-internet-of-things.html?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+TheCloudInfographic+%28The+Cloud+Infographic%29&\\_m=3n.007d.204.vl0ao06ikp.42m](http://www.thecloudinfographic.com/2016/01/07/things-you-need-to-know-about-internet-of-things.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheCloudInfographic+%28The+Cloud+Infographic%29&_m=3n.007d.204.vl0ao06ikp.42m)>

Kickstarter, 'LOON Cup – the world's first smart menstrual cup' (Sept 2015 accessed 17 Apr 2016) <https://www.kickstarter.com/projects/700989404/looncup-the-worlds-first-smart-menstrual-cup/description>

Kidman, Angus 'Malcolm Turnbull: The Internet of Things relies on imagination, not regulation' *Lifehacker* (26 Mar 2015 accessed 11 May 2016) <<http://www.lifehacker.com.au/2015/03/malcolm-turnbull-the-internet-of-things-relies-on-imagination-not-regulation/>>

King, N. J., & Forder, J. (2016). Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data. *Computer Law and Security Review* (2016) <doi:10.1016/j.clsr.2016.05.002>

King, Stephen P., 'Sharing Economy: What challenges for Competition Law?' *Journal of European competition Law & Practice*, 2015, 6: 10 <<http://jeclap.oxfordjournals.org.ezproxy.bond.edu.au/content/6/10/729.full.pdf+html>>

King & Wood Mallesons, 'The Australian Cyber Security Centre Threat Report 2015' (30 Jul 2015 accessed 23 Mar 2016) <<http://www.kwm.com/en/au/knowledge/insights/australian-cyber-security-centre-threat-report-2015-data-20150730>>

Kingsley-Hughes, Adrian, 'Nest to deliberately brick old smart hubs' *ZDNet* (4 April 2016 accessed 7 Apr 2016) <http://www.zdnet.com/article/nest-to-deliberately-brick-old-smart-hubs/>

Kirchner, Lauren, 'Your Smart Home Knows a Lot About You' *ProPublica* (9 Oct 2015 Accessed 4 Feb 2016) < <https://www.propublica.org/article/your-smart-home-knows-a-lot-about-you>>

Kirk, Jeremy, 'Pacemaker Hack can delivery deadly 830-volt jolt' *Computerworld* (17 Oct 2012 accessed 18 Apr 2016) *IDG News Service* <<http://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html>>

Koops, Caroline and Bobbi Murphy, 'Australian consumer law in the spotlight: ACL Review Issues Paper released' *King & Wood Mallesons* (1 Apr 2016 accessed 2 Apr 2016) <<http://www.kwm.com/en/au/knowledge/insights/australian-consumer-law-review-issues-paper-submissions-reforms-20160401#>>

Kiss, Jemima, 'Your next car will be hacked. Will autonomous vehicles be worth it?' *The Guardian* (14 Mar 2016 accessed 16 Mar 2016) <<http://www.theguardian.com/technology/2016/mar/13/autonomous-cars-self-driving-hack-mikko-hypponen-sxsw>>

Koebler, Jason, 'Don't Use Allo' *Motherboard* (21 Sept 2016 accessed 2 Nov 2016) <<http://motherboard.vice.com/read/dont-use-google-allo>>

Kollewe, Julia, 'Volvo to seek volunteers for self-driving car trial in UK' *The guardian* (2 Feb 2017 accessed 7 Feb 2017) <<https://www.theguardian.com/business/2017/feb/02/volvo-seeks-volunteers-for-self-driving-car-trial-in-west-london-public-roads>>

Koren, Michael J., 'Tesla has 780 million miles of driving data, and adds another million every 10 hours' *Quartz* (28 May 2016 accessed 20 Nov 2016) <<http://qz.com/694520/tesla-has-780-million-miles-of-driving-data-and-adds-another-million-every-10-hours/>>

Korosec, Kristen, 'Volvo CEO: We will accept all liability when our cars are in autonomous mode' *Fortune* (7 Oct 2015 accessed 2 Feb 2016) <<http://fortune.com/2015/10/07/volvo-liability-self-driving-cars/>>

Korosec, Kristen, 'GM's First Self-Driving Cars Will Still Be Driven by Humans' *Fortune* (15 Mar 2016 accessed 16 Mar 2016) <http://fortune.com/2016/03/15/gm-self-driving-cars-humans/?iid=leftrail>

Kosinski, Michal, David Stillwell and Thore Graepel, 'Private traits and attributes are predictable from digital records of human behaviour' *PNAS University of Cambridge* (2013 accessed 10 Feb 2016) < <http://www.pnas.org/content/110/15/5802.full.pdf>>

Kovacs, Eduard, 'Over 500,000 IoT devices vulnerable to Mirai botnet' *SecurityWeek* (7 Oct 2016 accessed 7 Oct 2016) < <http://www.securityweek.com/over-500000-iot-devices-vulnerable-mirai-botnet>>

KPMG, 'Creepy or cool? Staying on the right side of the consumer privacy line' (Nov 2016 accessed 9 Nov 2016) <<https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2016/advisory/creepy-or-cool.pdf>>

Krauss, Eric B., 'Driverless Cars and the Law – The Tesla Accidents' *Husch Blackwell* (8 Jul 2016 accessed 10 Jul 2016) < <http://www.tmtindustryinsider.com/07-08-2016-driverless-cars-and-the-law-the-tesla-accidents/#page=1>>

Krawiec, RJ, Jessica Nadler et al, 'No appointment necessary: How the IoT and patient-generated data can unlock health care value' *Deloitte University Press* (27 Aug 2015 accessed 25 Apr 2016) <[http://d27n205l7rookf.cloudfront.net/wp-content/uploads/2015/08/DUP-885\\_IoT\\_PatientGeneratedData\\_MASTER\\_082715.pdf](http://d27n205l7rookf.cloudfront.net/wp-content/uploads/2015/08/DUP-885_IoT_PatientGeneratedData_MASTER_082715.pdf)>

Krazit, Tom. 'The Internet of Things Will Make Big Data Look Small' *Forbes* (3 Mar 2-16 accessed 3 Mar 2-16) <http://fortune.com/2016/03/03/internet-data-structure/>

Krebs, 'IoT Reality: Smart Devices, Dumb Defaults' (8 Feb 2016 accessed 3 Mar 2016) <<http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/>>

Krebs, 'DDoS Mitigation Firm Has History of Hijacks' (20 Sept 2016 accessed 23 Oct 2016) <<https://krebsonsecurity.com/2016/09/ddos-mitigation-firm-has-history-of-hijacks/>>

Krebs, 'Who makes the IoT Things under Attack?' (16 Oct 2016 accessed 30 Oct 2016) <https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/>

Krebs, DDoS on Dyn Impacts Twitter, Spotify, Reddit (21 Oct 2016 accessed 23 Oct 2016) <<https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/>>

Krebs, 'Hacked Cameras, DVRs Powered Today's Massive Internet Outage' *KrebsonSecurity* (21 Oct 2016 accessed 23 Oct 2016) < <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>>

Krotowski, Aleks, 'Big Data age puts privacy in question as information becomes currency' *The Guardian* (22 April 2012 accessed 28 Mar 2015) <http://www.theguardian.com/technology/2012/apr/22/big-data-privacy-information-currency>

Kumar, Ajay 'Internet of Things (IOT): Seven enterprise risks to consider' *IoTAgenda* (29 Jun 2016 accessed 2 Jul 2016) < <http://internetofthingsagenda.techtarget.com/tip/Internet-of-Things-IOT-Seven-enterprise-risks-to-consider>>

Kwederis, Joe and Greg Boehmer, 'Caution: Cyber Risks Ahead for Connected Cars', *CIO The Wall Street Journal* (18 Apr 2016 accessed 20 Apr 2016) <<http://deloitte.wsj.com/cio/2016/04/18/caution-cyber-risks-ahead-for-connected-cars/tab/print/>>

## L

La Diega, Guido Noto, & Ian Walden, 'Contracting for the 'Internet of Things': Looking into the Nest', *Queen Mary University of London, School of Law, Legal Studies Research Paper No. 219/2016* (1 Feb 2016 accessed 3 Mar 2016) <SSRN:<http://ssrn.com/abstract=2725913>>

Lambert, Fred, 'Tesla reveals all the details of its 'Autopilot' and its software v7.0 [slide presentation and audio conference]' *electrek* (14 Oct 2015 accessed 2 Aug 2016) <<https://electrek.co/2015/10/14/tesla-reveals-all-the-details-of-its-autopilot-and-its-software-v7-0-slide-presentation-and-audio-conference/>>

Lambert, Fred 'Tesla CEO Elon Musk drops his prediction of full autonomous driving from 3 years to just 2' *electrek* (21 Dec 2015 accessed 2 Aug 2015) <<https://electrek.co/2015/12/21/tesla-ceo-elon-musk-drops-prediction-full-autonomous-driving-from-3-years-to-2/>>

Lambert, Fred, 'BMW CEO doesn't think Tesla has a lead with the Autopilot, compares the system to an unreliable app' *electrek* (2 Dec 2015 accessed 2 Aug 2016) <<https://electrek.co/2015/12/02/bmw-ceo-doesnt-think-tesla-has-a-lead-with-the-autopilot-compares-the-system-to-an-unreliable-app/>>

Lambert, Fred 'Google Deep learning founder says Tesla's Autopilot system is irresponsible' *electrek* (30 May 2016 accessed 2 Aug 2016) <<https://electrek.co/2016/05/30/google-deep-learning-andrew-ng-tesla-autopilot-irresponsible/>>

Lambert, Fred, 'Tesla Autopilot crash in Montana: Drivers reveals new details and claims a 'cover up' by Tesla' *electrek* (10 Jun 2016 accessed 29 Aug 2016) <<https://electrek.com/2016/06/10/>>

Lambert, Fred 'Elon Musk on Tesla fully autonomous car: 'What we've got will blow people's minds, it blows my mind... it'll come sooner than people think' *electrek Blog* (3 Aug 2016 accessed 10 Aug 2016) <https://electrek.co/2016/08/03/elon-musk-tesla-fully-autonomous-car-blows-mind/>

Lambert, Fred, 'Tesla will soon introduce new Autopilot safety restrictions after recent accidents' *electrek* (28 Aug 2016 accessed 2 Sept 2016) <<https://electrek.co/2016/08/28/tesla-autopilot-safety-restrictions-v8-0-accidents/>>

Lambert, Fred, 'Transcript: Elon Musk's press conference about Tesla Autopilot under v8.0 update [Parts 1-7]' (11 Sept 2016 accessed 2 Oct 2016)  
Part 1 <<https://electrek.co/2016/09/11/transcript-elon-musks-press-conference-about-tesla-autopilot-under-v8-0-update-part-1/>>  
Part 2 <<https://electrek.co/2016/09/11/transcript-elon-musks-press-conference-tesla-autopilot-under-v8-0-update-part-2/>>  
Part 3 <<https://electrek.co/2016/09/11/transcript-elon-musks-press-conference-about-tesla-autopilot-under-v8-0-update-part-3/>> Part 4 <<https://electrek.co/2016/09/11/transcript-elon-musks-press-conference-about-tesla-autopilot-under-v8-0-update-part-4/>> Part 5 <<https://electrek.co/2016/09/11/transcript-elon-musks-press-conference-about-tesla-autopilot-under-v8-0-update-part-5/>> Part 6 <<https://electrek.co/2016/09/11/transcript-elon-musks-press-conference-about-tesla-autopilot-under-v8-0-update-part-6/>> Part 7 <<https://electrek.co/2016/09/11/transcript-elon-musks-press-conference-about-tesla-autopilot-under-v8-0-update-part-7/>>

Lambert, Fred, 'Elon Musk defends level 3 autonomy against Google and Volvo, says 'morally wrong to withhold functionalities that may improve safety' *Electrek* (13 Sept 2016 accessed 2 Oct 2016)

<<https://electrek.co/2016/09/13/elon-musk-defends-level-3-autonomy-against-google-volvo-says-morally-wrong-to-withhold-functionalities-that-improve-safety/>>

Lambert, Fred, 'A few Tesla owners filed a class-action lawsuit over the rollout of Tesla Autopilot 2.0 [Updated]' *electrek* (19 Apr 2017 accessed 20 Apr 2017) <<https://electrek.co/2017/04/19/tesla-owners-class-action-lawsuit-tesla-autopilot-2-0/>>

Lamkin, Paul 'Fitbit heart rate tech 'puts consumers at risk' according to lawsuit scientist', *WAREABLES* (May 2016 accessed 2 Aug 2016) < <https://www.wareable.com/fitbit/fitbit-hrm-heart-rate-tech-health-risk-2764>>

Lanxon, Nate, Jeremy Kahn and Joshua Brustein, 'US web host knocked offline in curiously timed attack' *AFRWeekend* (22 Oct 2016 accessed 23 Oct 2016) <<http://www.afr.com/technology/us-web-host-knocked-offline-in-curiously-timed-attack-20161021-gs873w>>

Lapowski, Issie, 'The Insurance Company That Pays People to Stay Fit', *WIRED* (8 Dec 2014 accessed 12 Jul 2016) < <http://www.wired.com/2014/12/oscar-misfit/>>

Laudati, Laraine, 'Summaries of EU Court Decisions Relating to Data Protection 2000- 2015' *Data Protection Office & European Anti-Fraud Office (OLAF)* (28 Jan 2016 accessed 5 Mar 2016) <[https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw\\_2001\\_2015\\_en.pdf](https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf)>

Law Council of Australia, 'Exposure draft – Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (4 Mar 2016 accessed 5 Apr 2016) <<https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Submissions/Law-Council-of-Australia.PDF>>

Law Council of Australia, 'Australian Consumer Law Review' *Submission* (23 Jun 2016 accessed 4 Sept 2016) < [http://consumerlaw.gov.au/files/2016/07/Law\\_Council\\_of\\_Australia.pdf](http://consumerlaw.gov.au/files/2016/07/Law_Council_of_Australia.pdf)>

Law Council of NSW, 'Regulatory barriers to more automated road and Rail Vehicle: NTC Discussion Paper' (24 Mar 2016 accessed 15 May 2016) <[http://www.ntc.gov.au/Media/Reports/\(5874B550-2716-44A2-AA04-585D1F97D59B\).pdf](http://www.ntc.gov.au/Media/Reports/(5874B550-2716-44A2-AA04-585D1F97D59B).pdf)>

Law Society of NSW, 'Submission to NTC' (24 Mar 2016 accessed 30 May 2016) < [http://www.ntc.gov.au/Media/Reports/\(5874B550-2716-44A2-AA04-585D1F97D59B\).pdf](http://www.ntc.gov.au/Media/Reports/(5874B550-2716-44A2-AA04-585D1F97D59B).pdf)>

Law Institute of Victoria, 'Submission to NTC' (16 Mar 2016 accessed 30 May 2016) < [http://www.ntc.gov.au/Media/Reports/\(82EA8807-66F0-46B6-ADD5-53F21B59E444\).pdf](http://www.ntc.gov.au/Media/Reports/(82EA8807-66F0-46B6-ADD5-53F21B59E444).pdf)>

Lawson, P., 'The Connected Car: Who is in the Driver's Seat?' *British Columbia, BC Freedom of Information and Privacy Association* (2015 accessed Aug 2016) <<https://fipa.bc.ca/connected-car-download/>>

Ledger, Dan & Daniel McCaffrey, "Inside Wearables: How the Science of Human Behaviour Change Offers the Secret to Long-Term Engagement." *Endeavour Partners* (Jan 2014 accessed 26 Mar 2016) <<http://endeavourpartners.net/assets/Endeavour-Partners-Wearables-and-the-Science-of-Human-Behavior-Change-Part-1-January-20141.pdf>>

Lee, Dave 'Tony Fadell flies from faltering Nest' (4 Jun 2016 accessed 5 Jun 2016) *BBC* <<http://www.bbc.com/news/technology-36450762>>

Lee, Joel, 'Memory Sizes Explained – Gigabytes, Terabytes & Petabytes in Layman's Terms' (14 Aug 2012 accessed 18 Mar 2016) < <http://www.makeuseof.com/tag/memory-sizes-gigabytes-terabytes-petabytes/>>

Lee, Joel 'What is the Internet Of Things & How Will It Affect Our Future [MakeUseOf Explains]' (28 Jun 2013 accessed 18 Mar 2016) < <http://www.makeuseof.com/tag/what-is-the-internet-of-things-and-how-will-it-affect-our-future-makeuseof-explains/>>

Lee, Joel, 'Smart TVs are a growing security risk: how do you deal with this?' *MUD* (24 May 2014 accessed 2 Sept 2016) < <http://www.makeuseof.com/tag/smart-tvs-are-a-growing-security-risk-how-do-you-deal-with-this/>>

Lee, Joel, '5 reasons why you shouldn't buy a smart TV in 2016' *MUD* (28 Jan 2016 accessed 2 Sept 2016) < <http://www.makeuseof.com/tag/5-reasons-shouldnt-buy-smart-tv-anymore/>>

Lee, Stephanie, 'Why Activity Trackers could be Running out of Steps' *BuzzFeed News* (28 Feb 2015 accessed 23 Mar 2016) < <http://www.buzzfeed.com/stephaniemlee/why-activity-trackers-could-be-running-out-of-steps#.cgReqWyJd>>

Lee, Peter, 'Learning from Tay's introduction' *Microsoft Blog* (25 Mar 2016 accessed 15 Aug 2016) <https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/>>

Lee, Yuna, 'Amazon challenges search warrant in Benton County murder case' (22 Feb 2017 accessed 24 Feb 2-17) < <http://www.4029tv.com/article/amazon-responds-to-local-search-warrant-in-murder-case/8964554>>

Legg, Michael & Claire Golding, 'How the Internet of Things will affect the future of litigation' *Law Society Journal* (November 2016 accessed 2 Dec 2016) < <http://www.law.unsw.edu.au/news/2016/11/how-internet-things-will-affect-future-litigation>>

Legislative and Governance Forum on Consumer Affairs, 'ACL Review: Terms of Reference' (12 Jun 2015 accessed 29 June 2015) <<http://consumerlaw.gov.au/review-of-the-australian-consumer-law/terms-of-reference/>>

Legislative and Governance Forum on Consumer Affairs, 'Strategic Agenda 2015- 2017' (12 Nov 2015 accessed 2 Jan 2016) <[http://consumerlaw.gov.au/files/2015/09/CAF\\_strategic\\_agenda\\_2015.pdf](http://consumerlaw.gov.au/files/2015/09/CAF_strategic_agenda_2015.pdf)>

Legislative and Governance Forum on Consumer Affairs, 'Charter' (12 Nov 2015 accessed 2 Jan 2016) <[http://consumerlaw.gov.au/files/2016/04/CAF\\_Charter\\_2015-17.pdf](http://consumerlaw.gov.au/files/2016/04/CAF_Charter_2015-17.pdf)>

Leibowicz, Jon, 'Remarks' (1 Feb 2013 accessed 17 Mar 2016) <<https://www.ftc.gov/public-statements/2013/02/remarks-federal-trade-commission-chairman-jon-leibowitz-prepared-delivery>>

Leonard, Peter 'Customer data analytics: privacy settings for 'Big data' *Business International Data Privacy Law* 4 (1) (2014 accessed 10 Apr 2015) 53 – 68 <http://idpl.oxfordjournals.org/>

Leonard, Peter 'Australian privacy law: swimming in the porridge of offshore disclosure', *G+T* (6 Nov 2014 accessed 28 May 2015) < <http://www.lexology.com/library/detail.aspx?g=61f5ad3e-95cf-4576-a128-c112278b2790>>

Leonard, Peter, 'Ben Grubb v Telstra Corporation' (2015) 15(3) *E-Commerce Law Reports* <<https://www.gtlaw.com.au/?q=ben-grubb-v-telstra-corporation>>

Leonard, Peter, 'Fishing by Subpoena in the Rising Communications 'Metadata': a debate yet to start' *Gilbert & Tobin* (Sept 2015 accessed 7 Apr 2016) < <http://www.lexology.com/library/document.aspx?g=eb05ca80-ac3a-44b6-93ed-9db5a1bf9ef7>>

Leonard, Peter, 'A Mandatory Data Breach Notification Scheme for Australia?' *G&T Law* (31 Mar 2016 accessed 7 Apr 2016) <http://www.gtlaw.com.au/sites/default/files/Peter%20Leonard%20%20A%20Serious%20Data%20Breach%20Notification%20Scheme%20for%20Australia.PDF>

Leonard, Peter, 'The Internet of Things (aka The Internet of Everything): What Is It About and Who Should Care' (4 Aug 2016 accessed 8 Aug 2016) < <https://www.gtlaw.com.au/?q=internet-things-aka-internet-everything-what-it-about-and-who-should-care>>

Leonard, Peter G., 'Mandatory Data Breach arrives in Australia: A Review of the Australian Privacy Amendment (Notifiable Data Breaches Act)', *G+T* (17 Feb 2017 accessed 20 Feb 2017) <<https://www.gtlaw.com.au/insights/mandatory-data-breach-notification-arrives-australia>>

Leonard, Peter G., 'A review of *Australian Privacy Commissioner v Telstra Corporation Limited*', *G+T* (16 Feb 2017 accessed 20 Feb 2017) <https://www.gtlaw.com.au/insights/review-australian-privacy-commissioner-v-telstra-corporation-limited>

Lever, Rob, 'Secrets from smart devices find path to US legal system' *PhysORG* (19 Mar 2017 accessed 15 April 2017) <<https://phys.org/news/2017-03-secrets-smart-devices-path-legal.html>>

Levin, Doron 'Here are some of the worst car scandals in history' *Fortune* (26 Sept 2015 accessed 2 Jan 2016) < <http://fortune.com/2015/09/26/auto-industry-scandals/>>

Levin, Sam and Nicky Woolf, 'Tesla driver killed while using autopilot was watching Harry Potter, witness says' *The Guardian* (2 Jul 2016 accessed 2 Jul 2016) <<https://www.theguardian.com/technology/2016/jul/01/tesla-driver-killed-autopilot-self-driving-car-harry-potter>>

Levin, Sam, Julia Carrie Wong and Nicky Woolf, 'Elon Musk's self-driving evangelism masks risk of Tesla autopilot, experts say' *The Guardian* (2 Jul 2016 accessed 2 Jul 2016) < <https://www.theguardian.com/technology/2016/jul/02/elon-musk-self-driving-tesla-autopilot-joshua-brown-risks>>

Libicki, Martin C., 'How I Learned to Stop Worrying and Love the Internet of Things' *The RAND Blog* (4 Aug 2015 accessed 2 Jan 2016) <<http://www.rand.org/blog/2015/08/how-i-learned-to-stop-worrying-and-love-the-internet.html#>>

Lim, Cheng & Patrick Gunning, 'The Australian Cyber Security Centre Threat Report 2015' *King & Wood Mallesons* (30 Jul 2015 accessed 8 Mar 2016)  
<http://www.lexology.com/library/detail.aspx?g=b0c4608b-6a27-406d-9641-5976354dbe75>

Lindsay, Greg, Beau Woods and Joshua Corman, 'Smart Homes and the Internet of things' *Atlantic Council Brent Scowcroft Center on International Security* (Mar 2016 accessed 12 Aug 2016)  
[https://otalliance.org/system/files/files/initiative/.../smart\\_homes\\_0317\\_web.pdf](https://otalliance.org/system/files/files/initiative/.../smart_homes_0317_web.pdf)

Link Labs, '16 Ridiculous Internet of Things Statistics as we head into 2016' (2 Dec 2015 accessed 11 Apr 2016) <<http://www.link-labs.com/internet-of-things-statistics-2016/>>

Linthicum, David, 'The cloud and the Internet of things are inseparable' *InfoWorld* (12 Jan 2016 accessed 5 Feb 2016) <http://searchcloudapplications.techtarget.com/feature/How-IoT-and-consumer-IoT-handle-data-differently>

Linthicum, David, 'IoT standards must start in the cloud' *InfoWorld* (29 Sept 2015 accessed 5 Feb 2016) <http://www.infoworld.com/article/2986307/cloud-computing/iot-standards-must-start-in-the-cloud.html>

Lissowska, Maria, 'Overview of Behavioural Economics Elements in the OECD Consumer Policy Toolkit' 34 *J Consum Policy* (2011): 393- 398.

Listokin, Siona, 'Industry Self-Regulation of Consumer Data Privacy and Security' *Submitted to FTC PrivacyCon 2016* < [https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00031-97822.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00031-97822.pdf)>

Lithium, 'The State of Social Media Engagement 2016' (Mar 2016 accessed 2 Apr 2016)  
<<http://www.lithium.com/pages/state-of-social-engagement>>

Lloyd's, 'Autonomous Vehicles: Handing Over Control: Risks and opportunities in insurance' (Mar 2014 accessed 2 Mar 2016) < <https://www.lloyds.com/news-and-insight/risk-insight/library/technology/autonomous-vehicles>>

Loeb, Matt, 'Internet of Things Security Issues Require a Rethink on Risk Management' *The Wall Street Journal* (14 October 2015 accessed 29 Apr 2016) <<http://blogs.wsj.com/cio/2015/10/14/internet-of-things-security-issues-require-a-rethink-on-risk-management/tab/print/>>

Lohr, Steve, 'Redrawing the route to online privacy' *Taipei Times, NY Times News Service* (3 Mar 03, 2010 accessed 10 Jan 2016)  
<<http://www.taipetimes.com/News/editorials/archives/2010/03/03/2003467037>>

Loos, Marco and Joasia Luzak, 'Wanted: a Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers' *Journal of Consumer Policy* (March 2016) 39:1: 63–90  
<http://link.springer.com/article/10.1007/s10603-015-9303-7#Sec7>

Lopez Research, 'An Introduction to the Internet of things' *Part 1 of the IoT Series* (Nov 2013 accessed 4 Apr 2016) <[http://www.cisco.com/c/dam/en\\_us/solutions/trends/iot/introduction\\_to\\_loT\\_november.pdf](http://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_loT_november.pdf)>

Love, Julie, 'Apple 'privacy czars' grapple with internal conflicts over user data' *Reuters Technology* (21 Mar 2016 accessed 24 Mar 2016) <http://www.reuters.com/article/us-apple-encryption-privacy-insight-idUSKCN0WN0BO>

Luger, Ewa, Lachlan Urquhart, Tom Rodden & Michael Golembewski, 'Playing the Legal Card: Using Ideation Cards to raise Data Protection Issues within the Design Process' (2015 accessed 6 Apr 2016) <[https://www.ftc.gov/system/files/documents/public\\_comments/2015/09/00004-97144.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/09/00004-97144.pdf)>

Lunn, Pete, 'Regulatory Policy and Behavioural Economics' *OECD* (2014 accessed 16 Feb 2016) <<http://dx.doi.org/10.1787/9789264207851-en>>

Lutz, Lennart S. 'Automated Vehicles in the EU: A Look at Regulations and Amendments' *GenRe Publications* (Mar 2016 accessed 5 Apr 2016) <http://www.genre.com/knowledge/publications/cmint16-1-en.html>

Lux Research, 'Key Takeaway - The Internet of Everyone: Consumer Relationships in the Age of IoT' (2015 accessed 6 Mar 2016) [http://www.luxresearchinc.com/sites/default/files/FCP\\_KTA\\_12\\_15.pdf](http://www.luxresearchinc.com/sites/default/files/FCP_KTA_12_15.pdf)>

Lux Research, 'The Internet of Everyone: Consumer Relationships in the Age of IoT' *LRFP-R-15-5* (December 2015 accessed 3 Feb 2016) <[www.luxresearchinc.com](http://www.luxresearchinc.com)>

Lyngaas, Sean, 'NIST official: Internet of things is indefensible' *FCW* (16 Apr 2015 accessed 7 Apr 2016) <<https://fcw.com/articles/2015/04/16/iot-is-indefensible.aspx>>

Lyons, Tim, 'Addressing privacy concerns: a question solely for regulators?' *DLA Piper* (4 Aug 2015 accessed 7 Apr 2016) <<http://www.lexology.com/library/detail.aspx?g=04e68b1d-587c-4800-993d-4502e30aaeb6>>

Lyons, Tim, Peter Jones and Sharon Rowe, 'The top six things you need to know about the Internet of Things: a legal perspective' *DLA Piper* (11 Aug 2015 accessed 7 Apr 2016) <<http://www.lexology.com/library/detail.aspx?g=ed67e0af-b2bc-4c12-ac5a-c4849f1f4d08>>

Lyons, Tim, 'Building privacy into the internet of things' *DLA Piper* (3 Nov 2015 accessed 7 Apr 2016) <<http://www.lexology.com/library/detail.aspx?g=d27a64f5-24b3-43b9-8410-ec3bc7c1a1f6>>

## M

McAuley, Derek, 'What is IOT? That is not the question' *Blog* (1 Feb 2016 accessed 5 Mar 2016) <<http://iotuk.org.uk/what-is-iot-that-is-not-the-question/>>

McCarthy, Niall 'Connected Cars by the Numbers' *Statista Report* (28 Jan 2015 accessed 20 Jun 2016) <https://www.statista.com/chart/3168/connected-cars-by-the-numbers/>

McColl, Ruth, "Privacy, Business and the Digital Era" [2014] *NSWJSchol* 15  
 <<http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/NSWJSchol/2014/15.html?stem=0&synonyms=0&query=APP1.3>>

McConnell, Emily & Robert Prosser, 'Unfair contract terms protections extended to small business' *Freehills Herbert Smith* (2015 accessed 26 Nov 2015)  
 <<http://www.herbertsmithfreehills.com/insights/legal-briefings/unfair-contract-terms-protections-extended-to-small-business>>

McCowen, David 'Tech wrap: Car companies bet on ridesharing' *The Sydney Morning Herald, Drive* (26 May 2016 accessed 24 Jun 2016) <<http://www.drive.com.au/motor-news/tech-wrap-car-companies-bet-on-ridesharing-20160526-gp46dn.html>>

McCullagh, Adrian, 'The Validity and Limitations of Electronic Agents in Contract Formation' (n.d. accessed 25 Apr 2016) <[http://www.law.uq.edu.au/documents/mod-legal-framework-conf-2013/A-McCullagh\\_The-Validity-and-Limitations-of-Software-Agents-in-Contract-Formation.pdf](http://www.law.uq.edu.au/documents/mod-legal-framework-conf-2013/A-McCullagh_The-Validity-and-Limitations-of-Software-Agents-in-Contract-Formation.pdf)>

McDermott, Will and Emery, 'UK data anonymisation code' (13 Mar 2013 accessed 2 Jan 2016) <<http://www.lexology.com/library/detail.aspx?g=1933b480-70ad-460b-bfc0-90ae435dc8d8>>

McDonald, A. M. and L. F. Cranor, 'The Cost of Reading Privacy Policies', *I/S: A Journal of Law and Policy for the Information Society* (2008) <<http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>>

McDonald, Simon, 'Internet of Things – security' *K&L Gates* (9 Nov 2015 accessed 7 Apr 2016) <<http://www.lexology.com/library/detail.aspx?g=7c35b5cc-cc74-42fb-b7a5-bf09b4e4accf>>

McGoogan, Cara, 'BMW, Audi and Toyota cars can be unlocked and started with hacked radios' *The Telegraph* (25 Apr 2016 accessed 25 Apr 2016)  
 <<http://www.telegraph.co.uk/technology/2016/03/23/hackers-can-unlock-and-start-dozens-of-high-end-cars-through-the/>>

McGrath, Sean 'OFCOM releases vague IoT report' *MicroScope* (28 Jan 2015 accessed 19 Nov 2015)  
 <<http://www.microscope.co.uk/news/2240239003/Ofcom-releases-vague-iot-report>>

McMillan, 'Cybersecurity and the Internet of Things' (1 Mar 2016 accessed 4 Apr 2016) <<http://www.lexology.com/library/detail.aspx?g=43be5ccf-4d89-46e3-b6e6-d28198d4df84>>

McNamara, Rosalind, 'Insurance tracker apps: good for the consumer?' *CHOICE* (6 Oct 2016 accessed 8 Oct 2016) <<https://www.choice.com.au/electronics-and-technology/phones/mobile-phones/articles/insurance-tracker-apps>>

McSweeney, Terrell, 'Consumer Protection in the Age of Connected Everything' *Keynote remarks, New York Law School, New York* (3 February 2017 accessed 5 Feb 2017) <<https://www.ftc.gov/public-statements/2017/02/consumer-protection-age-connected-everything>>

McSweeney, Terrell, 'Connected Cars USA 2016', *Keynote remarks* (6 Feb 2016 accessed 12 Feb 2016)  
 <[https://www.ftc.gov/system/files/documents/public\\_statements/913813/mcsweeney\\_-\\_connected\\_cars\\_usa\\_2016\\_2-4-16.pdf](https://www.ftc.gov/system/files/documents/public_statements/913813/mcsweeney_-_connected_cars_usa_2016_2-4-16.pdf)>

McWhirter, Lisa and Lisa Eckstein, 'Australian Consent Study' (2015 accessed 20 Mar 2016) <<http://www.utas.edu.au/law-and-genetics/research-and-projects/australian-consent-project>>

Madden, Mary and Lee Rainie, 'Americans' Attitudes About Privacy, Security and Surveillance' *Pew Research* (20 May 2015 accessed 6 Jun 2016) <<http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>>

Maddox, Teena, 'Wozniak talks: Self-driving cars, Apple Watch, and how AI will benefit humanity' *TechRepublic* (24 June 2015 accessed 25 May 2016) < <http://www.techrepublic.com/article/wozniak-talks-self-driving-cars-apple-watch-and-how-ai-will-benefit-humanity/>>

Magill, Jared, 'The Crooked Path to Determining Liability in Data Breach Cases' *WIRED* (date unclear!!!) < <http://www.wired.com/insights/2015/03/crooked-path-determining-liability-data-breach-cases/>>

Maingate, 'The Key to Unlocking 50 Billion Connected Devices' *White Paper* (Oct 2014 accessed 23 Mar 2016) < <http://iotbusinessnews.com/download/white-papers/WIRELESS-MAINGATE-The-key-to-unlocking-50-billion-connected-devices.pdf>>

Mak, Vanessa, 'Policy Choices in European Consumer Law: Regulation through 'Targeted Differentiation' *European Review of Contract Law*, (Jun 2011) 257-274.

Malbon, Justin, Taking Fake Online Consumer Reviews Seriously (March 24, 2013). 36(2) *Journal of Consumer Policy* 139-157 <<http://ssrn.com/abstract=2238889>>

Malbon, Justin and Luke Nottage (eds), *Consumer Law & Policy in Australia & New Zealand*, The Federation Press, 2013.

Mankey, Derek, 'Fortinet 2017 Cybersecurity Predictions: Accountability Takes the Stage' *Fortinet* (21 Nov 2016 accessed 5 Feb 2017) <<https://blog.fortinet.com/2016/11/15/fortinet-2017-cybersecurity-predictions-accountability-takes-the-stage>>

Mannatt Phelps and Phillips LLP, 'Fitbit can't sleep on false advertising suit over sleep measurement claims' *Lexology* (29 May 2015 accessed 2 Oct 2016) <<http://www.lexology.com/library/detail.aspx?g=0193042e-7c61-45bc-85c7-54decbb42579> >

Mannatt Phelps and Phillips LLP, 'Be Still, My Heart: New Suit Says Fitbits Fail to Track Heartbeats as Promised' (29 Jan 2016 accessed 2 Sept 2016) <<http://www.lexology.com/library/detail.aspx?g=5e17c086-b548-401d-90da-7899673ba9e5>>

Manta, Irina D & David S. Olson, 'Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly.' 67 *Alabama Law Review* 135 (2015) <[https://law.depaul.edu/about/centers-and-institutes/center-for-intellectual-property-law-and-information-technology/programs/ip-scholars-conference/Documents/ipsc\\_2015/abstracts-papers-presentation/OlsonD\\_abstract.pdf](https://law.depaul.edu/about/centers-and-institutes/center-for-intellectual-property-law-and-information-technology/programs/ip-scholars-conference/Documents/ipsc_2015/abstracts-papers-presentation/OlsonD_abstract.pdf)>

Marin, Eduard, Dave Singelée, Flavio D. Garcia, Tom Chothia, Rik Willems & Bart Preneel, 'On the (in)security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them' (2016 accessed 2 Dec 2016) < <https://www.esat.kuleuven.be/cosic/publications/article-2678.pdf>>

Markoff, John 'Researchers Show How a Car's Electronics Can Be Taken Over Remotely' *The New York Times* (9 Mar 2011 accessed 16 Mar 2016)  
<<http://www.nytimes.com/2011/03/10/business/10hack.html>>  
And <<http://www.autosec.org/pubs/cars-oakland2010.pdf> and <http://www.autosec.org/pubs/cars-usenixsec2011.pdf>>

Marr, Bernard 'The 5V's of Data' (9 Apr 2015 accessed 10 Dec 2015) Data Science Central  
<<http://www.datasciencecentral.com/profiles/blogs/the-5-v-s-of-big-data-by-bernard-marr>>

Mason Hayes and Curran, 'Appy Campers - Mobile Apps and Data Privacy' (6 Mar 2014 accessed 2 Jan 2016) < <http://www.mhc.ie/latest/blog/appy-campers-mobile-apps-and-data-privacy>>

Mason Hayes and Curran, 'The Internet of Things, Part 2: Top 7 Recommendations from EU privacy regulators' (14 Nov 2014 accessed 2 Jan 2016) <<http://www.mhc.ie/latest/blog/the-internet-of-things-part-2-top-7-recommendations-from-eu-privacy-regulators>>

Mason Hayes and Curran, 'Reforming Data Protection Law – Introducing the General Data Protection Regulation' *Tech Law Blog* (24 Mar 2016 accessed 8 Apr 2016) <<http://www.mhc.ie/latest/blog/reforming-data-protection-law-introducing-the-general-data-protection-regulation>>

Mason Hayes and Curran, 'Rethinking Cloud Computing Contracts in the Age of Disruption' *Tech Law Blog* (26 Feb 2016 accessed 8 Apr 2016) < <http://www.mhc.ie/latest/blog/rethinking-cloud-computing-contracts-in-the-age-of-disruption>>

Mason Hayes and Curran, 'Privacy Shield Revealed: A Look at the Proposed Replacement of Safe Harbour' (2 Mar 2016 accessed 8 Apr 2016) < <http://www.mhc.ie/latest/blog/privacy-shield-revealed-a-look-at-the-proposed-replacement-of-safe-harbor>>

Mason Hayes and Curran, 'Are retailers responsible for User Activity on their Free Wi-Fi?' *Tech law blog* (1 Apr 2016 accessed 8 Apr 2016) < <http://www.mhc.ie/latest/blog/are-retailers-responsible-for-user-activity-on-their-free-wi-fi>>

Mason Hayes and Curran, 'E-sign on the Dotted Line – The EU's New Rules on Electronic Identification' *Tech Law Blog* (13 May 2016 accessed 19 May 2016) < <http://www.mhc.ie/latest/blog/e-sign-on-the-dotted-line-the-eus-new-rules-on-electronic-identification>>

Mason Hayes and Curran, 'General Data Protection Regulation: 6 Things You Need to Know' *Tech Law Blog* (16 May 2016 accessed 19 May 2016) <<http://www.mhc.ie/latest/insights/general-data-protection-regulation-6-things-you-need-to-know>>

Mason Hayes and Curran, 'Untangling the Web of Liability in the Internet of Things' *Tech Law Blog* (19 May 2016 accessed 20 May 2016) < <http://www.mhc.ie/latest/blog/untangling-the-web-of-liability-in-the-internet-of-things>>

Mason Hayes and Curran, 'Spam, Cookies and Consent: 7 Talking Points from Proposals to Reform the ePrivacy Directive' (12 Aug 2016 accessed 2 Sept 2016) <http://www.mhc.ie/latest/blog/spam-cookies-and-consent-7-talking-points-from-proposals-to-reform-the-eprivacy-directive>

Mason Hayes and Curran, 'Are Dynamic IP Addresses Personal Data?' (29 September 2016 accessed 20 Oct 2016) <<http://www.mhc.ie/latest/blog/are-dynamic-ip-addresses-personal-data>>

Mason Hayes and Curran, 'DPC Publishes Guidance on Anonymisation and Pseudonymisation' *Tech Law Blog* (7 October 2016 accessed 20 Oct 2016) <<http://www.mhc.ie/latest/blog/dpc-publishes-guidance-on-anonymisation-and-pseudonymisation>>

Mason Hayes and Curran, 'DPC Guidance on Anonymisation – Techniques and Data Protection Obligations' *Tech Law Blog* (14 Oct 2016 accessed 20 Oct 2016) <<http://www.mhc.ie/latest/blog/dpc-guidance-on-anonymisation-techniques-and-data-protection-obligations>>

Mason Hayes and Curran 'Location, Location, Location – New DPC Guidance' (4 November 2016 accessed 5 Nov 2016) < <https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf>>

Mason Curran and Hayes, 'Getting ready for the GDPR' A Guide' (Apr 2017 accessed Apr 2017) <https://www.mhc.ie/uploads/pdf/getting-ready-for-the-general-data-protection-regulation.pdf>

Manwaring Kayleen, 'Data breach notifications: an Australian perspective', *Privacy & Data Security Law Journal*, (2009) 4: 848 - 864,  
<[http://international.westlaw.com/result/default.wl?mt=WLIGeneralSubscription&origin=Search&srch=TRUE&utid=3&db=PRIVDSLJ&rt=CLID\\_QRYRLT4725443022148&method=TNC&service=Search&eq=search&rp=%2fsearch%2f](http://international.westlaw.com/result/default.wl?mt=WLIGeneralSubscription&origin=Search&srch=TRUE&utid=3&db=PRIVDSLJ&rt=CLID_QRYRLT4725443022148&method=TNC&service=Search&eq=search&rp=%2fsearch%2f)>

Manwaring K, 2011, 'Enforceability of Clickwrap and Browsewrap Terms in Australia: Lessons from the US and the UK', *Studies in Ethics, Law, and Technology* Vol 5, <http://dx.doi.org/10.2202/1941-6008.1102>

Manwaring, Kayleen and Roger Clarke, 'Surfing the third wave of computing: A framework for research into eObjects' *Computer Law and Security Review* (2015) 586- 603 < <https://www.ntia.doc.gov/files/ntia/publications/kayleen-manwaring.pdf>>

Manwaring, Kayleen, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (1 September 2016) *Deakin Law Review* <<https://ssrn.com/abstract=2833663>>

Manwaring K.E., 2016, 'Surfing the third wave of computing: contracting with eObjects', in *Proceedings Doctoral Consortium (DCIT 2016)*, SCITEPress, Rome, Italy (22 - 25 April 2016)

Manwaring Kayleen 'A Legal Analysis of Socio-Technological Change Arising Out of eObjects' *Working Paper* (2016 accessed Jun 2016) <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2690024](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2690024)>

Marchant, Gary E., and Rachel A Lindor, 'The Coming Collision between Autonomous Vehicles and the Liability System' (2012) 52 *Santa Clara Law Review* 1321

Mathews-Hunt, Kate, 'Gaming the system: Fake online reviews v. consumer law' *Computer Law & Security Review*, 31 (1) (2015): 3-25

Mathews-Hunt, Kate. 'CloudConsumer: contracts, codes and the law' *Computer Law & Security Review* 31 (2015) 450- 477 <http://dx.doi.org/10.1016/j.clsr.2015.05.006>

Mathews-Hunt, Kate, 'CookieConsumer: Tracking online behavioural advertising in Australia' *Computer Law & Security Review* 32(2016): 55- 90

Manne, Geoffrey A. and Ben Sperry, 'FTC Process and the Misguided Notion of an FTC "Common Law" of Data Security' <[http://masonlec.org/site/rte\\_uploads/files/manne%20%26%20sperry%20-%20ftc%20common%20law%20conference%20paper.pdf](http://masonlec.org/site/rte_uploads/files/manne%20%26%20sperry%20-%20ftc%20common%20law%20conference%20paper.pdf)>

Marcus, Amy Dockser, 'How New Technology Is Illuminating a Classic Ethical Dilemma' *The Wall Street Journal* (8 Jun 2016 Accessed 9 June 2016) < <http://www.wsj.com/articles/how-new-technology-is-illuminating-a-classic-ethical-dilemma-1465395082>>

MarketWatch, 'Proofpoint Uncovers Internet of Things (IoT) Cyberattack' *Press Release* (16 Jan 2014 accessed 2 Feb 2016) < <http://www.marketwatch.com/story/proofpoint-uncovers-internet-of-things-iot-cyberattack-2014-01-16>>

Markey, Senator Edward J., "Tracking and Hacking: Security and Privacy Gaps Put American Drivers at Risk" (Feb 2015 accessed 16 Mar 2016) < [http://www.markey.senate.gov/imo/media/doc/2015-02-06\\_MarkeyReport-Tracking\\_Hacking\\_CarSecurity%202.pdf](http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf)>

Marr, Bernard, '17 Internet of Things Facts Everyone Should Read' *Forbes* (27 Oct 2015 accessed 10 Mar 2016) <http://www.forbes.com/sites/bernardmarr/2015/10/27/17-mind-blowing-internet-of-things-facts-everyone-should-read/#6381e8161a7a>

Marshall, Aarian, 'Lazy automakers can just buy self-driving cars from Delphi' *WIRED* (24 Aug 2016 accessed 25 Aug 2016) < <https://www.wired.com/2016/08/lazy-automakers-can-just-buy-self-driving-cars-delphi/?CNDID=>>

Matussek, Karin ' VW Sued for Record \$9.2 Billion in German Investor Lawsuits' *Bloomberg Markets* (22 Sept 2016 accessed 23 Sept 2016) <http://www.bloomberg.com/news/articles/2016-09-21/vw-investors-sue-for-8-2-billion-euros-in-germany-over-diesel>

May, Gareth, 'The future of sex tech: Pleasure chips, VR teledildonics & haptic deviants' *WAREABLES* (30 Nov 2016 accessed 16 Jan 2017) < <https://www.wearable.com/wearable-tech/future-sex-tech-888>>

Mayer, Jonathan, Patrick Mutchler and John C. Mitchell, 'Evaluating the privacy properties of telephone metadata' *PNAS* (1 Mar 2016 accessed 6 Jun 2016) <<http://www.pnas.org/content/113/20/5536.full>>

Maynard, Andrew, 'What is the precautionary principle and is it Good or Bad' *University of Maryland* <<https://www.youtube.com/watch?v=3RC7EGDtOYM>>

Medcraft, Greg, 'World Economic Forum and cyber security' *ASIC Media Release* (20 Jan 2017 accessed 2 Feb 2017) <https://www.asic.gov.au/about-asic/media-centre/asic-responds/world-economic-forum-and-cyber-security/>

MEF, 'Global Consumer Survey: The Impact of Trust on IOT' (2016 accessed 10 Nov 2016) <[http://www.mobileecosystemforum.com/wp-content/uploads/2016/04/IoT\\_Exec\\_Summary.pdf](http://www.mobileecosystemforum.com/wp-content/uploads/2016/04/IoT_Exec_Summary.pdf)>

Mehrotra, Kartikay, Margaret Cronin Fisk and Dana Hull, 'Concerns grow about Tesla's Autopilot feature' *Brisbane Times*, (17 Jul 2016 accessed 17 Jul 2016) <

<http://www.brisbanetimes.com.au/business/energy/concerns-grow-about-teslas-autopilot-feature-20160717-gq7hut.html>>

Melby, B. & A. Benjamin Klaber, 'Contract Corner: Standard Terms in the IoT Age' *Morgan Lewis & Brockius LLP* (13 Apr 2017 accessed 14 Apr 2017)  
<<http://www.lexology.com/library/detail.aspx?g=69f405ae-ead6-442c-a961-bb266bac135b>>

Meola, Andrew, 'Consumers don't care if their connected car can get hacked – where's why that's a problem' *Bi Intelligence, Business Insider* (7 Mar 2016 accessed 2 May 2016)  
<<http://www.businessinsider.com/smart-car-hacking-major-problem-for-iot-internet-of-things-2016-3/?r=AU&IR=T>>

Mercer, Christina, 'What is the Internet of Things? Everything you need to know about IoT' *Techworld* (7 Dec 2015 accessed 10 Mar 2016) < <http://www.techworld.com/big-data/what-is-internet-of-things-3631109/>>

Mercer, Christina, 'Driverless cars: 11 questions the insurance industry must answer' (12 May 2016 accessed 16 May 2016) < <http://www.techworld.com/picture-gallery/personal-tech/driverless-cars-questions-insurance-industry-must-answer-3640145/#12>

Metz, Cade, 'Artificial intelligence is setting up the internet of things for a huge clash with Europe' *WIRED* (11 Jul 2016 accessed 12 Jul 2016) <<http://www.wired.com/2016/07/artificial-intelligence-setting-internet-huge-clash-europe/>>

Metz, Cade, 'Self-driving cars will teach themselves to save lives – but also take them' *WIRED* (9 Jun 2016 accessed 10 Jun 2016) <<http://www.wired.com/2016/06/self-driving-cars-will-power-kill-wont-conscience/>>

Meyer, David, 'If You Ever Had a Myspace Account, Thus Hack May Affect You' *Fortune* (30 May 2016 accessed 2 Jun 2016) < <http://fortune.com/2016/05/30/myspace-data-hack/>>

Micklitz, Hans-W, Lucia A. Reisch and Kornelia Hagen, 'An Introduction to the Special Issue on 'Behavioural Economics, Consumer Policy and Consumer Law' *Journal of Consumer Policy* (Sept 2011) 34(3): 271- 276

Microsoft, 'Response to Request for Comment' (2016 accessed 15 Jan 2017)  
<[https://www.ntia.doc.gov/files/ntia/publications/microsoft\\_corporations\\_response\\_to\\_the\\_green\\_paper\\_-\\_march\\_2017.pdf](https://www.ntia.doc.gov/files/ntia/publications/microsoft_corporations_response_to_the_green_paper_-_march_2017.pdf)>

Millar, Sheila A., 'The Internet of Things: A World of Compliance Challenges' *Keller & Heckmen LLP* (21 Jan 2016 accessed 20 Mar 2016) <<https://www.khlaw.com/8709>>

Miller, Charlie & Chris Valasek, 'Adventures in Automotive Networks and Control Units' (2014 accessed 16 Mar 2016) < [http://illmatics.com/car\\_hacking.pdf](http://illmatics.com/car_hacking.pdf)>

Miller, Cheryl, 'Federal, State Officials Face Sharp Curves in Regulating Driverless Cars' *National Law Journal* (1 May 2017 accessed 1 May 2017) <  
<http://www.nationallawjournal.com/printerfriendly/id=1202784803423>>

Miller, R. V., *Miller's Australian Competition and Consumer Law Annotated* (38<sup>th</sup> edition) Lawbook Co. 2016

Millman, Rene, 'TalkTalk loses 250,000 customers post-breach – now supplier scam too' *SC Magazine* (30 Jan 2016 accessed 20 Oct 2016) <<http://www.scmagazineuk.com/talktalk-loses-250000-customers-post-breach--now-supplier-scam-too/article/469535/>>

Ministerial Council of Consumer Affairs, 'Review of the Australian Consumer Product Safety System' *Options Paper* (Aug 2005 accessed 2 Nov 2016) <<http://www.pc.gov.au/inquiries/completed/product-safety/optionspaper>>

Minister for Roads and Road Safety, 'Victoria Leading the Way on Autonomous Vehicle Trials' *Press release* (15 Dec 2016 accessed 18 Jan 2017) <<http://www.premier.vic.gov.au/victoria-leading-the-way-on-autonomous-vehicle-trials/>>

Miniwatts Marketing Group, 'Internet World Penetration Rates by Geographic Regions- June 2016' (accessed 2 Nov 2016) <<http://www.internetworldstats.com/stats.htm>>

Minter Ellison, 'Perspectives on Cyber risk' (n.d. accessed 10 Jun 2016) <[http://www.minterellison.com/files/uploads/documents/publications/newsletters/15%20189%20Cyber%20Report\\_Final%20v1.pdf](http://www.minterellison.com/files/uploads/documents/publications/newsletters/15%20189%20Cyber%20Report_Final%20v1.pdf)>

Minter Ellison, 'Minter Ellison's submission to the Australian Consumer Law Review' (23 May 2016 accessed 4 Sept 2016) <<http://consumerlaw.gov.au/files/2016/07/MinterEllison.pdf>>

Mobile Ecosystem Forum, 'The Impact of Trust on IoT' *Global Consumer Survey* (2016 accessed 11 May 2016) [http://www.mobileecosystemforum.com/wp-content/uploads/2016/04/IoT\\_Exec\\_Summary.pdf](http://www.mobileecosystemforum.com/wp-content/uploads/2016/04/IoT_Exec_Summary.pdf)

Mole, Beth, 'Lawsuit claims Fitbit devices dangerously underestimate heart rate' *arstechnica* (7 Jan 2016 accessed 2 Mar 2016) <<http://arstechnica.com/tech-policy/2016/01/lawsuit-claims-fitbit-devices-dangerously-underestimate-heart-rate/>>

Molteni, Megan, 'Wellness apps evade the FDA, only to land in court' *WIRED* (3 Apr 2017 accessed 3 Apr 2-17) <[https://www.wired.com/2017/04/wellness-apps-evade-fda-land-court/?mbid=nl\\_4317\\_p8&CNDID=>](https://www.wired.com/2017/04/wellness-apps-evade-fda-land-court/?mbid=nl_4317_p8&CNDID=>)>

Morey, Timothy Theodore Forbath and Allison Schoop, "Customer Data: Designing for Transparency & Trust," *Harvard Business Review* \*May 2014 accessed 3 Mar 2016) <<https://hbr.org/2015/05/customer-datadesigning-for-transparency-and-trust>>

Morgan, Jacob, 'Which Companies Dominate the "Internet of Things?"' *CloudAve* (16 Jul 2014 accessed 2 Jan 2016) <<https://www.cloudave.com/35202/companies-dominate-internet-things/>>

Morgan Stanley, 'The Internet of Things is Now' (2014 accessed 10 Feb 2016) <http://www.technologyinvestor.com/wp-content/uploads/2014/09/internet-of-Things-2.pdf>

Morrison, Scott & Kelly O'Dwyer, MPs, 'Productivity Commission to examine arrangements supporting Australian Consumer Law', *Joint Press Release* (29 Apr 2016 accessed 3 May 2016) <<http://kmo.ministers.treasury.gov.au/media-release/048-2016/>>

Moynihan, Tim, 'Alexa and Google Home record what you say. But what happens to that data?' *WIRED* (5 Dec 2016 accessed 15 Jan 2017) <<https://www.wired.com/2016/12/alex-and-google-record-your-voice/>>

Mui, Chunka, 'Is Tesla Racing Recklessly Towards Driverless Cars?' *Forbes* (19 Apr 2016 accessed 26 May 2016) <<http://www.forbes.com/sites/chunkamui/2016/04/19/is-tesla-reckless/#4f9b968c1a26>>

Munro, Kelsey, 'Data Collection: wearable fitness device information tracking your life' *The Sydney Morning Herald* (18 Apr 2015 accessed 2 Feb 2016) <<http://www.smh.com.au/digital-life/digital-life-news/data-collection-wearable-fitness-device-information-tracking-your-life-20150416-1mmzbq.html>>

Muncaster, Phil, 'UK's ICO doubled number of data breach fines in 2016' *InfoSecurity* (5 Jun 2017 accessed 7 Jun 2017) <https://www.infosecurity-magazine.com/news/uks-ico-doubled-number-of-data/>

Murphy, Margi, 'How many ways can I hack a Tesla?' *Techworld* (30 Oct 2015 accessed 12 Aug 2016) <<http://www.techworld.com/security/driverless-cars-tesla-models-self-learning-capabilities-easily-manipulate-3628448/>>

Murphy, Margi and Charlotte Jee, 'The great driverless car race: Where will the UK place?' *Techworld* (13 May 2016 accessed 26 May 2016) <<http://www.techworld.com/personal-tech/great-driverless-car-race-where-will-uk-place-3598209/>>

Murphy, Samantha, 'Samsung: By 2020, all of our products will be connected to the web' *Mashable Australia* (6 Jan 2015 accessed 20 Feb 2016) <<http://mashable.com/2015/01/05/samsung-internet-of-things/#4PJcq4DVGqR>>

Musk, Elon 'Master Plan, Part Deux' *Tesla Blog* (20 July 2016 accessed 2 Aug 2016) [https://www.tesla.com/en\\_AU/blog/master-plan-part-deux](https://www.tesla.com/en_AU/blog/master-plan-part-deux)

**N**

Narayanan, Arvin & Vitaly Shmatikov, 'Robust De-Anonymisation of Large Sparse Datasets (How to Break the Anonymity of the Netflix Prize Dataset)', *IEEE Symp. On Security and Privacy* 111 (5 Feb 2008) cited in FTC Letter to Reed

National Safety Council (US), 'Motor Vehicle Deaths Increase by largest Percent in 50 Years' (17 Feb 2016 accessed 5 May 2016) <

<http://www.nsc.org/Connect/NSCNewsReleases/Lists/Posts/Post.aspx?List=1f2e4535-5dc3-45d6-b190-9b49c7229931&ID=103&var=hppress&Web=36d1832e-7bc3-4029-98a1-317c5cd5c625>>

National Conference of State Legislatures (NCSL), 'Autonomous Self-Driving Legislation' (1 July 2016 accessed 2 Jul 2016) <<http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx>>

### **National Highway Traffic Safety Administration (NHTSA)**

NHTSA, 'Preliminary Statement of Policy concerning Automated Vehicles' (2013) <<http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development>>

NHTSA, ODI Investigation Report (15 Nov 2015 accessed 2 Apr 2016) <<http://www-odi.nhtsa.dot.gov/acms/cs/jaxrs/download/doc/UCM452870/INCLA-PE13037-2071.PDF>>

NHTSA, 'Guidelines for the Safe Deployment and Operation of Automated Vehicle Safety Technologies Meetings' (8 and 28 Apr 2016 accessed 2 Aug 2016)  
<<http://www.nhtsa.gov/Research/Crash+Avoidance/Automated+Vehicles>>

NHTSA, 'ODI Resume Investigation PE 16-007' (28 June 2016 accessed 2 Jul 2016) <<http://www-odi.nhtsa.dot.gov/acms/cs/jaxrs/download/doc/UCM530776/INOA-PE16007-7080.PDF>>

NHTSA, 'ODI Resume Investigation PE 16-007 re Tesla Motors Inc.' (19 Jan 2017 accessed 22 Jan 2017) <<https://static.nhtsa.gov/odi/inv/2016/INCLA-PE16007-7876.PDF>>

NHTSA, 'Letter to Mathew Schwall Tesla Motors, Inc.' (8 Jul 2016 accessed 20 Jul 2016) <<https://www.scribd.com/document/318112513/NHTSA-s-ODI-Opens-A-PE-On-Tesla>>

NHTSA and U.S. Department of Transportation, 'Federal Automated Vehicles Policy: Accelerating The Next Revolution In Road Safety' (September 2016 accessed 2 Oct 2016)  
<https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf>

NHTSA, 'Secretary Foxx unveils President Obama's FY17 budget proposal of nearly \$4 billion for automated vehicles and announces DOT initiatives to accelerate vehicle safety innovations' (14 Jan 2016 accessed 2 Jul 2016) <<http://www.nhtsa.gov/About+NHTSA/Press+Releases/dot-initiatives-accelerating-vehicle-safety-innovations-01142016>>

NHTSA, 'Policy statement concerning Automated Vehicles' (2016 update accessed 2 Jul 2016)  
<http://www.nhtsa.gov/About+NHTSA/Press+Releases/dot-initiatives-accelerating-vehicle-safety-innovations-01142016>

NHTSA, 'Policy update to NHTSA, 'Preliminary Statement of policy concerning Automated Vehicles' (2016 accessed 2 Aug 2016) < <http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Autonomous-Vehicles-Policy-Update-2016.pdf>>

NHTSA, 'Federal Automated Vehicles Policy: Accelerating the Next Revolution in Road Safety' (Sept 2016 accessed 22 Nov 2016)  
<<https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf>> and Fact Sheet: < [https://www.transportation.gov/sites/dot.gov/files/docs/DOT\\_AV\\_Policy.pdf](https://www.transportation.gov/sites/dot.gov/files/docs/DOT_AV_Policy.pdf)>

NHTSA, 'Cybersecurity best practices for modern vehicles' Report No. DOT HS 812 333 (October 2016 accessed 20 Nov 2016) <<https://www.transportation.gov/briefing-room/us-dot-issues-federal-guidance-automotive-industry-improving-motor-vehicle>>

NBN, 'The Internet of Things and the ACMA's Areas of Focus' *Submission to ACMA* (11 Dec 2015 accessed 10 mar 2016)  
<http://www.acma.gov.au/~media/Regulatory%20Frameworks%20and%20International%20Engagement/Issues%20for%20comment/pdf/IEuroT%20nbn%20response.pdf>>

Navigant Research 'Navigant Research Leaderboard Report: Automated Driving' (Apr 2017 accessed 3 Apr 2017) <<https://www.navigantresearch.com/research/navigant-research-leaderboard-report-automated-driving>>

Newman, Lily Hay, 'Medical devices are the next security nightmare' *WIRED* (3 Feb 2017 accessed 3 Feb 2017) < <https://www.wired.com/2017/03/medical-devices-next-security-nightmare/>>

National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure Cybersecurity' (12 Feb 2014 accessed 2 Sept 2016) version 1.0  
<<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>>

### **National Transport Commission, Australia (NTC)**

NTC, 'Compliance and enforcement framework for heavy vehicle telematics' (Nov 2014 accessed Jan 2016) < [http://www.ntc.gov.au/Media/Reports/\(C5F39CEF-3F43-490C-8D2B-569185379C55\).pdf](http://www.ntc.gov.au/Media/Reports/(C5F39CEF-3F43-490C-8D2B-569185379C55).pdf)>

NTC, 'Regulatory Options for Automated Vehicles' *Discussion Paper Executive Summary*: (May 2016 accessed 30 May 2016) [http://www.ntc.gov.au/Media/Reports/\(80E9EBF1-53F0-44F7-96CF-07D60A324122\).pdf](http://www.ntc.gov.au/Media/Reports/(80E9EBF1-53F0-44F7-96CF-07D60A324122).pdf)

NTC, 'Cooperative Intelligent Transport Systems Policy Paper' (December 2013 accessed 2 Jan 2016)  
<[https://www.ntc.gov.au/Media/Reports/\(55AFE902-73F4-073B-E6ED-AE684E3BE595\).pdf](https://www.ntc.gov.au/Media/Reports/(55AFE902-73F4-073B-E6ED-AE684E3BE595).pdf)>

NTC, 'Compliance and enforcement framework for heavy vehicle telematics' (Nov 2014 accessed 14 Oct 2016) <[http://www.ntc.gov.au/Media/Reports/\(C5F39CEF-3F43-490C-8D2B-569185379C55\).pdf](http://www.ntc.gov.au/Media/Reports/(C5F39CEF-3F43-490C-8D2B-569185379C55).pdf)>

NTC, 'Executive Summary, Regulatory Options for Automated Vehicles' *Issues Paper* (Feb 2016 accessed 30 May 2016) < [http://www.ntc.gov.au/Media/Reports/\(66E42530-B078-4B69-A5E3-53C22759F26E\).pdf](http://www.ntc.gov.au/Media/Reports/(66E42530-B078-4B69-A5E3-53C22759F26E).pdf)>

NTC, 'Regulatory Options for Automated Vehicles' *Discussion Paper* (May 2016 accessed 30 May 2016) <http://www.ntc.gov.au/current-projects/preparing-for-more-automated-road-and-rail-vehicles/>  
Note this link has changed to here: <[https://www.ntc.gov.au/Media/Reports/\(049B1ED1-5761-44D5-9E3C-814A9195285D\).pdf](https://www.ntc.gov.au/Media/Reports/(049B1ED1-5761-44D5-9E3C-814A9195285D).pdf)>

NTC, 'Regulatory reforms for Automated Road Vehicles' *Policy Paper* (Nov 2016 accessed 11 Nov 2016) < [https://www.ntc.gov.au/Media/Reports/\(32685218-7895-0E7C-ECF6-551177684E27\).pdf](https://www.ntc.gov.au/Media/Reports/(32685218-7895-0E7C-ECF6-551177684E27).pdf)>

NTC, 'National guidelines for automated vehicle trials,' *Discussion Paper* (Nov 2016 accessed 16 Nov 2016) <[https://www.ntc.gov.au/Media/Reports/\(FEAAC3B0-8F38-2C35-5FBC-4968034E6565\).pdf](https://www.ntc.gov.au/Media/Reports/(FEAAC3B0-8F38-2C35-5FBC-4968034E6565).pdf)>

NTC, 'NTC seeks feedback on proposal for drivers to allow hands off the wheel in some automated vehicles' (12 April 2017 accessed 13 Apr 2017) < <https://www.ntc.gov.au/about-ntc/news/media-releases/ntc-seeks-feedback-on-proposal-for-drivers-to-allow-hands-off-the-wheel-in-some-automated-vehicles/>>

NTC, 'Guidelines for Trials of Automated Vehicles in Australia' (April 2017 accessed 20 May 2017) < <https://www.ntc.gov.au/current-projects/automated-vehicle-trial-guidelines/>>

### **National Security Telecommunications Advisory Committee (NSTAC)**

NSTAC, 'NSTAC Report to the President on the Internet of Things' (19 Nov 2014 accessed 7 Apr 2016)  
<<https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf>>

National Telecommunications Information Administration (NTIA), 'The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things' [Docket No. 160331306-6306-01] RIN 0660-XC024, Federal Register, Vol 81, No. 66 (6 Apr 2016 accessed 2 Jun 2016) <[https://www.ntia.doc.gov/files/ntia/publications/fr\\_rfc\\_iot\\_04062016.pdf](https://www.ntia.doc.gov/files/ntia/publications/fr_rfc_iot_04062016.pdf)>

National Telecommunications and Information Commission (NTIA) and Department of Commerce, 'Notice of Extension of Comment Period on Fostering the Advancement of the Internet of Things' (12 Jan 2017 accessed 15 Jan 2017) <<https://www.ntia.doc.gov/federal-register-notice/2017/notice-extension-comment-period-fostering-advancement-internet-things>> to March 13, 2017.

National Telecommunications and Information Commission (NTIA) and Department of Commerce, 'Green Paper: Fostering the Advancement of the Internet of Things' (12 Jan 2017 accessed 15 Jan 2017) <<https://www.ntia.doc.gov/other-publication/2017/green-paper-fostering-advancement-internet-things>>

National Transport Safety Board, 'Preliminary Report, Highway HWY16FH018' (26 Jul 2016 accessed 2 Aug 2016) <<http://www.nts.gov/investigations/AccidentReports/Pages/HWY16FH018-preliminary.aspx>>

Naughton, Keith and Dana Hull, 'Ford Plans Leap from Driver's Seat with Autonomous Car by 2021' *Bloomberg Technology* (17 Aug 2016 accessed 18 Aug 2016) <<http://www.bloomberg.com/news/articles/2016-08-16/ford-aims-to-offer-fully-autonomous-ride-sharing-vehicle-by-2021>>

NBC, 'New Wi-Fi Enabled Barbie Can be Hacked, researchers Say' *NBC 5 Reports* (17 Dec 2015 accessed 10 May 2016) [http://www.nbcchicago.com/investigations/WEB-10p-pkg-Surveillance-Toy\\_Leitner\\_Chicago-353434911.html](http://www.nbcchicago.com/investigations/WEB-10p-pkg-Surveillance-Toy_Leitner_Chicago-353434911.html)

NBN Co Ltd, 'Aussie App-etite: connected devices building the future home' *Media Release* (2015 accessed 3 Dec 2015) [www.nbnco.com.au/content/dam/nbnco2/documents/aussie-app-etite-connected-devices-building-the-future-home.pdf](http://www.nbnco.com.au/content/dam/nbnco2/documents/aussie-app-etite-connected-devices-building-the-future-home.pdf)

Nest, 'Terms of Service' (UK) (updated 10 Mar 2016 accessed 2 Apr 2016) <<https://nest.com/uk/legal/terms-of-service/>>

Neagle, Colin, 'Scary stories of hacking Internet of Things devices are emerging, but how realistic is the threat?' *NetworkWorld* (2 Apr 2015 accessed 2 Sept 2016) <<http://www.networkworld.com/article/2905053/security0/smart-home-hacking-is-easier-than-you-think.html>>

Nestlé Australia, 'Disclaimer' (27 Nov 2001 accessed 10 Jun 2016) <<http://www.nestle.com.au/info/disclaimer>>

Nestlé Australia, MILO Champions, Webpage <<http://www.milo.com.au/milo-champions>>

Nestlé Australia, Privacy Policy' (updated Sept 2015 accessed 10 Jun 2016) <<http://www.nestle.com.au/info/full-privacy-policy>> and Condensed Privacy Policy' (updated Sept 2015 accessed 10 Jun 2016) <<http://www.nestle.com.au/info/privacypolicy>>

New, Joshua & Daniel Castro, 'Why Countries Need National Strategies for the Internet of things' (16 Dec 2015 accessed 5 Mar 2016) <http://www2.datainnovation.org/2015-national-iot-strategies.pdf>

New, Joshua, 'Bipartisan DIGIT Act Could Make US the Global Leader on the Internet of Things' Centre for Data Innovation (1 Mar 2016 accessed 5 Mar 2016)

<https://www.datainnovation.org/2016/03/bipartisan-digit-act-could-make-us-the-global-leader-on-the-internet-of-things/>

Newitz, Annalee, 'Facebook explains that it is totally not doing racial profiling' *Ars Technica* (22 Mar 2016 accessed 22 Mar 2016) < <http://arstechnica.co.uk/information-technology/2016/03/facebook-racial-profiling/>>

Newitz, Annalee, 'Facebook's ad platform now guesses at your race based on your behavior' *Ars Technica* (22 Mar 2016 accessed 22 Mar 2016) <<http://arstechnica.com/information-technology/2016/03/facebooks-ad-platform-now-guesses-at-your-race-based-on-your-behavior/>>

N. Newman 'How big data enables economic harm to consumers, especially to low-income and other vulnerable sectors of the population' *Journal of Internet Law*, 18(6), 11-23 (2014 accessed 3 Apr 2015) <<http://search.proquest.com/docview/1639829818?accountid=26503>>

New York Attorney-General, 'A.G. Schneiderman Announces Settlement with Uber to Enhance Rider Privacy' Media release (Jan 2016 accessed 2 Nov 2016) <<http://www.ag.ny.gov/press-release/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy>>

New York City, Guidelines for the Internet of Things, (n.d. accessed 2 Dec 2016) <<https://iot.cityofnewyork.us/>>

New York City, 'Open Data Law' (29 February 2012 accessed 2 Dec 2016) <<http://www1.nyc.gov/site/doitt/initiatives/open-data-law.page>>

New Zealand Ministry of Transport, 'Testing autonomous vehicles in New Zealand' (18 Feb 2016 accessed 2 Aug 2016) < <http://www.transport.govt.nz/ourwork/technology/specific-transport-technologies/road-vehicle/autonomous-vehicles/testing-autonomous-vehicles-in-nz/>>

Ng, Andrew & Yuanqing Lin, 'Self-driving Cars won't work until we change our roads – and attitudes' WIRED (15 Mar 2016 accessed 2 Aug 2016) < <https://www.wired.com/2016/03/self-driving-cars-wont-work-change-roads-attitudes/>>

Niccolai, James 'Thousands of medical devices are vulnerable to hacking security researchers say' *PCWorld* (29 Sept 2015 accessed 4 Apr 2016) <<http://www.pcworld.com/article/2987813/thousands-of-medical-devices-are-vulnerable-to-hacking-security-researchers-say.html>>

Nielsen, 'The Internet of Things: Can It Find a Foothold with American Audiences Today?' (Nov 2014 accessed 3 Mar 2016) <<http://www.affinova.com/resource-story/internet-of-things/>>

Nielsen, 'Australian online landscape review' (19 Jan 2016 accessed 10 May 2016) <https://www.iabaustralia.com.au/research-and-resources/research-resources/item/12-research-and-resource/2035-australian-online-landscape-review-interactive-and-pdf-dec-2015>>

Nielsen, 'Usage-based Insurance and telematics' (2016 accessed 2 Aug 2016) <  
<http://www.nielsen.com/us/en/insights/reports/2016/usage-based-insurance-and-telematics.html>>

Ninan, Simon, Bharath Gangula, Matthias von Alten & Brenna Sniderman, 'Who owns the road' Deloitte (2015 accessed 5 Apr 2016) <  
<http://dupress.com/articles/internet-of-things-iot-in-automotive-industry/?id=us:2em:3na:dup1161:eng:dup:060816>>

Nissenbaum, Helen, 'A contextual approach to privacy online' (2011 accessed 2 Jan 2016) 140  
*Daedulus, Journal of the American Academy of Arts and Sciences*, 32- 48

### **Norwegian Consumer Council (FORBRUKERRÅDET)**

FORBRUKERRÅDET, '250,000 words of app terms and conditions' (14 May 2016 accessed 22 Aug 2016) <https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/>

FORBRUKERRÅDET (Norwegian Consumer Council), 'Formal Complaint' (3 Nov 2016 accessed 2 Dec 2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/11/2016-11-03-formal-complaint-wristbands-final1.pdf>

FORBRUKERRÅDET, 'Consumer protection in fitness wearables' (Nov 2016 accessed 2 Dec 2016) <  
[https://www.forbrukerradet.no/side/fitness-wristbands-violate-european-law/Norwegian Consumer Council](https://www.forbrukerradet.no/side/fitness-wristbands-violate-european-law/Norwegian%20Consumer%20Council)>

FORBRUKERRÅDET, 'Complaint regarding user agreements and privacy policies for internet-connected toys – the Cayla doll and i-Que robot' (6 Dec 2016 accessed 15 Jan 2017) <  
<https://fil.forbrukerradet.no/wp-content/uploads/2016/12/complaint-dpa-co.pdf>>

FORBRUKERRÅDET, 'Report: Investigation of privacy and security issues with smart toys' (2 Nov 2016 accessed 15 Jan 2017) <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf>

FORBRUKERRÅDET, '#Appfail' (Nov 2016 accessed 2 Dec 2016)  
<<https://www.forbrukerradet.no/undersokelse/2015/appfail-threats-to-consumers-in-mobile-apps/>>

FORBRUKERRÅDET, '#Toyfail' (Dec 2016 accessed 15 Jan 2017) <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf>

Nolan, Philip and Mark Adair, 'The 'Internet of Things': Legal Challenges in an Ultra-connected World' *Mason Hayes & Curran* (22 Jan 2016 accessed 7 Apr 2016) <  
<http://www.lexology.com/library/detail.aspx?g=90b1f2fc-6a14-4629-aca1-69bbee850124>>

Nolan, Philip and Mark Adair, 'The 'Internet of Things' – 10 Data Protection and Privacy Challenges' *Mason Hayes & Curran* (30 Oct 2014 accessed 7 Apr 2016) <<http://www.mhc.ie/latest/blog/the-internet-of-things-10-data-protection-and-privacy-challenges> 'Part 2- top 7 Recommendations from EU Privacy regulators' (14 Nov 2014 accessed 7 Apr 2016) <<http://www.mhc.ie/latest/blog/the-internet-of-things-part-2-top-7-recommendations-from-eu-privacy-regulators>>

Nottage, Luke, 'The Government's Proposed 'Review of Australian Contract Law': A Preliminary Positive Response University of Sydney - Faculty of Law; University of Sydney - Australian Network for

Japanese Law (16 Jul 2012 accessed 17 Apr 2016)  
<[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2111826](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2111826)>

Nott, George Nott, 'Australia leads APAC for data breaches' (21 Sept 2016 accessed 29 Sept 2016)  
CIO <<http://www.cio.com.au/article/607231/australia-leads-apac-data-breaches/>>

NSW Government, 'Driverless Vehicles and Road Safety' (17 May 20-16 accessed 4 Jun 2016) <  
<https://www.parliament.nsw.gov.au/committees/DBAssets/InquirySubmission/Body/54185/Submission%2017%20-%20Inquiry%20into%20Driverless%20Vehicles%20and%20Road%20Safety%20-%20NSW%20Government.pdf>>

NSW Legislative Council Standing Committee of Law and Justice, 'Final report: remedies for the serious invasion of privacy in New South Wales' (3 Mar 2016 accessed 10 Mar 2016) <  
<https://www.parliament.nsw.gov.au/committees/DBAssets/InquiryReport/ReportAcrobat/6043/Report%20no%2057%20Remedies%20for%20the%20serious%20invasion%20of%20.pdf>>

Null, Christopher, 'Hack Your Pearly Whites with These High Tech Toothbrushes' *WIRED* (16 Apr 2017 accessed 16 Apr 2016) <[https://www.wired.com/2017/04/hack-pearly-whites-high-tech-toothbrushes/?mbid=nl\\_41617\\_p7&CNDID=>](https://www.wired.com/2017/04/hack-pearly-whites-high-tech-toothbrushes/?mbid=nl_41617_p7&CNDID=>)

## O

O'Brien, H. M., 'The Internet of Things: the inevitable collision with product liability' *Wilson Elser Product Liability Blog* (2 Feb 2015 accessed 7 Apr 2016)  
<<http://www.lexology.com/library/detail.aspx?g=d2011572-dd37-4709-a283-0f2171ab7c3d>>

O'Brien, H. M., 'The Internet of Things and the Inevitable Collision with Products Liability part 2' *Wilson Elser Product Liability Blog* (15 Jul 2015 accessed 7 Apr 2016) <  
<http://www.lexology.com/library/detail.aspx?g=b4aab3b-f02d-443a-9af1-9e5ad89fa7e0>>

O'Brien, H. M., 'The Internet of Things and the Inevitable Collision with Products Liability part 3' *Wilson Elser Product Liability Blog* (16 Oct 2015 accessed 7 Apr 2016)  
<<http://www.lexology.com/library/detail.aspx?g=3236b004-c640-4c6b-b403-7f4a13bc8f7c>>

O'Brien, H. M., 'The Internet of Things and the Inevitable Collision with Products Liability part 4' *Wilson Elser Product Liability Blog* (16 Oct 2015 accessed 7 Apr 2016) <  
<http://www.lexology.com/library/detail.aspx?g=1b8ef485-0b6c-4e0b-9e8f-6fa469d27680>>

O'Brien, H. M., 'The Internet of Things and the Inevitable Collision with Products Liability part 5' *Wilson Elser Product Liability Blog* (24 Nov 2015 accessed 7 Apr 2016) <  
<http://www.lexology.com/library/detail.aspx?g=defa40b8-f260-4236-8ca8-1363e40934da>>

Obama, President Barack, 'Now is the greatest time to be alive' *WIRED* (12 Oct 2016 accessed 12 Oct 2016) <<https://www.wired.com/2016/10/president-obama-guest-edits-wired-essay/>>

Obar, Jonathan, 'Big Data and the Phantom Public: Walter Lippman and the fallacy of data privacy self-management' *Big Data and Society* (July-Dec 2015 accessed 5 Jul 2016) 1-15 <  
[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00076-98127.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00076-98127.pdf)>

## Office of the Australian Information Commissioner (OAIC)

OAIC, 'Guide to information security' (April 2013 accessed 10 Apr 2015) [2] <  
<http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-securing-personal-information>>

OAIC, 'Guidelines for developing codes' (Sept 2013 accessed 2 Aug 2016)  
<https://www.oaic.gov.au/agencies-and-organisations/advisory-guidelines/guidelines-for-developing-codes>

OAIC, Annual Report 2014- 2015' <https://www.oaic.gov.au/resources/about-us/corporate-information/annual-reports/oaic-annual-report-201415/oaic-annual-report-2014-15.pdf>

OAIC, 'Legal Services Expenditure Report 2015-6' < <https://www.oaic.gov.au/about-us/corporate-information/legal-services/legal-services-expenditure-report-2015-16>>

OAIC, 'Privacy Commissioner: Website privacy policies are too long and complex ' (14 Aug 2013 accessed 2 Nov 2016) < <https://www.oaic.gov.au/media-and-speeches/media-releases/privacy-commissioner-website-privacy-policies-are-too-long-and-complex>>

OAIC, 'Community Attitudes to Privacy' Research Report & Survey Appendix (2014 accessed 8 Apr 2016) < <https://www.oaic.gov.au/resources/engage-with-us/community-attitudes/oaic-community-attitudes-to-privacy-survey-research-report-2013/2013-community-attitudes-to-privacy-survey-report.pdf>>

OAIC, Privacy Fact sheet 17 – Australian Privacy Principles' (Jan 2014 accessed 7 Jun 2016) <  
<https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles>>

OAIC, 'Guide to undertaking privacy impact assessments' (May 2014 accessed 2 Jan 2016)  
<<https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments>>

OAIC, 'Guide to developing an APP privacy policy' (May 2014 <<https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-developing-an-app-privacy-policy>>

OAIC, 'De-identification of Data and Information' *Privacy Business Resource 4* (April 2014 accessed 20 Apr 2015) <[http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-business-resources/privacy\\_business\\_resource\\_4.pdf](http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-business-resources/privacy_business_resource_4.pdf)>

OAIC, 'Mobile privacy: a better practice guide for mobile app developers' (Sept 2014 accessed 21 Jan 2016) < <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-for-mobile-app-developers>>

OAIC, 'Optus Enforceable undertaking' (n.d. 2015 accessed 4 Feb 2016)  
<<http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/enforceable-undertakings/enforceable-undertaking-optus.pdf>>

OAIC, 'Guide to securing personal information' (Jan 2015 accessed 8 Apr 2016)  
<https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>

OAIC, 'Australian Privacy Principles Guidelines' (1 April 2015 accessed 5 April 2015)  
[http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP\\_guidelines\\_complete\\_version\\_1\\_April\\_2015.pdf](http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP_guidelines_complete_version_1_April_2015.pdf)

OAIC, 'Productivity: a regulator's perspective' (10 Jun 2015 accessed 1 Sept 2015)  
<<https://www.oaic.gov.au/media-and-speeches/speeches/big-data-and-privacy-a-regulators-perspective>>

OAIC, Privacy Action Regulatory Policy (June 2015 accessed 3 Jan 2016) <  
<https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/>>

OAIC, 'Guide to privacy regulatory action' (June 2015 accessed 8 Apr 2016) <  
<https://www.oaic.gov.au/resources/about-us/our-regulatory-approach/guide-to-oaic-s-privacy-regulatory-action/oaic-regulatory-action-guide.pdf>>

OAIC, 'Data availability and use: submission to the Productivity Commission Issues paper' (2016 accessed 2 Sept 2016) < <https://www.oaic.gov.au/engage-with-us/submissions/data-availability-and-use-submission-to-productivity-commission-issues-paper>>

OAIC, 'Guide to developing a data breach response plan' (April 2016 accessed 8 Apr 2016)  
<<https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-developing-a-data-breach-response-plan.pdf>>

OAIC, 'Guide to Big Data and the Australian Privacy Principles' *Consultation Draft* (May 2016 accessed 2 May 2016) < <https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/>>

OAIC, 'Discussion Paper - Consent and Privacy' *Submission to Office of the Privacy Commissioner of Canada* (Jul 2016 accessed 2 Sept 2016) <<https://www.oaic.gov.au/resources/engage-with-us/submissions/discussion-paper-on-consent-and-privacy-submission-to-the-office-of-the-privacy-commissioner-of-canada.pdf>>

OAIC, Privacy management framework: enabling compliance and encouraging good practice' (n.d. accessed 10 May 2016) < <https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework>>

OAIC, 'Privacy shortcomings of Internet of Things businesses revealed' (23 Sept 2016 accessed 28 Sept 2016) < <https://www.oaic.gov.au/media-and-speeches/news/privacy-shortcomings-of-internet-of-things-businesses-revealed>>

OAIC, 'Community Attitudes to Privacy' Research Report & Survey Appendix (2017 accessed 15 May 2017): iii <https://www.oaic.gov.au/resources/engage-with-us/community-attitudes/acaps-2017/acaps-2017-report.pdf>

OAIC 'Corporate Plan 2016-17' <<https://www.oaic.gov.au/about-us/corporate-information/key-documents/corporate-plan-2016-17>>

OECD, Recommendation of the Council concerning Guidelines for Consumer Protection in the Context of Electronic Commerce [C(99)184/FINAL] (9 Dec 1999)

<[http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=C\(99\)184/FINAL&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=C(99)184/FINAL&docLanguage=En)>

OECD, 'Consumer policy toolkit' (OECD Publishing, 9 Jul. 2010)  
<<http://www.oecd.org/sti/consumer/consumer-policy-toolkit-9789264079663-en.htm>>

OECD, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013 accessed 5 Jun 2016) <  
<https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>>

OECD, 'OECD Recommendation on Consumer Policy Decision Making' (Mar 2014 accessed 5 Jun 2016) < <http://www.oecd.org/sti/consumer/Toolkit-recommendation-booklet.pdf>>

OECD, 'Consumer Protection in E-commerce: OECD Recommendation' (2016 accessed 5 Apr 2016)  
*OECD Publishing, Paris* <http://dx.doi.org/10.1787/9789264255258-en>  
[http://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf?utm\\_source=govdelivery](http://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf?utm_source=govdelivery)

OECD, 'Data-driven Innovation for Growth and Well-being: What Implications for Governments and Businesses?' STI Policy Notice (Oct 2015 accessed 16 Feb 2-16)  
<<http://www.oecd.org/sti/ieconomy/PolicyNote-DDI.pdf>>

OECD, 'Internet of Things: Seizing the Benefits and Addressing the Challenges' Working Party on Communication Infrastructures and Services Policy (May 2016 accessed 2 Aug 2016)  
<[http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP\(2015\)3/FINAL&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En)>

OFCOM, 'Promoting investment and innovation in the Internet of Things: Call for input' (23 July 2014 accessed 10 Mar 2016) < <http://stakeholders.ofcom.org.uk/binaries/consultations/iot/summary/iot-cfi.pdf>>

OFCOM, 'Promoting investment and innovation in the Internet of Things: Summary of responses and next steps' (27 Jan 2015 accessed 23 Feb 2016)  
<<http://stakeholders.ofcom.org.uk/binaries/consultations/iot/statement/loTStatement.pdf>>

Office of the Privacy Commissioner of Canada, 'Global internet of Things Sweep finds connected devices fall short on privacy' *News release* (22 Sept 2016 accessed 23 Sept 2016) <  
[https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/nr-c\\_160922/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/nr-c_160922/)>

Office of the Privacy Commissioner of Canada, "Wearable Computing — Challenges and opportunities for privacy protection", published January 2014 <[https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc\\_201401/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc_201401/)>

Office of the Privacy Commissioner in Canada, 'The Internet of Things', *Policy & Research Group* (Feb 2016 accessed 12 Apr 2016) <[https://www.priv.gc.ca/information/research-recherche/2016/iot\\_201602\\_e.pdf](https://www.priv.gc.ca/information/research-recherche/2016/iot_201602_e.pdf)>

Office of the Privacy Commissioner of Canada, 'An introduction to privacy issues with a focus on the retail and home environments', Research paper prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada, (February 2016 accessed 16 Aug 2016) <  
[https://www.priv.gc.ca/media/1808/iot\\_201602\\_e.pdf](https://www.priv.gc.ca/media/1808/iot_201602_e.pdf)>

Office of the Privacy Commissioner of Canada, 'Results of the 2016 Global Privacy Enforcement Network Sweep' (22 Sept 2016 accessed 23 Sept 2016) [https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/bg\\_160922/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/bg_160922/)>

Ohlhausen, Maureen K. 'The Internet of Things and the FTC: Does Innovation Require Intervention?' Remarks before the US Chamber of Commerce (18 Oct 2013 accessed 1 Mar 2016) <<http://www.ftc.gov/speeches/ohlhausen/130725section5speech.pdf>.>

Ohlhausen, Maureen K. 'The Internet of Things: When Things Talk Among Themselves', *FTC Internet of Things Workshop* (19 November 2013 accessed 1 Mar 2016) <[https://www.ftc.gov/sites/default/files/documents/public\\_statements/remarks-commissioner-maureen-k.ohlhausen-ftc-internet-things-workshop/131119iotspeech.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen-ftc-internet-things-workshop/131119iotspeech.pdf)>

Okpaku, Joseph, 'Testimony of Joseph Okpaku' *US Senate Commerce, Science and Transportation Committee* (15 Mar 2016 accessed 16 Mar 2-16) <[http://www.commerce.senate.gov/public/\\_cache/files/e71edd46-43d1-4498-be86-a67022e8ed90/8D352DC6542FC3045D06A357D5896D7A.testimony-of-joseph-okpaku-to-senate-commerce-committee.pdf](http://www.commerce.senate.gov/public/_cache/files/e71edd46-43d1-4498-be86-a67022e8ed90/8D352DC6542FC3045D06A357D5896D7A.testimony-of-joseph-okpaku-to-senate-commerce-committee.pdf)>

Olmstead, Kenneth & Michelle Atkinson, 'Apps permissions in the Google Play Store' *Pew Research Center* (10 Nov 2015 accessed 5 Apr 2016) < [http://www.pewinternet.org/files/2015/11/PI\\_2015-11-10\\_apps-permissions\\_FINAL.pdf](http://www.pewinternet.org/files/2015/11/PI_2015-11-10_apps-permissions_FINAL.pdf)>

### **Online Trust Alliance (OTA)**

OTA, 'The Smart Home Checklist' (21 Oct 2015 accessed 2016) <[https://otalliance.org/system/files/files/initiative/documents/ota\\_smarthome\\_check\\_list.pdf](https://otalliance.org/system/files/files/initiative/documents/ota_smarthome_check_list.pdf)>

OTA, 'IoT Trust Framework ' *Congressional Staff Briefing* (25 Nov 2015 accessed 3 Mar 2016) <[https://otalliance.org/system/files/files/initiative/documents/ota\\_-\\_iot\\_trust\\_framework\\_hill\\_staff\\_briefing\\_0.pdf](https://otalliance.org/system/files/files/initiative/documents/ota_-_iot_trust_framework_hill_staff_briefing_0.pdf)>

OTA, 'IoT Trust Framework' (8 Feb 2016 accessed 3 Mar 2016) [https://otalliance.org/system/files/files/initiative/documents/iot\\_trust\\_framework\\_2-8\\_no\\_fn.pdf](https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_2-8_no_fn.pdf)

OTA, 'Internet of Things: A Vision for the Future' (2016 accessed 20 Jan 2017) <<http://otalliance.actonsoftware.com/acton/attachment/6361/f-0099/1/-/-/-/OTA%20IoT%20Vision%20Paper.pdf>>

OTA, 'IoT Trust Framework' (8 Feb 2016 accessed 3 Mar 2016) [https://otalliance.org/system/files/files/initiative/documents/iot\\_trust\\_framework\\_2-8\\_no\\_fn.pdf](https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_2-8_no_fn.pdf)>

OTA, 'IoT Trust Framework – Resource Guide (Updated 9/1/2016)' (accessed 20 Sept 2016) <<http://otalliance.actonsoftware.com/acton/attachment/6361/f-008e/1/-/-/-/IoT%20Framework%20Resource%20Guide.pdf>>

OTA, 'Diffusing-the-IoT-Time-Bomb-Security-and-Privacy Trust Code of Conduct' (3 Jan 2016 accessed 3 Mar 2016) (RSAC 2016 Deck from Panel)

Session) <[https://otalliance.org/system/files/files/initiative/documents/ast2-w02-diffusing-the-iot-time-bomb-security-and-privacy\\_trust\\_code\\_of\\_conduct\\_v3.pdf](https://otalliance.org/system/files/files/initiative/documents/ast2-w02-diffusing-the-iot-time-bomb-security-and-privacy_trust_code_of_conduct_v3.pdf)>

OTA, 'OTA IoT Trust Framework' (3 Feb 2016 accessed 3 Mar 2016) <  
[https://otalliance.org/system/files/files/initiative/documents/iot\\_trust\\_framework\\_released\\_3-2-2016.pdf](https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_released_3-2-2016.pdf)>

OTA, Submission to Federal Communications Commission, (30 Mar 2016 accessed 4 Apr 2016) <  
<https://otalliance.org/system/files/files/initiative/documents/ota-fcc-nprm3-30.pdf>>

OTA, 'OTA Finds 100% of Recently Reported IoT Vulnerabilities Easily Avoidable' (8 Sept 2016  
accessed 20 Sept 2016) < <https://otalliance.org/news-events/press-releases/ota-finds-100-recently-reported-iot-vulnerabilities-easily-avoidable>>

OTA, 'Internet of Things: A Vision for the Future' (Oct 2016 accessed 16 Oct 2016) <  
<http://otalliance.actonsoftware.com/acton/attachment/6361/f-0099/1/-/-/-/OTA%20IoT%20Vision%20Paper.pdf>>

OTA, 'Consumer IoT Checklist' (4 Oct 2016 accessed 16 Oct 2016)  
<http://otalliance.actonsoftware.com/acton/attachment/6361/f-0096/1/-/-/-/IoT%20Checklist.pdf>

OTA, 'OTA Releases Consumer IoT Checklist' (4 Oct 2016 accessed 12 Oct 2016) <  
<https://otalliance.org/news-events/press-releases/ota-releases-consumer-iot-checklist>>

OTA, 'Enhancing the Security, Privacy and Safety of Connected Devices', Checklist  
<<http://otalliance.actonsoftware.com/acton/attachment/6361/f-0096/1/-/-/-/IoT%20Checklist.pdf>>

OTA, 'The Role of Connected Devices in Recent Cyber Attacks', Testimony of OTA Executive Director  
and President Craig Spiegle, the U.S. House of Representatives Energy and Commerce Committee (16  
Nov 2016 accessed 20 Jan 2017) <<https://otalliance.org/resources/role-connected-devices-recent-cyber-attacks>>

OTA, 'OTA Calls IoT Cyberattacks "Shot Across the Bow" IoT Trust Framework 2.0 Released -  
Coalition Embrace IoT Principles; Press Release (5 Jan 2017 accessed 20 Jan 2017)  
<<https://otalliance.org/news-events/press-releases/ota-calls-iot-cyberattacks-%E2%80%9Cshot-across-bow%E2%80%9D>>

OTA, 'Comment to NTIA', (13 Mar 2017 accessed 15 Mar 2017)  
<<https://www.ntia.doc.gov/files/ntia/publications/ota-docket170105023-7023-01.pdf>>

Open Notice, Mark Lizar and John Wunderlich, 'Kantara Consent Receipt Presentation' (n.d. accessed  
Apr 2017) <https://kantarainitiative.org/wp-content/uploads/2014/10/Kantara-Consent-Receipt-Presentation.pdf>

Oracle, 'The Internet of things from a Consumer Perspective' (26 Jan 2015 accessed 2 Mar 2016) <  
[https://blogs.oracle.com/IOT/entry/the\\_internet\\_of\\_things\\_from](https://blogs.oracle.com/IOT/entry/the_internet_of_things_from)>

Orbit City Lab, 'Submission' (11 May 2016 accessed 30 May 2016)  
<<http://www.ntc.gov.au/media/1401/ntc-discussion-paper-regulatory-options-for-automated-vehicles-may-2016-james-niles-orbit-city-lab-may-2016.pdf>>

Ormandy, Travis 'How to compromise the Enterprise Endpoint' *Google's Project Zero* (28 Jun 2016 accessed 3 Jul 2016) <<http://googleprojectzero.blogspot.com.au/2016/06/how-to-compromise-enterprise-endpoint.html>>

Ortiz, Eric, 'Prosecutors Get Warrant for Amazon Echo Data in Arkansas Murder Case' NBC News (28 Dec 2016 accessed 14 Jan 2017) <<http://www.nbcnews.com/tech/internet/prosecutors-get-warrant-amazon-echo-data-arkansas-murder-case-n700776>>

Orton-Jones, Charles, 'Ingenious ways wearables can enhance life and enterprise' *Raconteur Wearable Technology* (3 Sept 2015 accessed 2 Feb 2016) <<https://raconteur.uberflip.com/i/565601-wearable-technology/3>>

Orton-Jones, Charles, 'Ingenious ways wearables can enhance life and enterprise' *Raconteur Wearable Technology* (8 Sept 2015 accessed 2 Feb 2016) <<https://raconteur.uberflip.com/i/565601-wearable-technology/3>>

Orton-Jones, Charles, 'Disruptive startups set to make billions' *Raconteur, The Times* (28 January 2016 accessed 1st February 2016) <<http://raconteur.net/business/disruptive-startups-set-to-make-billions>>

Orton-Jones, Charles, 'Don't let the kettle take over' in *Raconteur, 'Internet of Things' The Times* (30 Mar 2016 accessed 30 Mar 2016) 10 <<https://raconteur.uberflip.com/i/658948-internet-of-things/9>>

Osborne, Charlie, 'IoT devices offered by firms ranging from Samsung to Phillips may be vulnerable to exploit and hijacking' ZDNet (6 Aug 2015 accessed 3 Jan 2016) <<http://www.zdnet.com/article/critical-security-flaws-leave-connected-home-devices-vulnerable/>>

## **Open Web Application Security Project (OWASP)**

OWASP 'Internet of Things Project'  
<[https://www.owasp.org/index.php/OWASP\\_Internet\\_of\\_Things\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project)>

OWASP, 'Internet of Things Top Ten Project' (n.d. accessed 7 Apr 2016)  
<[https://www.owasp.org/index.php/OWASP\\_Internet\\_of\\_Things\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project)>

OWASP, 'Consumer IoT Security Guidance' (14 May 2016 accessed 2 Jun 2016)  
<[http://www.owasp.org/index.php?title=IoT\\_Security\\_Guidance&oldid=216879](http://www.owasp.org/index.php?title=IoT_Security_Guidance&oldid=216879)>

Ozsale Pty Limited, Undertaking to the ACCC (27 June 2016 accessed 2 Sept 2016)  
<<http://registers.accc.gov.au/content/item.phtml?itemId=1197453&nodeId=3cfd5bc647e386a7aaa760ff17f06e99&fn=Undertaking%20-%20s87B%20-%20Ozsale%20Pty%20Limited%20-%20signed%2027%20July%202016.pdf>>

## **P**

Page, Carly 'Sales of wearables set to soar in 2016 thanks to Apple Watch success' *The Inquirer* (2 Feb 2016 accessed 29 Mar 2016) <<http://www.theinquirer.net/inquirer/news/2444610/sales-of-wearables-set-to-soar-in-2016-thanks-to-apple-watch-success>>

Page, Carly 'Samsung buys Viv AI tool to build its own assistant to rival Siri and Cortana' (6 Oct 2016 accessed 10 Oct 2016) <<http://www.computing.co.uk/ctg/news/2473325/samsung-buys-viv-ai-tool-to-build-its-own-assistant-to-rival-siri-and-cortana>>

Palese, Emma, 'From neuromorphic sensors to a chip under skin; Morality and ethics in the world of the internet of things'

*Journal of Information, Communication and Ethics in Society* (2013)11:2: 72-80 (Accessed 26 Jun 2016) <<http://www.emeraldinsight.com.ezproxy.bond.edu.au/doi/pdfplus/10.1108/JICES-12-2012-0023>>

Parks Associates, 'Top 2016 Trends for the Consumer IoT' (2016 accessed 2 Oct 2016) <<http://www.parksassociates.com/bento/shop/whitepapers/files/Parks%20Assoc%20-%20Top%202016%20Trends%20in%20IoT.pdf>>

Parks Associates, 'Parks Associates: Safety and Home/Away Use Cases Dominate Smart Home Interoperability Matrix' (29 Nov 2016 accessed 22 Jan 2017) <<http://www.marketwired.com/press-release/parks-associates-safety-home-away-use-cases-dominate-smart-home-interoperability-matrix-2179177.htm>>

Parliamentary Joint Committee on Intelligence and Security, 'Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Feb 2015 accessed 6 Mar 2016) <[http://www.aph.gov.au/Parliamentary\\_Business/Committees/Joint/Intelligence\\_and\\_Security/Data\\_Retention/Report](http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Report)>

Passikoff, Robert, 'Progressive Adds 'Bad Driver' Surveillance to Snapshot Telematics' *Forbes* (31 Mar 2015 accessed 11 Apr 2016) <<http://www.forbes.com/sites/robertpassikoff/2015/03/31/progressive-adds-bad-driver-surveillance-to-snapshot-telematics/print/>>

Patel, Neil 'How the internet of things is changing online marketing' *Forbes* (10 Dec 2015 accessed 10 Mar 2016) <<http://www.forbes.com/sites/neilpatel/2015/12/10/how-the-internet-of-things-is-changing-online-marketing/#21f2a271456e>>

Paterson, Jeannie Marie, "The Australian Unfair Contract Terms Law: The Rise of Substantive Unfairness as a Ground for Review of Standard Form Consumer Contracts" [2009] U Melb LRS 20 <<http://www.austlii.edu.au/au/journals/UMelbLRS/2009/20.html#fn37>>

Paterson, Jeannie Marie, 'Developments in consumer protection law in Australia', *Legaldate* (May 2013 accessed 25 Apr 2016) 25 <<http://search.informit.com.au.ezproxy.bond.edu.au/documentSummary;dn=323880862424908;res=IELHSS>>

Paterson, Jeannie Marie and Jonathan Gadir, "Looking at the Fine Print: Standard Form Contracts for Telecommunications Products and Consumer Protection Law in Australia" (2013) 37(1) *University of Western Australia Law Review* 45

Pattinson, Michael, 'First enforceable undertaking under new privacy laws' *Allens Linklaters* (31 Mar 2015 accessed 20 Apr 2015) <<http://www.allens.com.au/pubs/priv/fopriv31mar15.htm>>

Paton, Laura P., Sarah E. Wetmore and Clinton T Magill, 'How wearable devices could impact personal injury litigation in South Carolina' *South Carolina Lawyer* (Jan 2015 accessed 6 Apr 2016) <[http://mydigitalpublication.com/publication/?i=286946&article\\_id=2365717&view=articleBrowser&ver=html5#"complete"](http://mydigitalpublication.com/publication/?i=286946&article_id=2365717&view=articleBrowser&ver=html5#)>

Patto, James, 'These toys have eyes (and ears too): VTech security breach raises 'Internet of Things' privacy fears' *Minter Ellison Blog TMT and IP blog* (21 Apr 2016 accessed 25 Apr 2016) <<http://www.lexology.com/library/detail.aspx?g=e9fc4a57-4bbb-43d7-a414-24c72b383ac4>>

Patto, James and Paul Kallenbach, 'When IT hurts, it hurts: cyber attacks, business interruption and loss of intellectual property' *Minter Ellison Blog TMT and IP Blog* (21 Apr 2016 accessed 25 Apr 2016) <<http://www.lexology.com/library/detail.aspx?g=9b3562d6-c365-4e0f-a5d8-626f4cdec5ac>>

Pauli, Daron. 'DEFCON 23 to Host Internet of Things Slaughterfest' *The Register* (6 May 2015 accessed 3 Mar 2016) <[http://www.theregister.co.uk/2015/05/06/defcon\\_23\\_to\\_host\\_internet\\_of\\_things\\_slaughterfest/](http://www.theregister.co.uk/2015/05/06/defcon_23_to_host_internet_of_things_slaughterfest/)>

Pentland, Alex, 'Reality mining of mobile communications: Toward a New Deal on Data' *The Global Information Technology Report 2008- 2009, World Economic Forum* <[http://hd.media.mit.edu/wef\\_globalit.pdf](http://hd.media.mit.edu/wef_globalit.pdf)>

Peppet, Scott R., 'Privacy & the Personal Prospectus: should we Introduce Privacy Agents or Regulate Privacy Intermediaries?' *Iowa Law Review Bulletin* 77 <[http://lawweb.colorado.edu/profiles/pubpdfs/peppet/ILRB\\_97\\_Peppet.pdf](http://lawweb.colorado.edu/profiles/pubpdfs/peppet/ILRB_97_Peppet.pdf)>

Peppet, Scott R., 'Unravelling Privacy: The Personal Prospectus & the Threat of a Full Disclosure Future' (7 August 2010) *Northwestern University Law Review* 105 <<http://ssrn.com/abstract=1678634>>

Peppet, Scott, R., 'Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts' *UCLA Law Review* (2012) U of Colorado Law Legal Studies Research Paper No. 11-14 <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1919013](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1919013)>

Peppet, Scott R. 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' *Texas Law Review* (2104) 93 (1) 85- 178 <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2409074](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074)>

Perkins, Earl & Ant Allan, 'The Identity of Things for the Internet of Things' *Gartner* (2 Feb 2015 accessed 3 Mar 2016) < <https://www.gartner.com/doc/2975217?ref=ddisp>>

Perlow, Scott, 'Nest killed its smart home hub: What do they owe customers?' *ZDNet* (5 Apr 2016 accessed 7 Apr 2016) < <http://www.zdnet.com/article/nest-killed-its-smart-home-hub-what-do-they-owe-customers/>>

Petraeus, David, 'Excerpts from Remarks Delivered by Director David H. Petraeus at the In-Q-Tel CEO Summit' (1 Mar 2012 accessed 1 Apr 2016) <https://www.cia.gov/news-information/speeches-testimony/2012-speeches-testimony/in-q-tel-summit-remarks.html>

PIAF, 'A Privacy Impact Assessment framework for data protection and privacy rights' (21 Sept 2011 accessed 6 Mar 2016) < [http://www.piafproject.eu/ref/PIAF\\_D1\\_21\\_Sept2011Revlogo.pdf](http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf)>

Pilgrim, Timothy 'Defining the sensor society' Presentation by the Privacy Commissioner, to the 'Defining the Sensor Society Conference' at University of Queensland, Brisbane (8 May 2014 accessed 30 May 2016 ) <<https://www.oaic.gov.au/media-and-speeches/speeches/defining-the-sensor-society>>

Pilgrim, Timothy, 'Big data and privacy: a regulators perspective' (10 Jun 2015 accessed 3 Apr 2016) <<https://www.oaic.gov.au/media-and-speeches/speeches/big-data-and-privacy-a-regulators-perspective>>

Pilgrim, Timothy, 'Mandatory data breach notification discussion paper — submission to Attorney-General's Department' (3 March 2016 accessed 8 Apr 2016) <<https://www.oaic.gov.au/engage-with-us/submissions/mandatory-data-breach-notification-discussion-paper-submission-to-attorney-general-s-department>>

Pilgrim, Timothy, 'Privacy, Data & De-identification' *Speech by Timothy Pilgrim to CeBIT, Sydney* (2 May 2016 accessed 30 May 2016) <<https://www.oaic.gov.au/media-and-speeches/speeches/privacy-data-de-identification>>

Pilgrim, Timothy, 'Privacy Awareness Week Launch 2016 (16 May 2016 accessed 12 Jun 2016) *Speech by Timothy Pilgrim to the PAW Business Breakfast, Sydney* <<https://www.oaic.gov.au/media-and-speeches/speeches/privacy-awareness-week-launch-2016>>

Plouffe, Jim, 'Privacy is dead, tech evangelist tells entrepreneurs' *The Lead* (14 Jun 2016 accessed 25 Jun 2016) <<http://www.theleadsouthaustralia.com.au/industries/technology/entrepreneurs-converge-on-south-australia/>>

Pollach, I., 'A typology of communicative strategies in online privacy policies: Ethics, power and informed consent' (2005) *Journal of Business Ethics* 62(3): 221-235.

Pollach, I., 'What's wrong with online privacy policies?' (2007) *Communications of the ACM* 50(9): 103-108.

Ponemon Institute LLC, '2016 Cost of Data Breach Study: Australia' (Oct 2016 accessed 20 Oct 2016) <<http://www-03.ibm.com/security/data-breach/>>

Posner, Richard A., 'Rational Choice, Behavioural Economics, and the Law' *Stanford Law Review*, Vol. 50, No. 5 (May, 1998) 1551-1575 <<<http://www.jstor.org/stable/1229305>>

Poulin, Chris, 'Connected car security: Separating fear from fact' *TechCrunch* (23 oct 2015 accessed 11 Apr 2016) <<http://techcrunch.com/2015/10/23/connected-car-security-separating-fear-from-fact/>>

Poulsen, Kevin, 'Hacker Disables More than 100 Cars Remotely, *WIRED* (Mar. 17, 2010) <<https://www.wired.com/2010/03/hacker-bricks-cars/>>

Powell, Rose, 'Apple co-founder Steve Wozniak warns of coming 'internet of things' bubble' *The Sydney Morning Herald* (29 May 2015 accessed 25 May 2016) <<http://www.smh.com.au/business/world-business/apple-cofounder-steve-wozniak-warns-of-coming-internet-of-things-bubble-20150528-ghbjw9.html>>

Powles, Julia & Carissa Veliz, 'How Europe is fighting to change tech companies' 'wrecking ball' ethics', *The Guardian* (31 Jan 2016 accessed 31 Jan 2016)

<<https://www.theguardian.com/technology/2016/jan/30/europe-google-facebook-technology-ethics-eu-martin-schulz>>

Press, Gil, 'It's official: The Internet of Things Takes Over Big Data As the Most hyped Technology' *Forbes* (18 Aug 2014 accessed 10 Apr 2016) <http://www.forbes.com/sites/gilpress/2014/08/18/its-official-the-internet-of-things-takes-over-big-data-as-the-most-hyped-technology/#10c29f111aaa>

Press, Gil, 'Internet of Things by the Numbers: Market estimates and forecasts' *Forbes* (22 Aug 2014 accessed 26 Mar 2016) <http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/print/>

Pressman, Aaron, 'Why you probably won't be getting a Fitbit this Christmas' *Fortune.Com* (4 Nov 2016 accessed 4 Nov 2016) <<http://fortune.com/2016/11/04/probably-wont-fitbit-this-christmas/>>

Price, Rob, 'Google is deliberately deactivating some of its customers' old smart home devices' *Business Insider Australia* (5 Apr 2016 accessed 6 Apr 2016) <<http://www.businessinsider.com.au/googles-nest-closing-smart-home-company-revolv-bricking-devices-2016-4?r=US&IR=T>>

PRIPARE, 'Contribution to Study Periods Security Guidelines for the IoT and Privacy Guidelines for the IoT: Security and Privacy from an Interoperability Perspective' (10 Mar 2017 accessed 22 Mar 2017) <<http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-contribution-to-Study-periods-on-Security-and-Privacy-guidelines-for-the-IoT1.pdf>>

Pritchard, Stephen, 'The Internet of things is revolutionizing the world of sport' *The Guardian* (2 Mar 2015 accessed 17 Apr 2016) <<https://www.theguardian.com/technology/2015/mar/02/internet-of-things-sport-six-nations>>

Productivity Commission, 'Precaution and the precautionary principle: two Australian case studies', Staff Working paper by Annette Weier & Paulo Loke, (Sept 2007 accessed 2 Apr 2016) <<http://www.pc.gov.au/research/supporting/precautionary-principle/precautionaryprinciple.pdf>>

Productivity Commission, 'Review of Australia's Consumer Policy Framework' *Chapters and Appendices* (30 Apr 2008) <<http://www.pc.gov.au/inquiries/completed/consumer-policy/report/consumer2.pdf>>

Productivity Commission, 'Consumer policy framework' *Inquiry Report* (8 May 2008 accessed 20 Jan 2016) <<http://www.pc.gov.au/inquiries/completed/consumer-policy/report>>

Productivity Commission, 'Identifying and Evaluating Regulation reforms – Research Report' (2011 accessed 2 Feb 2016) <<http://www.pc.gov.au/inquiries/completed/regulation-reforms/report>>

Productivity Commission, 'Data Availability and Use' Productivity Commission Issues Paper (April 2016 accessed 26 Apr 2016) <<http://www.pc.gov.au/inquiries/current/data-access/issues>>

Productivity Commission, 'Consumer Law Enforcement and Administration' *Terms of Reference* (29 Apr 2016 accessed 29 Apr 2016) <<http://www.pc.gov.au/inquiries/current/consumer-law/terms-of-reference>>

Productivity Commission, 'Digital Disruption: What do governments need to do?' *Research Paper* (June 2016 accessed 10 June 2016) < <http://www.pc.gov.au/research/completed/digital-disruption/digital-disruption-research-paper.pdf>>

Productivity Commission, 'Consumer Law Enforcement and Administration' *Issues Paper* (July 2016 accessed 16 Jul 2016) < <http://www.pc.gov.au/inquiries/current/consumer-law/issues/consumer-law-issues.pdf>>

Productivity Commission, 'Data Availability and Use' *Draft Report* (October 2016 accessed 2 Nov 2016) <<http://www.pc.gov.au/inquiries/current/data-access/draft/data-access-draft.pdf>>

Productivity Commission, 'Draft Consumer Law Enforcement and Administration' (8 Dec 2016 accessed 8 Dec 2016) <<http://www.pc.gov.au/inquiries/current/consumer-law/draft/consumer-law-draft-overview.pdf>>

PTC Cloud Services, 'Securing the Internet of Things: Seven Steps to Minimise IoT Risk in the Cloud' (accessed 5 Feb 2016) <[http://www.ptc.com/~media/Files/PDFs/Services/PTC\\_IoT\\_CloudSecurity\\_WP.ashx?la=en](http://www.ptc.com/~media/Files/PDFs/Services/PTC_IoT_CloudSecurity_WP.ashx?la=en)>

## Q

Qina, Quan Yongrui, Z. Shenga, Nickolas J.G. Falknera, Schahram Dustdarb, Hua Wangc, Athanasios V. Vasilakosd 'When things matter: A survey on data-centric internet of things' *Journal of Network and Computer Applications*, Volume 64, April 2016, Pages 137–153

Quain, John R., 'One Day, Cars Will Connect with Your Fridge and Your Heartbeat' *The New York Times* (13 Oct 2016 accessed 16 Oct 2016) < [https://www.nytimes.com/2016/10/14/automobiles/steering-cars-toward-the-internet-of-things-on-ramp.html?\\_r=0](https://www.nytimes.com/2016/10/14/automobiles/steering-cars-toward-the-internet-of-things-on-ramp.html?_r=0)>

Queensland Government, 'Cloud computing for business' (22 May 2014 accessed 7 June 2014) <http://www.business.qld.gov.au/business/running/technology-for-business/cloud-computing-business>

Queensland University of Technology, 'Comparative analysis of overseas consumer policy frameworks' (May 2016 accessed 2 June 2016) < <http://eprints.qut.edu.au/95636/>>

Quinn, Ben, 'Google given access to healthcare data of up to 1.6 million patients' *The Guardian* (4 May 2016 accessed 4 May 2016) <<https://www.theguardian.com/technology/2016/may/04/google-deepmind-access-healthcare-data-patients>>

## R

Raconteur, 'Internet of Things' *The Times* (30 Mar 2016 accessed 30 Mar 2016) <<https://raconteur.uberflip.com/i/658948-internet-of-things/9>>

Raconteur, 'Cyber Security' *The Times* (8 Mar 2016 accessed 8 Mar 2016) <[http://raconteur.net/cyber-security-2016?utm\\_source=pardot&utm\\_medium=email&utm\\_campaign=cs0316](http://raconteur.net/cyber-security-2016?utm_source=pardot&utm_medium=email&utm_campaign=cs0316)>

Raconteur, 'Business Transformation' *The Times* (3 Mar 2016 accessed 8 Mar 2016)  
<<https://raconteur.uberflip.com/i/648003-business-transformation/0?>>

Raconteur, 'Cyber Security' *The Times* (8 Mar 2016 accessed 8 Mar 2016) <[http://raconteur.net/cyber-security-2016?utm\\_source=pardot&utm\\_medium=email&utm\\_campaign=cs0316](http://raconteur.net/cyber-security-2016?utm_source=pardot&utm_medium=email&utm_campaign=cs0316)>

RACV, '2016 Motoring Cost Report' (2016 accessed 2 Aug 2016)  
<<http://www.racv.com.au/wps/wcm/connect/racv/internet/primary/my+car/Operating+Costs>

Rainie, Lee & Shiva Maniam, 'Americans feel the tensions between privacy and security concerns' *Pew Research Centre FactTank* (19 Feb 2016 accessed 5 Apr 2016) <<http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/>>

Rainie, Lee, Sara Kiesler, Ruogu Kang and Mary Madden, 'Anonymity, Privacy, and Security Online' *Pew Research* (5 September 2013 accessed 6 Jun 2016)  
<<http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>>

Rainie, Lee & Janna Anderson, 'The Internet of Things Will Thrive by 2025' *Pew Research Center* (14 May 2014 accessed 6 Apr 2016) <[http://www.pewinternet.org/files/2014/05/PIP\\_Internet-of-things\\_0514142.pdf](http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf)>

Rainie, Lee & Maeve Duggan, 'Privacy & Information Sharing' *Pew Research Center* (14 Jan 2016 accessed 6 Apr 2016) <[http://www.pewinternet.org/files/2016/01/PI\\_2016.01.14\\_Privacy-and-Info-Sharing\\_FINAL.pdf](http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf)>

Ramirez, Edith, 'Opening Remarks of FTC Chairwoman Edith Ramirez, *FTC PrivacyCon 2017*, Washington, DC (12 January 2017 accessed 20 Jan 2017)  
<[https://www.ftc.gov/system/files/documents/public\\_statements/1049653/ramirez\\_-\\_privacycon\\_remarks\\_1-12-17.pdf](https://www.ftc.gov/system/files/documents/public_statements/1049653/ramirez_-_privacycon_remarks_1-12-17.pdf)>

Ramsay, Iain, 'Consumer Law and structures of thought; A Comment' *Journal of Consumer Policy* (1 Mar 1993 accessed 2 Feb 2016)  
<http://web.a.ebscohost.com.ezproxy.bond.edu.au/ehost/pdfviewer/pdfviewer?sid=1545548c-8247-408e-9dce-d44b5dbb52af%40sessionmgr4002&vid=1&hid=4209>

Ramsay, Iain, 'Consumer Law and Policy: Text and Materials on Regulating Consumer Markets' (3<sup>rd</sup> ed) Oxford and Portland, Oregon 2012

Ramsay, Iain, 'Consumer Law Regulatory Capitalism and the 'New learning' in Regulation' *Sydney Law Review* (2006) 29: 9– 35 <[https://sydney.edu.au/law/slr/slr28\\_1/Ramsay.pdf](https://sydney.edu.au/law/slr/slr28_1/Ramsay.pdf)>

Ramsey, Mike 'Tesla's Elon Musk says autonomous driving not all that hard to achieve' *WSJ* (17 Mar 2015 accessed 2 Aug 2016) <<http://www.wsj.com/articles/teslas-elon-musk-says-autonomous-driving-not-all-that-hard-to-achieve-1426624848>>

Rand Europe, 'Developing a Research Evaluation Framework' Research Brief by Susan Guthrie, Watu Wamae, Stephanie Diepeveen, Steven Wooding, Jonathan Grant  
<[http://www.rand.org/content/dam/rand/pubs/research\\_briefs/RB9700/RB9716/RAND\\_RB9716.pdf](http://www.rand.org/content/dam/rand/pubs/research_briefs/RB9700/RB9716/RAND_RB9716.pdf)>

Rand Corporation, 'Autonomous vehicle technology: a Guide for Policymakers' by James M. Anderson, Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras, Oluwatobi A. Oluwatola, (2015 accessed 2 Feb 2016) [http://www.rand.org/content/dam/rand/pubs/research\\_reports/RR400/RR443-2/RAND\\_RR443-2.pdf](http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-2/RAND_RR443-2.pdf)

Ranger, Steve, 'Five years until the Internet of things arrives? Why I hope it's a lot lot longer?' *ZDNet* (6 Jan 2015 accessed 7 Apr 2016) <http://www.zdnet.com/article/windows-10-tip-find-any-setting-in-seconds/>

Ranger, Steve, 'Welcome to the dystopian Internet of Things, powered by and starring you' *ZDNet* (7 Jan 2015 accessed 7 Apr 2016) <<http://www.zdnet.com/article/welcome-to-the-dystopian-internet-of-things-powered-by-and-starring-you/>>

Ranger, Steve, 'Inside the panopticon economy: The next internet revolution, privacy and you' *ZDNet* (2 Mar 2015 accessed 7 Apr 2016) < <http://www.zdnet.com/article/inside-the-panopticon-economy-privacy-the-iot-and-you/>>

Rao, Ashwini, Florian Schaub, Norman Sadeh, Alessandro Acquisti & Ruogo Kang, 'Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online' *Submission to ACM Conference on Human Factors in Computing* (2016 accessed 5 Apr 2016) < [https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00081-99936.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00081-99936.pdf)>

Rares, Steven, 'Striking the modern balance between freedom of contract and consumer rights" (FCA) [2013] *FedJSchol* 21 (accessed 2 Aug 2016) <<http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/FedJSchol/2013/21.html?query=>>

Rauscher, Karl, 'It's Time to Write the Rules of Cyberwar: The World needs a Geneva Convention for cybercombat' *IEEE Spectrum* (27 Nov 2013 accessed 16 Mar 2016) <<http://spectrum.ieee.org/telecom/security/its-time-to-write-the-rules-of-cyberwar>>

Ravindranath, Mohana, 'Who's in charge of regulating the internet of things?' *Nextgov* (1 Sept 2016 accessed 16 Oct 2016) <<http://www.nextgov.com/emerging-tech/2016/09/internet-things-regulating-charge/131208/>>

Raynor, Michael E. & Brenna Sniderman, 'Power struggle: customers, companies and the Internet of Things' *Deloitte Review Issue 17* (27 Jul 2015 accessed 26 Apr 2016) <<http://dupress.com/articles/internet-of-things-customers-companies/?id=us:2em:3na:dup1202:awa:dup:042816>>

Rebeiro, Mike, 'Big Data and the Internet of Things' *Norton Rose Fulbright* (10 Dec 2014 accessed 10 Apr 2016) <<http://www.nortonrosefulbright.com/search-site/big~00data>>

Rechtin, Mark, 'Early build Tesla Models face quality issues' *ConsumerReports* (19 Apr 2016 accessed 21 Apr 2016) <http://www.consumerreports.org/tesla/tesla-model-x-quality-issues/>

Rechtin, Mark, 'NHTSA Opens Investigation into Tesla Self-Driving Fatality: Crash underscores Consumer Reports' concerns about beta testing self-driving technology on public roads', (30 June 2016 accessed 16 Jul 2016) < <http://www.consumerreports.org/tesla/nhtsa-opens-investigation-into-tesla-self-driving-fatality/>>

Rendle, Adam 'Who owns the data in the Internet of Things?' *Taylor Wessing* (Feb 2014 accessed 19 Nov 2015) <[http://united-kingdom.taylorwessing.com/download/article\\_data\\_lot.html](http://united-kingdom.taylorwessing.com/download/article_data_lot.html)>

Reese, Hope, 'Our autonomous future: how driverless cars will be the first robots we learn to trust' *TechRepublic* <<http://www.techrepublic.com/article/our-autonomous-future-how-driverless-cars-will-be-the-first-robots-we-learn-to-trust/>>

Retter, Paul, 'The 716 Rules blocking driverless cars' *Brisbane Times* (10 May 2016 accessed 10 May 2016) <<http://www.brisbanetimes.com.au/business/consumer-affairs/the-716-rules-blocking-driverless-cars-20160509-gopyoa.html>>

Reuhs, Nichols, 'Insurance Coverage for the Internet of (Defective) Things' *Ice Miller LLP* (21 Oct 2016 accessed 29 Oct 2016) <[http://www.icemiller.com/ice-on-fire-insights/publications/insurance-coverage-for-the-internet-of-\(defective\)/](http://www.icemiller.com/ice-on-fire-insights/publications/insurance-coverage-for-the-internet-of-(defective)/)>

Reuters, 'Tesla to recall 2,700 Model X SUVs over rear seat crash risk' *The Guardian* (12 Apr 2016 accessed 21 Apr 2016) <<https://www.theguardian.com/technology/2016/apr/11/tesla-recall-model-x-suv-rear-seat>>

Reuters, 'Tesla says it has 'no way of knowing' if autopilot was used in fatal Chinese crash' *The Guardian* (15 Sept 2016 accessed 16 Oct 2016) <<https://www.theguardian.com/technology/2016/sep/14/tesla-fatal-crash-china-autopilot-gao-yaning>>

Reuters, 'Tesla Autopilot not to blame for bus accident in Germany, company says' *The Guardian* (1 Oct 2016 accessed 16 Oct 2016) <<https://www.theguardian.com/technology/2016/sep/30/tesla-autopilot-bus-crash-germany>>

Reuters, 'US East Coast hit by massive cyberattack' *AFR Weekend* (22 Oct 2016 accessed 23 Oct 2016) <<http://www.afr.com/technology/us-east-coast-hit-by-massive-cyberattack-20161021-gs8704>>

Revolv, 'A letter from Revolv's founders' (n.d. accessed 7 Apr 2016) <<http://revolv.com/>>

Richards, Kelly 'The Australian Business User Assessment of Computer User Security: a National Survey' *Australian Institute of Criminology* (2009 accessed 19 Nov 2015) <[http://www.aic.gov.au/media\\_library/publications/rpp/102/rpp102.pdf](http://www.aic.gov.au/media_library/publications/rpp/102/rpp102.pdf)>

Richardson, M. & R. Bosua; K. Clark; J. Webb, A. Ahmad & S. Maynard, 'Towards responsive regulation of the Internet of Things: Australian perspectives' (Mar 2017) *Internet Policy Review*, 6(1). (Accessed 12 Mar 2017 <DOI: 10.14763/2017.1.455>

Riederer, Chris, Sebastien Zimmeck et al, "'I don't have a photograph but you can have my footprints"- Revealing the Demographics of Location Data' *Submission to FTC Privacy Con 2016* (n.d. accessed 6 Apr 2016) <[https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00078-98129.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00078-98129.pdf)>

Roads Australia, 'National Summit of Scope of Automated vehicles: Communiqué' (23 Aug 2016 accessed 1 Sept 2016) <[http://www.austroads.com.au/images/CAV/AV\\_Meeting\\_Communique\\_23Aug2016.pdf](http://www.austroads.com.au/images/CAV/AV_Meeting_Communique_23Aug2016.pdf)> IMPORTANT RE POLICY

Roberts, Adam, 'Bentonville warrant for Amazon Echo records in murder case gets privacy advocates' attention', *4029 News* (28 Dec 2016 accessed 14 Jan 2017) <<http://www.4029tv.com/article/bentonville-warrant-for-amazon-echo-records-in-murder-case-gets-privacy-advocates-attention/8539414>>

Roberts, Al, 'Has advertising arrived on Google Home?' *ClickZ* (9 May 2017 accessed 10 May 2017) <https://www.clickz.com/has-advertising-arrived-on-google-home/110247/>

Roberts, Jeff John, 'Volkswagens, Voting Machines and Hype over Hacking' *Fortune* (14 Aug 2016 accessed 15 Aug 2016) < <http://fortune.com/2016/08/14/volkswagens-voting-machines-and-hype-over-hacking/>>

Roberts, Jeff John, 'How to Stop Hackers from Taking Over Your Home' *Fortune* (12 Oct 2016 accessed 14 Oct 2016) <<http://fortune.com/2016/10/12/hackers-home/>>

Robinson, Georgina, 'Do you remember our first ATM?' *Brisbane Times* (17 September 2007 accessed 4 Apr 2016) <http://www.brisbanetimes.com.au/news/queensland/do-you-remember-our-first-atm/2007/09/17/1189881397885.html>

Rockoff, Johnathan D., 'J&J Warns Insulin Pump Vulnerable to Cyber Hacking' *The Wall Street Journal* (4 Oct 2016 accessed 6 Oct 2016) <http://www.wsj.com/articles/j-j-warns-insulin-pump-vulnerable-to-cyber-hacking-1475610989>

Romonosky, Sasha, David Hoffman and Alessandro Acquisti, 'Empirical Analysis of Data Breach Litigation' (6 Apr 2013 accessed 6 Apr 2016) <<http://dx.doi.org/10.2139/ssrn.1986461>>

Roose, Kevin, 'Driving should be illegal' *Fusion* (6 Oct 2015 accessed 20 Aug 2016) <<http://fusion.net/story/207965/driving-should-be-illegal/>>

Rosenblatt, Seth 'Internet of Things,' not privacy, to dominate at Black Hat' *CNET* (6 Aug 2014 accessed 3 Mar 2016) < <http://www.cnet.com/news/internet-of-things-not-privacy-to-dominate-at-black-hat/>

Ross, Phillip 'A Cloud connected car is a hackable car, worries Microsoft' *IEEE Spectrum*, (11 Apr 2014 accessed 5 Sept 2016) < <http://spectrum.ieee.org/tech-talk/transportation/advanced-cars/a-connected-car-is-a-hackable-car>>

Roth, Fredric & Melissa Ventrone, '11th Circuit better defines FTC's 'Unfair' standard – The details are in the damage' *Thompson & Coburn LLP* (29 Nov 2016 accessed 5 Dec 2016) <<http://www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes/post/2016-11-29/11th-circuit-better-defines-ftc-s-unfair-standard----the-details-are-in-the-damage>>

Rothenberg, Randall, 'IAB Head: 'The Digital Advertising Industry Must Stop Having Unprotected Sex'' *Business Insider* (6 Feb 2014 accessed 9 Apr 2015) <http://www.businessinsider.com.au/iab-randall-rothenberg-supply-chain-2014-2>

Rubenstein, Ira S. & Woodrow Hartzog, 'Anonymisation and Risk' (17 Aug 2015 accessed 6 Apr 2016) *Submission to FTC PrivacyCon 2016* < [https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00033-97824.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00033-97824.pdf)>

Rushe, Dominic, 'Most cars are vulnerable to 'hacking or privacy intrusions' – report' *The Guardian* (10 Feb 2015 accessed 16 Mar 2016) < <http://www.theguardian.com/business/2015/feb/09/most-cars-vulnerable-hacking-privacy-intrusions-senate-report>>

Russell, Prof Stewart, 'The long term future of (Artificial) Intelligence' *CRASSH Cambridge* (15 May 2015 accessed 21 Apr 2016) <<https://www.youtube.com/watch?v=GYQrNfSmQ0M&app=desktop>>

Ryan, Margaret, 'Do you own your computer software?' *Phillips Ormonde Fitzpatrick* (13 Sept 2016) < <https://www.pof.com.au/do-you-own-your-computer-software/>>

## S

Saadati, Reyhaneh and Alec Christie, 'Big Data, Big issues? Is Australian Privacy Law keeping Up?' *DLA Piper* (26 July 2013 accessed 25 Mar 2015) <[https://www.dlapiper.com/en/australia/insights/publications/2013/07/big-data-big-issues-is-australian-privacy-law-ke\\_\\_/](https://www.dlapiper.com/en/australia/insights/publications/2013/07/big-data-big-issues-is-australian-privacy-law-ke__/)>

SAE International, 'Automated Driving: New International Standard J3016' (16 Jan 2014 accessed 2 Feb 2016) <[www.sae.org/misc/pdfs/automated\\_driving.pdf](http://www.sae.org/misc/pdfs/automated_driving.pdf)>

Saif, Irfan, Sean Peasley and Arun Perinkolam, 'Safeguarding the Internet of Things' *Issue 17 Deloitte Review* (2015 accessed 26 Apr 2016) <<https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ra-safeguarding%20the%20IoT.pdf>>

Salesforce, 'What is the Internet of Things?' (n.d. accessed 10 Mar 2016) <<http://www.salesforce.com/au/crm/internet-of-things/>>

Samani. Raj, '3 Key security challenges for the Internet of things' *Intel Security* (n.d. accessed 5 May 2016) <http://www.securingtomorrow.com/blog/knowledge/3-key-security-challenges-internet-things/>

Samson, Ted, 'Dropbox fiasco serves as reminder of cloud-storage insecurity' *Infoworld* (2 Aug 2012 accessed 30 July 2014): 108 <http://www.infoworld.com/t/cloud-security/dropbox-fiasco-serves-reminder-of-cloud-storage-insecurity-199197>

Samsung, 'Samsung Global Privacy Policy - SmartTV Supplement' (n.d. accessed 9 Apr 2016) <<https://www.samsung.com/uk/info/privacy-SmartTV.html>>

Samsung, 'Samsung Smart Home Terms of Service (Aust)' (n.d. accessed 2 Aug 2016) <<https://account.samsung.com/membership/etc/specialTC.do?fileName=smarthome.html>>

Samsung, 'Samsung Service Terms and Conditions' (n.d. accessed 9 Apr 2016) <<https://account.samsung.com/membership/terms>>

Samsung, 'Smart Things Product Usage Guidelines' (6 Mar 2013 accessed 9 Apr 2016) < <https://www.smartthings.com/guidelines/>>

Samsung Electronics Australia Pty Ltd, Terms and Conditions of Sale (Website only) V3.3' (3 Jun 2014 accessed 22 Aug 2016) <[http://www.samsung.com/au/estore/static/link\\_terms\\_and\\_conditions\\_of\\_sale.html](http://www.samsung.com/au/estore/static/link_terms_and_conditions_of_sale.html)>

Samsung, 'Samsung Smart TVs Do Not Monitor Living Room Conversations' *Press Release* (10 Feb 2015 accessed 10 May 2016) <<https://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-conversations>>

Samsung, 'Smart Things Privacy Policy' (3 Sept 2015 accessed 9 Apr 2016)  
<<https://www.smarthings.com/privacy>>

Samsung Electronics Australia Pty Ltd, 'Samsung Privacy Policy' (26 May 2016 Accessed 2 Aug 2016)  
<<http://www.samsung.com/au/info/privacy.html>>

Samsung, 'Smart Things Terms of Use [UK]' (3 Sept 2015 accessed 9 Apr 2016)  
<https://www.smarthings.com/uk/terms>

Samsung, 'Samsung Shows that the Internet of Things Is Now "In Sync With Real Life"' *Press Release* (8 Jan 2016 accessed 10 May 2016) <<https://news.samsung.com/global/samsung-shows-that-the-internet-of-things-is-now-in-sync-with-real-life>>

Samsung, 'Privacy Policy' (Effective 26 May 2016 accessed 3 Jun 2016)  
<<http://www.samsung.com/au/info/privacy.html>>

Samsung, "Letter to the National Telecommunications and Information Administration, US Department of Commerce On the Benefits, Challenges and Potential Roles for the Government in Fostering the Advancement of the Internet of Things" (2 June 2016 accessed 26 Jun 2016) Part 1  
<[https://www.ntia.doc.gov/files/ntia/publications/samsung\\_ntia\\_iot\\_letter\\_6-2-16-c1.pdf](https://www.ntia.doc.gov/files/ntia/publications/samsung_ntia_iot_letter_6-2-16-c1.pdf)>  
Part 2 <<https://www.ntia.doc.gov/files/ntia/publications/vc-kwon-keynote-remarks-6-2116.pdf>> and Part 3 <[https://www.ntia.doc.gov/files/ntia/publications/samsung\\_iot\\_framework\\_paper\\_july\\_2016.pdf](https://www.ntia.doc.gov/files/ntia/publications/samsung_iot_framework_paper_july_2016.pdf)>

Samsung, 'SmartThings Terms' (3 Sept 2016 accessed 9 Apr 2016)  
<<https://www.smarthings.com/uk/terms>> and Privacy (3 Sept 2016 accessed 9 Apr 2016)  
<<https://www.smarthings.com/uk/privacy>>

Samsung, 'Comment to NTIA' (13 Mar 2017 accessed 15 Mar 2017)  
<[https://www.ntia.doc.gov/files/ntia/publications/samsung\\_commerce-iot\\_comments\\_2017-03-13-c1.pdf](https://www.ntia.doc.gov/files/ntia/publications/samsung_commerce-iot_comments_2017-03-13-c1.pdf)>

Sample, Ian, 'Will your driverless car be willing to kill you to save the lives of others?' *The Guardian* (23 Jun 2016 accessed 25 Jun 2016) <<https://www.theguardian.com/science/2016/jun/23/will-your-driverless-car-be-willing-to-kill-you-to-save-the-lives-of-others>>

Samson, Alain, 'The Behavioural Economics Guide 2016' (2016 accessed 2 Sept 2016)  
<<http://www.behavioraleconomics.com/BEGuide2016.pdf>>

Sayer, Peter, 'Connected Cars gather too much data about drivers, say motorists associations' *Computerworld* (26 Nov 2015 accessed 15 Feb 2016)  
<<http://www.computerworld.com/article/3009253/data-privacy/connected-cars-gather-too-much-data-about-drivers-say-motorists-associations.html>>

Schaub, Florian, Rebecca Baleako, Adam L. Durity & Lorrie Faith Cranor, 'A design space for effective Privacy Notices' 2015 Symposium on Usable Privacy and Security, USENIX Association, *Submission to*

FTC PrivacyCon, (2016 accessed 5 Apr 2016) <<https://www.ftc.gov/policy/public-comments/initiative-623>>

Schiff, R., '3 reasons to be wary of the Internet of Things' CIO (12 Mar 2015) <<http://www.cio.com.au/article/print/570160/3-reasons-wary-internet-things/>>

Schneier, Bruce, 'How the internet of things limits consumer choice' *The Atlantic* (24 Dec 2015 accessed 22 May 2016) < <http://www.theatlantic.com/technology/archive/2015/12/internet-of-things-philips-hue-lightbulbs/421884/>>

Schneier, Bruce, 'The Internet of Things that Talk About You Behind Your Back' *Motherboard* (8 Jan 2016 accessed 26 Mar 2016) < [https://motherboard.vice.com/en\\_ca/read/the-internet-of-things-that-talk-about-you-behind-your-back](https://motherboard.vice.com/en_ca/read/the-internet-of-things-that-talk-about-you-behind-your-back)>

Schneier, Bruce, 'Data is a toxic asset, so why not throw it out?' *CNN* (1 Mar 2016 accessed 26 Mar 2016) <<http://edition.cnn.com/2016/03/01/opinions/data-is-a-toxic-asset-opinion-schneier/index.html>>

Schneier, Bruce, 'Real-World Security and the Internet of Things' (28 Jul 2016 accessed 2 Aug 2016) [https://www.schneier.com/blog/archives/2016/07/real-world\\_secu.html](https://www.schneier.com/blog/archives/2016/07/real-world_secu.html)

Schneier, Bruce, 'We Need to Save the Internet from the Internet of Things' *Motherboard* (6 Oct 2016 accessed 9 Oct 2016) < [https://www.schneier.com/essays/archives/2016/10/we\\_need\\_to\\_save\\_the\\_.html](https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html)>

Schulz, Bryta, '10 Internet of things Stats You May Not Have Known' *Vindicia Blog* (2015 accessed 23 Mar 2016) < <https://www.vindicia.com/10-internet-of-things-stats-you-may-not-have-known>>

Schulz, Martin, 'Keynote speech at #CPDP2016 on Technological, Totalitarianism, Politics and Democracy' *European Parliament the President* (28 Jan 2016 accessed 31 Jan 2016) <[http://www.europarl.europa.eu/the-president/en/press/press\\_release\\_speeches/speeches/speeches-2016/speeches-2016-january/html/keynote-speech-at-cpdp2016-on-technological-totalitarianism-politics-and-democracy;jsessionid=6519CA929AA0F0927789D0A1EA711398](http://www.europarl.europa.eu/the-president/en/press/press_release_speeches/speeches/speeches-2016/speeches-2016-january/html/keynote-speech-at-cpdp2016-on-technological-totalitarianism-politics-and-democracy;jsessionid=6519CA929AA0F0927789D0A1EA711398)>

Schuman, Evan, 'Does privacy exist anymore? Just barely.' *ComputerWorld from IDG* (11 Oct 2016 accessed 1 Nov 2016) <<http://www.computerworld.com/article/3135026/data-privacy/does-privacy-exist-anymore-just-barely.html>>

Schuman, Evan, 'Let's get serious about IoT security' *ComputerWorld from IDG* (11 Oct 2016 accessed 1 Nov 2016) <<http://www.computerworld.com/article/3130224/internet-of-things/let-s-get-serious-about-iot-security.html>>

Schuman, Evan, 'The limits of encryption' *ComputerWorld from IDG* (28 Oct 2016 accessed 1 Nov 2016) < <http://www.computerworld.com/article/3136255/data-privacy/the-limits-of-encryption.html>>

Schuman, Evan, 'The FCC's new privacy rules are toothless' *ComputerWorld from IDG* (31 Oct 2016 accessed 1 Nov 2016) < <http://www.computerworld.com/article/3136578/data-privacy/the-fcc-s-new-privacy-rules-are-toothless.html>>

Science and Environmental Health Network, 'Precautionary principle FAQs' (25 Oct 2016 accessed 6 Jul 2016) < <http://www.sehn.org/ppfaqs.html>>

Scudellari, Megan, 'Fitbit for Addicts Could Predict Relapse' *IEEE Spectrum* (14 Mar 2016 accessed 16 Mar 2016) <<http://spectrum.ieee.org/the-human-os/biomedical/diagnostics/fitbit-for-addicts-could-predict-relapse2>>

Seabrook, John, 'Network insecurity' *The New Yorker* (20 May 2013 accessed 10 Apr 2016) <http://www.newyorker.com/magazine/2013/05/20/network-insecurity>

Securities Industry and Financial Markets Association, the Asia Securities Industry and Financial Markets Association, the European Banking Association and the International Swaps and Derivatives Association, 'Position Paper: International Technical Principles' (10 May 2016 accessed 22 May 2016) <<http://www.ebf-fbe.eu/wp-content/uploads/2016/05/InternationalTechPrinciples.pdf>>

Shah, Saqib and Julian Chokkattu, 'Microsoft kills AI Chatbot Tay (twice) after it goes full Nazi' *DigitalTrends* (30 Mar 2016 accessed 4 Apr 2016) <<http://www.digitaltrends.com/social-media/microsoft-tay-chatbot/>>

Shah, Shrupti, Rachel Brody & Nick Olson, 'The regulator of tomorrow' *A GovLab report, Deloitte* (2015 accessed 5 Mar 2016) <<http://dupress.com/articles/us-regulatory-agencies-and-technology/>>

Shahan, Zachary, 'What Does Tesla Autopilot "Beta" Mean?' *Ars Technica* (11 July 2016 accessed 2 Aug 2016) <https://cleantechnica.com/2016/07/11/tesla-autopilot-beta-mean/>

Sherman, Don, 'Semi-Autonomous Cars Compared! Tesla Model S vs. BMW 750i, Infiniti Q50S, and Mercedes-Benz S65 AMG' *Car & Driver* (2 Feb 2016 accessed 3 Jun 2017) <http://www.caranddriver.com/features/semi-autonomous-cars-compared-tesla-vs-bmw-mercedes-and-infiniti-feature>

Sibley, Cain and Ken Powell, 'What about me? The Full Federal Court says personal information must be "about an individual"' *Clayton Utz* (2 Feb 2017 accessed 3 Mar 2017) <<https://www.claytonutz.com/knowledge/2017/february/what-about-me-the-full-federal-court-says-personal-information-must-be-about-an-individual>>

Siganto, Jennifer, Jodie Lomoff and Mark Burdon, 'The privacy commissioner and own-motion investigations into serious data breaches: a case of going through the motions?' *University of New South Wales Law Journal* (2015) 38 3: 1145-1185 <<http://espace.library.uq.edu.au/view/UQ:367575>>

Sims, Rod, 'ACCC's Complaint and Enforcement Policy' Speech to Committee for Economic Development of Australia, Sydney (21 February 2015 accessed 14 Jul 2015) <<http://www.accc.gov.au/speech/ceda-conference-looking-forward-to-2014>>

Sims, Rod, 'ACCC compliance and enforcement priorities for 2016' Speech to Committee for Economic Development of Australia, Sydney (23 February 2016 accessed 30 Feb 2016) <<http://www.accc.gov.au/speech/accc-compliance-and-enforcement-priorities-for-2016>>

Sims, Rod, 'Making markets work for consumers' *National Consumer Congress* (16 Mar 2016 accessed 11 Apr 2016) <<http://www.accc.gov.au/speech/making-markets-work-for-consumers>>

Sims, Rod, 'ACCC Chairman discusses the increasing concentration in Australia's economy' *Speech* (27 Oct 2016 accessed 28 Oct 2016) <<http://www.accc.gov.au/media-release/accc-chairman-discusses-the-increasing-concentration-in-australia-s-economy>>

Simonite, Tom, 'Microsoft and Google want to let artificial intelligence loose on our most sensitive data' *MIT Technology Review* (19 Apr 2016 accessed 21 Apr 2016) <<https://www.technologyreview.com/s/601294/microsoft-and-google-want-to-let-artificial-intelligence-loose-on-our-most-private-data/>>

Simpson, Angela, 'Increasing the Potential of IoT through Security and Transparency' NTIA Blog (August 02, 2016 by Angela Simpson, Deputy Assistant Secretary for Communications and Information (2 Aug 2016 accessed 4 Aug 2016) <<https://www.ntia.doc.gov/print/blog/2016/increasing-potential-iot-through-security-and-transparency>>

Singh, Rajneesh J. (ISOC) and Yoonee Jeong (TRPC) 'Does Big Data and the Internet of Things spell the End of Privacy As We Know It?', Presentation at the "Online Privacy in an Internet of Things World" Roundtable, Bangkok, Thailand (December 2014) <<http://www.internetsociety.org/blog/asia-pacific-bureau/2014/12/does-big-data-and-internet-things-spell-end-privacy-we-know-it>>

Singhvi, Anjali and Karl Russell, 'Inside the Self-Driving Tesla Fatal Accident' (updated 12 July 2016 accessed 2 Aug 2016) <<https://www.nytimes.com/interactive/2016/07/01/business/inside-tesla-accident.html>>

SINTEF. "Big Data, for better or worse: 90% of world's data generated over last two years." *ScienceDaily*, 22 May 2013. [www.sciencedaily.com/releases/2013/05/130522085217.htm](http://www.sciencedaily.com/releases/2013/05/130522085217.htm)>

Sloan, Martin and Kathryn Alexander, 'GDPR and the Digital Age of Consent for Online Services' *The IT Law Community* (3 Feb 2-16 accessed 22 Apr 2-16) <<http://www.scl.org/site.aspx?i=ed46357>>

Smith, Ian G et al (eds), 'The Internet of Things 2012 New Horizons' *Internet of Things European Research Cluster* <[http://www.internet-of-things-research.eu/pdf/IERC\\_Cluster\\_Book\\_2012\\_WEB.pdf](http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf)>

Smith, Mitch, 'Wisconsin, a Backlash Against Using Data to Foretell Defendants' Futures' *The New York Times* (22 Jun 2016 accessed 10 Feb 2017) <[https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html?\\_r=0](https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html?_r=0)>

Smith, Paul, 'Apple co-founder Steve Wozniak on the Apple Watch, electric cars and the surpassing of humanity' *Financial Review* (23 Mar 2015 accessed 25 May 2016) <<http://www.afr.com/technology/apple-cofounder-steve-wozniak-on-the-apple-watch-electric-cars-and-the-surpassing-of-humanity-20150320-1m3xxk>>

Snavely, Brent, 'Auto industry thrives despite scandals' *USA TODAY* (25 Jul 2016 accessed 5 Aug 2016) <http://www.usatoday.com/story/money/cars/2016/07/25/auto-industry-thrives-despite-scandals/87517968/>

SOHOpelesslyBroken, 'Responsible Disclosure' (2015 accessed 3 Mar 2016) <[https://www.sohopelesslybroken.com/RESPONSIBLE\\_DISCLOSURE.pdf](https://www.sohopelesslybroken.com/RESPONSIBLE_DISCLOSURE.pdf)>

Solijo, Simon, 'Unravelling: the 'internet of things' meets financial advice' *Allens* (5 Nov 2014 accessed 7 Apr 2016) <<http://www.lexology.com/library/detail.aspx?g=8e5c328a-c0c0-47a4-a875-31c6486170cc>>

Solon, Olivia, 'Should Tesla be 'beta testing' AutoPilot if there is a chance someone might die?' *The Guardian* (7 Jul 2016 accessed 2 Aug 2016) <https://www.theguardian.com/technology/2016/jul/06/tesla-autopilot-fatal-crash-public-beta-testing>>

Solon, Olivia, 'Team of hackers take remote control of Tesla Model S from 12 miles away' *The Guardian* (21 Sept 2016 accessed 3 Oct 2016) < <https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes>>

Solove, Daniel 'A Taxonomy of Privacy' *University of Pennsylvania Law Review* 154: 3 (Jan 2006 accessed 21 Apr 2016): 477- 564 <<http://www.jstor.org/stable/40041279>>

Sondergaard, Peter, 'Big Data Fades to the Algorithm Economy' Gartner Inc., *Forbes* (14 Aug 2015 accessed 6 Dec 2015) < <http://www.forbes.com/sites/gartnergroup/2015/08/14/big-data-fades-to-the-algorithm-economy/print/>>

Sondergaard, Peter, 'The Internet of Things Will Give Rise to The Algorithm Economy' Gartner (1 Jun 2015 accessed 3 Nov 2016) <<http://blogs.gartner.com/peter-sondergaard/the-internet-of-things-will-give-rise-to-the-algorithm-economy/>>

South, Tilly and Brent Savage, 'Ticked off with sneaky costs' *CHOICE* (2 Dec 2016 accessed 5 Dec 2016) <https://www.choice.com.au/travel/on-holidays/airlines/articles/preselected-extras-increase-airfare-costs>

Spary, Sara, 'Online criminals are Targeting Fitbit user accounts' *BuzzFeedNews* (7 Jan 2016 accessed 12 Nov 2016) [https://www.buzzfeed.com/saraspary/online-criminals-are-targeting-fitbit-user-accounts?utm\\_term=.ookqQKVP9#.ybxY0aWmR](https://www.buzzfeed.com/saraspary/online-criminals-are-targeting-fitbit-user-accounts?utm_term=.ookqQKVP9#.ybxY0aWmR)

Spary, Sara, 'These Fraudsters Say They Broke Into Fitbit Accounts Using Passwords Bought For 50 Cents' *BuzzFeedNews* (7 Jan 2016 accessed 12 Nov 2016) [https://www.buzzfeed.com/saraspary/revealed-the-self-styled-hackers-who-defrauded-fitbit?utm\\_term=.ney9vY8Pq#.ceaXrLZjW](https://www.buzzfeed.com/saraspary/revealed-the-self-styled-hackers-who-defrauded-fitbit?utm_term=.ney9vY8Pq#.ceaXrLZjW)

Spencer, Leon 'Valve calls for mediation before ACCC court challenge' *ZDNet* (23 Sept 2014 accessed 19 Nov 2015) < <http://www.zdnet.com/article/valve-calls-for-mediation-before-accc-court-challenge/>>

Spicer, Andre and Carl Cederstrom, 'You've heard of the internet of things, now behold the internet of me' *The Conversation* (20 Jan 2015 accessed 29 Apr 2016) <<https://theconversation.com/youve-heard-of-the-internet-of-things-now-behold-the-internet-of-me-36379>>

Staff & Agencies in Frankfurt and Tel Aviv, 'Autopilot supplier disowns Tesla for 'pushing the envelope on safety' *The Guardian* (15 Sept 2016 accessed 16 Oct 2016) <<https://www.theguardian.com/technology/2016/sep/15/autopilot-supplier-disowns-tesla-for-pushing-the-envelope-on-safety>>

Standards Australia, 'Submission to Standing Committee on Economics, Finance and Public Administration, Inquiry into the state of Australia's manufacturing industry now and beyond the resources boom (2007 accessed 4 Feb 2017) <<http://www.aphref.aph.gov.au/house/committee/efpa/manufacturing/subs.htm>>

Standards Australia, 'Submission' (9 Jun 2016 accessed 4 Sept 2016) <[http://consumerlaw.gov.au/files/2016/07/Standards\\_Australia.pdf](http://consumerlaw.gov.au/files/2016/07/Standards_Australia.pdf)>

Stanislav, Mark, 'R7-2015-27 and R7-2015-24 Fisher Price Smart Toy® and hereO GPS Platform Vulnerabilities (FIXED)' *Rapid7Community* (25 Jan 2016 accessed 7 Apr 2016) <<https://community.rapid7.com/community/infosec/blog/2016/02/02/security-vulnerabilities-within-fisher-price-smart-toy-hereo-gps-platform>>

Stanislav, Mark and Tod Beardsley, 'HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities' *Rapid7* (Sept 2015 accessed 4 Feb 2016) <https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf>

Stapleton, Jane, *Product Liability* (London: Butterworths 1994)

Statista, 'Internet of things units installed base worldwide by category from 2014 to 2016 and in 2020 (in million units)' (2016 accessed 20 Jun 2016) <<http://www.statista.com/statistics/485203/iot-units-installed-base-by-category-worldwide/>>

Statista, 'Projected size of the global connected car market in 2016 and 2021, by segment (in billion euros)' (2016 accessed 20 Jun 2016) <http://www.statista.com/statistics/297816/connected-car-market-size-by-segment/>

Statista, 'Smart Home' (2016 accessed 30 Jun 2016) <https://www.statista.com/outlook/279/100/smart-home/worldwide#>

Statista, 'Percentage of car customers in selected countries willing to share connected car data\* as of August 2015, by country and application type' (2016 accessed 20 Jun 2016) <http://www.statista.com/statistics/256157/drivers-willing-to-share-connected-car-data-with-oems-and-dealers/>

Statt, Nick, 'Nest is permanently disabling the Revolv smart home hub' *THE VERGE* (4 Apr 2016 accessed 8 Apr 2016) <<http://www.theverge.com/2016/4/4/11362928/google-nest-revolv-shutdown-smart-home-products>>

Stewart, Jack, 'After Probing Tesla's Deadly Crash, Feds say Yay to Self-driving' *WIRED* (20 Jan 2017 accessed 21 Jan 2017) <https://www.wired.com/2017/01/probing-teslas-deadly-crash-feds-say-yay-self-driving/>

Storm, Darlene, 'Pacemaker hack says worm could possibly 'commit mass murder' *ComputerWorld* (17 Oct 2012 accessed 18 Apr 2016) <<http://www.computerworld.com/article/2473402/cybercrime-hacking/pacemaker-hacker-says-worm-could-possibly--commit-mass-murder-.html>>

Streetinsider, 'Mobileye (MBLY) Issues Statement on Fatal Tesla (TSLA) Model S Autopilot' (1 Jul 2016 accessed 15 Jul 2016) <[http://www.streetinsider.com/Corporate+News/Mobileye+\(MBLY\)+Issues+Statement+on+Fatal+Tesla+\(TSLA\)+Model+S+Autopilot+Crash/11793789.html](http://www.streetinsider.com/Corporate+News/Mobileye+(MBLY)+Issues+Statement+on+Fatal+Tesla+(TSLA)+Model+S+Autopilot+Crash/11793789.html)>

Strengers, Yolande, Janine Morley, Larissa Nichols & Mike Hazas, 'The hidden cost of smart homes' (13 Jun 2016 accessed 23 Jun 2016) *The Conversation* <<http://theconversation.com/the-hidden-energy-cost-of-smart-homes-60306>>

Strickland, Eliza '5 Major Hospital Hacks: Horror Stories from the Cybersecurity Frontlines' *IEEE Spectrum* (15 Mar 2016 accessed 16 mar 2016) <<http://spectrum.ieee.org/the-human-os/biomedical/devices/5-major-hospital-hacks-horror-stories-from-the-cyber-security-frontlines>>

Subcommittee on Courts, Intellectual Property and the Internet, 'IoT Hearing - U.S. House of Representatives Judiciary Committee' (29 Jul 2015 accessed 3 Mar 2016) <[http://judiciary.house.gov/\\_cache/files/5378eb3d-fc2a-48e6-b45d-0a7ff050ec3d/114-38-95686.pdf](http://judiciary.house.gov/_cache/files/5378eb3d-fc2a-48e6-b45d-0a7ff050ec3d/114-38-95686.pdf)>

Sumner, Stuart, You: For Sale. Protecting Your Personal Data and Privacy Online (20 Aug 2015) *Elsevier Science EBLEbook Library*, ISBN 9780128034057 eISBN 9780128034231 <[http://reader.ebilib.com.au.ezproxy.bond.edu.au/\(S\(uvf0gje1akggryihw1ibszpq\)\)/Reader.aspx?p=2187472&o=297&u=1Bqg%2ffS%2by9I2WnrsEqXfBw%3d%3d&t=1457321182&h=796D5907E62FCB36249C7D476ED80E19CC5F9D57&s=23267256&ut=956&pg=1&r=img&c=-1&pat=n&cms=-1&sd=1#>](http://reader.ebilib.com.au.ezproxy.bond.edu.au/(S(uvf0gje1akggryihw1ibszpq))/Reader.aspx?p=2187472&o=297&u=1Bqg%2ffS%2by9I2WnrsEqXfBw%3d%3d&t=1457321182&h=796D5907E62FCB36249C7D476ED80E19CC5F9D57&s=23267256&ut=956&pg=1&r=img&c=-1&pat=n&cms=-1&sd=1#>)

Sung, Dan, 'What is the Internet of Things? The tech revolution explained' *WAREABLE* (4 Jul 2016 accessed 18 Jul 2016) <<http://www.wareable.com/internet-of-things/what-is-the-internet-of-things-examples-definition>>

Svantesson, Dan Jerker 'Unconscionability: Consumer Ecommerce' *Commercial Law Quarterly: The Journal of the Commercial Law Association of Australia* 25:1 (Mar/May 2011 accessed 23 May 2014) <<http://search.informit.com.au.ezproxy.bond.edu.au/document>>

Svantesson, Dan Jerker, *Extraterritoriality in Data Privacy Law* (Denmark, Narayana Press, 2013)

Svarcas, Francesca 'Turning a New Leaf: A Privacy Analysis of Carwings Electric Vehicle Data Collection and Transmission' (2012) 29 *Santa Clara Computer and High Technology Law Review* 16

Swan, Stephanie, 'Sailing into Australian Waters' *In Competition King & Wood Mallesons* (16 Nov 2016 accessed 17 Nov 2016) <http://incompetition.com.au/2016/11/sailing-australian-waters/?source=subscribe&medium=email&campaign=postnotify&id=6710&title=Sailing+into+Australia+n+waters>

Swartz, Anna, 'Microsoft's Tay AI Chatbot Went from Friendly Robot to Racist Nazi, Gets Its Plug Pulled' *Techmic* (24 mar 2016 accessed 22 May 2016) <<https://mic.com/articles/138808/microsoft-s-tay-ai-chatbot-went-from-friendly-robot-to-racist-nazi-gets-its-plug-pulled#.1M5AHtayn>>

Swinhoe, Dan, 'Infoshot: Happy Reading with Terms and Conditions', *IDG Connect* (3 Jul 2014, accessed 28 Jul 2014) <<http://www.idgconnect.com/abstract/8491/infoshot-happy-reading-with-terms-conditions>>.

## T

Takahashi, Dean, 'The Internet of Things: A Toaster That Can Tell You the Weather And A Lung Cancer Sniffer' *VB* (26 Oct 2016 accessed 28 Oct 2016) <<http://venturebeat.com/2016/10/26/the-internet-of-things-a-toaster-that-can-tell-you-the-weather-and-a-lung-cancer-sniffer/>>

Talevski, Alex, 'Why people don't care about the internet of things' *The Australian* (26 Apr 2016 accessed 29 Apr 2016) < <http://www.theaustralian.com.au/business/technology/why-people-dont-care-about-the-internet-of-things/news-story/2670ec1d7c9bc4017e10e632d1a8f90c>>

Talluri, Raj, 'We're All Building the Internet of Things, One Device at a Time' *re/code* (27 Mar 2016 accessed 4 Apr 2016) <http://recode.net/sponsored-content/were-all-building-the-internet-of-things-one-device-at-a-time/>

Tashea, Jason, 'Courts are Using AI to sentence criminals. That must stop now', *WIRED* (17 Apr 2017 accessed 18 Apr 2017) < [https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/?mbid=nl\\_41717\\_p1&CNDID=>](https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/?mbid=nl_41717_p1&CNDID=>)

Taub, Eric A., 'Owner's Manual, Out of the Glove Box and Onto the App' *The New York Times* (30 Jun 2016 accessed 16 Oct 2016) <http://www.nytimes.com/2016/07/01/automobiles/wheels/owners-manual-out-of-the-glove-box-and-onto-the-app.html?action=click&contentCollection=Automobiles&module=RelatedCoverage&region=EndOfArticle&pgtype=article>

Taub, Eric A., 'Your Car's New Software Is Ready. Update Now?' *The New York Times* (8 Sept 2016 accessed 16 Oct 2016) < <https://www.nytimes.com/2016/09/09/automobiles/your-cars-new-software-is-ready-update-now.html>>

Taylor, Josh, 'You people should stop with your whistleblowing and encryption, say Turnbull' *Crikey* (22 Apr 2016 accessed 22 Apr 2016) <http://www.crikey.com.au/2016/04/22/malcolm-turnbull-unveils-cybersecurity-strategy/>

Taylor, Louise 'Wearable technology enters business mainstream' *Taylor Wessing* (Dec 2013 accessed 19 Nov 2015) < [https://united-kingdom.taylorwessing.com/download/article\\_wearable\\_technology.html](https://united-kingdom.taylorwessing.com/download/article_wearable_technology.html)>

Taylor, Louise 'Privacy by design – essential for the growth of the Internet of Things?' *Taylor Wessing* (Feb 2014 accessed 19 Nov 2015) < [http://united-kingdom.taylorwessing.com/download/article\\_privacy\\_design.html](http://united-kingdom.taylorwessing.com/download/article_privacy_design.html)>

TechAmerica 'Mining the Big Data Gold mine' *Time News Group Advertising Feature* (2013 accessed 10 Apr 2015) [http://www.timeincnewsgroupcustompub.com/sections/120409\\_CloudComputing.pdf](http://www.timeincnewsgroupcustompub.com/sections/120409_CloudComputing.pdf)

Telstra Corp Limited, 'Telstra response to the ACA paper on the internet of Things: emerging issues in media and communications' (14 Dec 2015 accessed 10 Mar 2013) *Public Version* <http://www.acma.gov.au/~media/Regulatory%20Frameworks%20and%20International%20Engagement/Issues%20for%20comment/pdf/loT%20nbn%20response.pdf>

Telsyte, 'Digital Consumer Study' (n.d. accessed 20 Sept 2016) <<https://www.telsyte.com.au/digitalconsumerstudy/>>

Telsyte, 'Internet Uninterrupted Australian households of the Digital Future' *Research Paper* (2015 accessed 3 Dec 2015) <http://www.nbnco.com.au/content/dam/nbnco2/documents/Internet%20Uninterrupted%20Australian%20Households%20of%20the%20Connected%20Future.pdf>>

Telsyte, 'Cut through: how the Internet of things is sharpening Australia's competitive edge' A report sponsored by Microsoft (Feb 2015 accessed 17 Mar 2016)  
[http://mscorpnews.blob.core.windows.net/namedia/2015/02/Microsoft\\_IoT\\_Whitepaper.pdf](http://mscorpnews.blob.core.windows.net/namedia/2015/02/Microsoft_IoT_Whitepaper.pdf)>

Telsyte, 'Australian IOT@ Home market to reach \$3.2 Billion by 2019 embedding smart technology into Everyday Life' (10 Aug 2015 accessed 22 Apr 2016)  
<<http://www.telsyte.com.au/announcements/2015/8/10/australian-iot-home-market-to-reach-32-billion-by-2019-embedding-smart-technology-into-everyday-life-1>>

Telsyte, 'Australian Smartphone & Wearable Devices Market Study 2016-2020' (6 Sept 2016 accessed 20 Sept 2016) < <https://www.telsyte.com.au/announcements/2016/9/6/smartwatch-market-gathering-steam-as-australians-turn-to-wearable-gadgets-amid-flat-smartphone-sales>>

Tesla Motors Inc., 'Motor Vehicle Purchase Agreement Terms and Conditions' (AU) (n.d. accessed 10 Jul 2016) <[https://www.tesla.com/en\\_AU/order/download-order-agreement?country=AU&model\\_code=ms](https://www.tesla.com/en_AU/order/download-order-agreement?country=AU&model_code=ms)>

Tesla Motors Inc., 'New Vehicle Supplementary Warranty; (Model S only)' (n.d. accessed 3 Sept 2016)  
[https://www.tesla.com/.../Model\\_S\\_New\\_Vehicle\\_Limited\\_Warranty\\_201602\\_en\\_AU](https://www.tesla.com/.../Model_S_New_Vehicle_Limited_Warranty_201602_en_AU)

Tesla Motors Inc., 'About Tesla: Tesla's mission is to accelerate the world's transition to sustainable energy' (n.d. accessed 6 Jun 2016) < [https://www.teslamotors.com/en\\_AU/about](https://www.teslamotors.com/en_AU/about)>

Tesla Motors Inc., 'Service plans' (n.d. accessed 26 May 2016)  
[https://www.teslamotors.com/en\\_AU/support/service-plans](https://www.teslamotors.com/en_AU/support/service-plans)>

Tesla Motors, 'Model S Owner's Manual v 5.9' (2016 accessed 22 Aug 2016)  
<[https://www.tesla.com/sites/default/files/blog\\_attachments/model\\_s\\_owners\\_manual\\_na\\_english\\_5.9.pdf](https://www.tesla.com/sites/default/files/blog_attachments/model_s_owners_manual_na_english_5.9.pdf)

Tesla Motors, 'Model S Owner's Manual US v 8' (2015 accessed 2 May 2017)  
<<[https://www.tesla.com/sites/default/files/model\\_s\\_owners\\_manual\\_north\\_america\\_en\\_us.pdf](https://www.tesla.com/sites/default/files/model_s_owners_manual_north_america_en_us.pdf)>>

Tesla, 'Customer Privacy Policy & Terms of Use' Australia (Jan 2016 accessed 26 May 2016)  
[https://www.teslamotors.com/en\\_AU/about/legal](https://www.teslamotors.com/en_AU/about/legal)>

Tesla Motors Inc., 'A tragic loss' *Blog* (30 Jun 2016 accessed 3 Jul 2016)  
<[https://www.teslamotors.com/en\\_AU/blog/tragic-loss](https://www.teslamotors.com/en_AU/blog/tragic-loss)>

Tesla Motors Inc., 'A Tragic Loss' The Tesla Team (30 June 2016 accessed 5 July 2016) <  
[https://www.tesla.com/en\\_AU/blog/tragic-loss](https://www.tesla.com/en_AU/blog/tragic-loss)>

Tesla Motors Inc., 'Misfortune' The Tesla Team (6 July 2016 accessed 10 July 2016)  
<[https://www.tesla.com/en\\_AU/blog/misfortune](https://www.tesla.com/en_AU/blog/misfortune)>

Tesla Motors Inc., 'Upgrading Autopilot: Seeing the World in Radar' *Blog* (11 September, 2016 accessed 12 Sept 2016) < [https://www.tesla.com/en\\_AU/blog/upgrading-autopilot-seeing-world-radar](https://www.tesla.com/en_AU/blog/upgrading-autopilot-seeing-world-radar)>

Teslarati, 'Witnesses reveal new details behind deadly Tesla accident in Florida' (1 Jul 2016 accessed 4 Jul 2016) <<http://www.teslarati.com/witnesses-details-deadly-tesla-accident/>>

The Economist, 'The Rise of the Corporate Colossus threatens both competition and the legitimacy of business' (17 Sept 2016 accessed 20 Nov 2016) < <http://www.economist.com/news/leaders/21707210-rise-corporate-colossus-threatens-both-competition-and-legitimacy-business>>

Thibodeau, Patrick, 'Friday's IoT-based DDoS attack has security experts worried' *ComputerWorld* (25 Oct 2016 accessed 15 Feb 2017) <<http://www.computerworld.com/article/3134746/security/fridays-iot-based-ddos-attack-has-security-experts-worried.html>>

Thielman, Sam, "Someone is going to die": experts warn lawmakers over self-driving cars' *The Guardian* (16 Mar 2016 accessed 18 Mar 2016)  
<<https://www.theguardian.com/technology/2016/mar/15/self-driving-cars-danger-senate-general-motors-google>>

Thierer, Adam, '15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm' *Forbes Opinion* (12 Feb 2012 accessed 2 Feb 2016)  
<http://www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remain-the-perfect-paradigm/print/>

Thierer, Adam, 'Technopanics, threat inflation and the danger of the precautionary principle' 14 Minn. J. L. Sci. & Tech. 309 (2013) <<http://purl.umn.edu/144225>>

Thierer, Adam, 'Who Really believes in 'Permissionless Innovation'?' (4 Mar 2014 accessed 20 Apr 2016) < <https://techliberation.com/2013/03/04/who-really-believes-in-permissionless-innovation/>>

Thierer, Adam, 'The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation' *Mercatus Center* (19 Nov 2014 accessed 3 Mar 2016)  
<<http://mercatus.org/publication/internet-things-and-wearable-technology-addressing-privacy-and-security-concerns-without>>

Thierer, Adam & Ryan Hagemann, 'Removing Roadblocks to Intelligent Vehicles and Driverless Cars' *Mercatus Center* (17 Sept 2014 accessed 3 Mar 2016) < <http://mercatus.org/sites/default/files/Thierer-Intelligent-Vehicles.pdf>>

Thierer, Adam and Andrea Castillo, 'Projecting the Growth and Economic Impact of the Internet of Things' *Mercatus Center* (15 Jun 2015 accessed 3 Mar 2016) < <http://mercatus.org/print/1594637>>

Thierer, Adam and Michael Wilt, 'Permissionless Innovation: A 10 point Checklist for Public policymakers' *Mercatus Center* (2015 accessed 3 Mar 2016)  
<<http://mercatus.org/sites/default/files/Thierer-Permissionless-Innovation-EP-v1.pdf>>

Thierer, Adam, 'Internet of Things: Better Policy and Regulation' *Mercatus Center* (1 Oct 2015 accessed 3 Mar 2016) <http://mercatus.org/video/adam-thierer-internet-things-better-policy-and-regulation-regulation-university>

Thierer, Adam, 'The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things' *Testimony Before the National Telecommunications Information Administration* (1 Jun 2016 accessed 12 Jun 2016) < <http://mercatus.org/publication/benefits-challenges-and-potential-roles-government-fostering-advancement-internet-things>>

Thierer, Adam, Permissionless innovation: the Continuing Case for Comprehensive Technological Freedom, (2016 accessed 5 Mar 2016) <<http://mercatus.org/publication/permissionless-innovation-continuing-case-comprehensive-technological-freedom>>

Thierer, Adam, Christopher Koopman, Anne Hobson and Chris Kuiper, 'How the Internet, the Sharing Economy, and Reputational Feedback Mechanisms Solve the "Lemons Problem"' 70 *U. Miami L. Rev.* 830 (2016) <<http://repository.law.miami.edu/u/mlr/vol70/iss3/6>>

Thompson, Cadie, 'A Hacker Made a \$30 Gadget That Can Unlock Many Cars That Have Keyless Entry', *Tech Insider* (Aug. 6, 2015 accessed 25 Aug 2016) <<http://www.techinsider.io/samy-kamkar-keyless-entry-car-hack-2015-8>>

Thune, John (Chairman), 'Majority Statement' *Transportation 'The Connected World: Examining the Internet of Things' Full Committee Hearing* (11 Feb 2015 accessed 7 Mar 2016) (11 Feb 2015 accessed 7 Mar 2016) <<http://www.commerce.senate.gov/public/index.cfm/2015/2/the-connected-world-examining-the-internet-of-things>>

Tillemann, Levi & Colin McCormick, 'Will the Tesla model 3 Be the First truly Self-driving Car' *The New Yorker* (14 Apr 2016 accessed 26 May 2016) <http://www.newyorker.com/business/currency/will-the-tesla-model-3-be-the-first-truly-self-driving-car>

Timothy Tobin, Mark Brennan, Michele Farquhar and Julie Brill, 'NTIA commences Internet of Things Proceeding' *Hogan Lovells Chronicle of Data Protection Blog* (6 April 2016 accessed 17 Apr 2016) <http://www.hldataprotection.com/2016/04/articles/consumer-privacy/ntia-commences-internet-of-things-proceeding/>

Titcomb, James 'Motor insurers form alliance to tackle driverless cars' *The Telegraph* (18 Jan 2016 accessed 26 Mar 2016) <http://www.telegraph.co.uk/technology/news/12106757/Motor-insurers-form-alliance-to-tackle-driverless-cars.html>

Toesland, Finbarr, 'Starting from the ground up may be the smarter approach' in Raconteur, 'Internet of Things' *The Times* (30 Mar 2016 accessed 30 Mar 2016) <<https://raconteur.uberflip.com/i/658948-internet-of-things/9>>

Tonkinwise, Cameron, 'Ethics by design, or the Ethos of things' (2004) *Design Philosophy Papers*, 2:2, 129- 144  
<http://www.tandfonline.com.ezproxy.bond.edu.au/doi/pdf/10.2752/144871304X13966215067994>>

Towell, Noel, '96,000 public servants in new data breach' *The Canberra Times* (5 October 2016 accessed 10 Oct 2016) < <http://www.canberratimes.com.au/national/public-service/96000-public-servants-in-new-data-breach-20161004-grul2p.html>>

Toy Talk, 'Hello Barbie Companion Application Terms of Use' (14 Oct 2015 accessed 10 May 2016) <https://toytalk.com/hellobarbie/terms/>

Toy Talk, 'Hello Barbie Privacy Policy' (Revised 5 Jan 2016 accessed 10 May 2016) < <https://www.toytalk.com/hellobarbie/privacy/>>

Toy Talk, 'Privacy Policy' and 'Children's Privacy Policy' (Last revised 11 Jan 2016 accessed 10 May 2016) < <https://www.toytalk.com/legal/privacy/>>

Trader, Steven, 'Drivers in Fiat Car Hacking Suit Say their injuries are real' *Law360* (22 Mar 2016 accessed 16 Aug 2016) <[http://www.law360.com/articles/774475/drivers-in-fiat-car-hacking-suit-say-their-injuries-are-real?article\\_related\\_content=1](http://www.law360.com/articles/774475/drivers-in-fiat-car-hacking-suit-say-their-injuries-are-real?article_related_content=1)>

Tranter, Kieran, 'The Challenges of Autonomous Motor Vehicles for Queensland Road and Criminal Laws' 16:2 (2016) *QUT Law Review* 59- 81 <<https://lr.law.qut.edu.au/article/view/626/591>>

Troni, Frederica, 'Consider All Cost Elements When Planning for an Internet of Things Initiative' *Gartner* (1 July 2015 accessed 3 Mar 2016) <<https://www.gartner.com/doc/3085819?refval=&pcp=mpe>>

Trotter, J.K., 'Public NYC taxi cab Database Lets you see How celebrities Tip' *Gawker* (23 Oct 2014 accessed 12 Apr 2016) <<http://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546>>

TRUSTe, 'US Consumer Data Privacy Study: Consumer Privacy Edition' (2014 accessed 4 Apr 2016) <http://www.slideshare.net/trusteprivacyseals/2014-usconsumer-data-privacy-study-consumer-privacy-edition-fromtruste>>

TRUSTe, 'TRUSTe Guidance on Model Website Disclosures' (n.d. accessed 2 Dec 2016) <<https://chnm.gmu.edu/digitalhistory/links/pdf/chapter6/6.24c.pdf>>

Trzaskowski, Jan, 'Behavioural Economics, Neuroscience, and the Unfair Commercial Practices Directive' *Journal of Consumer Policy*, 2011 <<http://web.a.ebscohost.com.ezproxy.bond.edu.au/ehost/pdfviewer/pdfviewer?sid=53d96708-67f3-4bff-888d-860a5b6b7eb8@sessionmgr4009&vid=1&hid=4207>>

Trzaskowski, Jan, 'Lawful Distortion of Consumers' Economic Behaviour : Collateral Damage Under the Unfair Commercial Practices Directive', *European Business Law Review*, 27:1 (2016 accessed 2 Feb 2017) 25-49

Tsui, Mabel, 'The State of the Art Defence: Defining the Australian Experience in the Context of Pharmaceuticals' *QUT Law Review* 13, No 1, 2013 <<https://lr.law.qut.edu.au/article/viewFile/517/569>>

Tully, Jim 'IoT: Key Lessons to Date and Action Plan for 2016' *Gartner* (12 February 2016 accessed 3 Mar 2016) <<https://www.gartner.com/doc/3210021?plc=ddf>>

Tully, Jim, 'Mass Adoption of the Internet of Things Will Create New Opportunities and Challenges for Enterprises' *Gartner* (27 February 2015 accessed 3 Mar 2016) <<https://www.gartner.com/doc/2994817?ref=ddisp>>

Tung, Liam, 'Google Nest's battery-drain: Chilly users turn up heat over thermostat software glitch' (14 Jan 2016 accessed 7 Apr 2016) <<http://www.zdnet.com/article/google-nests-battery-drain-chilly-users-turn-up-heat-over-thermostat-software-glitch/>>

Tung, Liam, 'IoT devices will outnumber the world's population this year for the first time' *ZDNet* (7 Feb 2017 accessed 26 Feb 2017) <<http://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/>>

Turck, Matt, 'Making Sense of the Internet of Things' *TechCrunch* (25 May 2013 accessed 8 Feb 2016) <<http://techcrunch.com/2013/05/25/making-sense-of-the-internet-of-things/>>

Turck, Matt, 'The Internet of Things is Reaching Escape Velocity' *TechCrunch* (2 Dec 2014 accessed 8 Feb 2016) <<http://techcrunch.com/2014/12/02/the-internet-of-things-is-reaching-escape-velocity/>>

Turnbull, Malcolm, 'Speech to APNIC 2014' *Minister for the Department of Communications and the Arts* (15 Sept 2014 accessed 3 Apr 2016) <[http://www.minister.communications.gov.au/malcolm\\_turnbull/speeches/apnic\\_38\\_brisbane](http://www.minister.communications.gov.au/malcolm_turnbull/speeches/apnic_38_brisbane)>

Turnbull, Malcolm, 'Opening Address to AIIA Summit: Navigating the Internet of Things' (26 Mar 2015 accessed 11 May 2016) <[http://www.minister.communications.gov.au/malcolm\\_turnbull/speeches/internet\\_of\\_things\\_summit](http://www.minister.communications.gov.au/malcolm_turnbull/speeches/internet_of_things_summit)> Viewed at <<https://www.youtube.com/watch?v=t8lZl7hGCFI>>

Turnbull, Malcolm, 'Australia's Cyber Security Strategy' *Media Release* (21 Apr 2016 accessed 22 Apr 2016) <http://www.malcolmturnbull.com.au/media/australias-cyber-security-strategy>

Turow, Joseph, Michael Hennessy & Nora Draper, 'The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation', *University of Pennsylvania Annenberg School of Communications* (5 June 2015 accessed 3 Mar 2016) <<https://www.asc.upenn.edu/sites/default/files/>>

Turton, Felicity, 'Shifting the Burden of Consent under the GDPR' *SCR* (18 Feb 2016 accessed 22 Apr 2016) < <http://www.scl.org/site.aspx?i=ed46562>>

## U

UC Berkeley School of Information, 'Privacy dashboard' (n.d. accessed 20 Nov 2016) <<https://privacypatterns.org/patterns/Privacy-dashboard>>

Ublox, 'Short range low power wireless devices and Internet of things' White Paper (9 Feb 2015 accessed 22 Mar 2016) < <http://iotbusinessnews.com/download/white-papers/UBLOX-Short-Range-Low-Power-Internet-Of-Things.pdf>>

United Kingdom Government Office for Science, 'The Internet of Things: making the most of the Second Digital Revolution' (18 Dec 2014 accessed 20 Apr 2016) <<https://www.gov.uk/government/publications/internet-of-things-blackett-review>>

United Nations Human Rights Council, 'The right to privacy in the digital age' Report of the Office of the United Nations High Commissioner for Human Rights, (30 Jun 2014 accessed 13 Apr 2016) [http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37\\_en.pdf](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf)

United Nations, 'Guidelines on Consumer Protection' *Resolution 70/186 on Consumer Protection, adopted by the General Assembly on 22 December 2015* (2015 accessed 26 Jun 2016) <[http://unctad.org/meetings/en/SessionalDocuments/ares70d186\\_en.pdf](http://unctad.org/meetings/en/SessionalDocuments/ares70d186_en.pdf)>

United States Department of Health and Human Services, Food and Drug Administration, 'General Wellness: Policy for Low Risk Devices' (2016 accessed 2 Nov 2016)

<<https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429674.pdf>>

US Department of Homeland Security, 'Strategic principles for Securing the Internet of Things' (Nov 2016 accessed 15 Nov 2016)

<[https://www.dhs.gov/sites/default/files/publications/Strategic\\_Principles\\_for\\_Securing\\_the\\_Internet\\_of\\_Things-2016-1115-FINAL....pdf](https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf)>

United States Department of Justice, 'Google Forfeits \$500 Million Generated by Online Ads and Prescription Drug Sales by Canadian Online Pharmacies' (24 Aug 2011 accessed 25 April 2015)  
<<http://www.justice.gov/opa/pr/google-forfeits-500-million-generated-online-ads-prescription-drug-sales-Canadian-online>>

### **United States Government Accountability Office, (GAO)**

US GAO, 'Intelligent transportation Systems: vehicle-to-vehicle technologies Expected to offer Safety benefits, but a Variety of Deployment challenges exist' GAO-14-13, Report to congressional requesters  
<http://www.gao.gov/products/GAO-14-13>

U.S. GAO, GAO-16-350, 'Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack 8–9' (Mar. 2016 accessed 11 May 2016)  
<http://www.gao.gov/assets/680/676064.pdf>

U.S. GAO, 'Cyber Threats and Data Breaches Illustrate Need for stronger Controls across Several Agencies' *Statement of Gregory C Wilshusen* (8 Jul 2015 accessed 16 Mar 2016)  
<<http://www.gao.gov/assets/680/671253.pdf>>

United States House of Representatives, Committee on Energy and Commerce, 'Examining Ways to Improve Vehicle and Roadway Safety' *Commerce, Manufacturing, and Trade Sub-Committee (114th Congress)* (21 Oct 2015 accessed 29 May 2016) <https://energycommerce.house.gov/hearings-and-votes/hearings/examining-ways-improve-vehicle-and-roadway-safety>

United States Senate Committee on Commerce, Science and Transportation, 'Hands Off: The Future of Self-Driving Cars' < <http://www.commerce.senate.gov/public/index.cfm/2016/3/hands-off-the-future-of-self-driving-cars>>

United States Senate Committee of Commerce, Science and Transportation 'The Connected World: Examining the Internet of Things' *Full Committee Hearing* (11 Feb 2015 accessed 7 Mar 2016)  
<<http://www.commerce.senate.gov/public/index.cfm/2015/2/the-connected-world-examining-the-internet-of-things>>

Urmson, Chris, 'The view from the front seat of the Google Self-Driving Car' *Backchannel* (11 May 2015 accessed 2 Aug 2016) <https://backchannel.com/the-view-from-the-front-seat-of-the-google-self-driving-car-46fc9f3e6088#.pejix3j8>

Urmson, Chris, 'How a driverless car sees the road' *TED* (26 June 2015 accessed 5 May 2016)  
<<https://www.youtube.com/watch?v=tiwVMrTLUWg>>

Urmson, Chris, 'Google Self-Driving Car Project' *SXSW Interactive 2016* (12 Mar 2016 accessed 5 May 2016) <<https://www.youtube.com/watch?v=Uj-rK8V-rik>>

Urmson, Chris, 'Testimony of Dr Chris Urmson, Director, Self-Driving Cars, Google [X] Before the Senate Committee on Commerce, Science and Technology Hearing: "Hands Off: The Future of Self-Driving Cars" (15 Mar 2016 accessed 16 Mar 2016)

<[http://www.commerce.senate.gov/public/\\_cache/files/5c329011-bd9e-4140-b046-a595b4c89eb4/BEADFE023327834146FF4378228B8CC6.google-urmson-testimony-march152016.pdf](http://www.commerce.senate.gov/public/_cache/files/5c329011-bd9e-4140-b046-a595b4c89eb4/BEADFE023327834146FF4378228B8CC6.google-urmson-testimony-march152016.pdf)>

## V

Valasek, Chris, Charlie Miller; IOActive Security Services Technical Whitepaper; "Remote Exploitation of an Unaltered Passenger Vehicle" (10 August 2015 accessed 11 May 2016)

[http://www.ioactive.com/pdfs/IOActive\\_Remote\\_Car\\_Hacking.pdf](http://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf)

Valentino-Devries, Jennifer and Jeremy Singer-Vine, 'Websites vary prices, deals based on User's information' *The Wall Street Journal* (24 Dec 2012 accessed 20 Apr 2015)

<<http://www.wsj.com/articles/SB10001424127887323777204578189391813881534>>

Valentino-DeVries, Jennifer and Jeremy Singer-Vine, 'They Know What You're Shopping For' *The Wall Street Journal* (7 Dec 2012 accessed 28 Mar 2015)

<<http://www.wsj.com/articles/SB10001424127887324784404578143144132736214>>

Vardi, Moshe Y., 'Are Robots Taking Our Jobs' *The Conversation* (6 April 2016 accessed 8 Apr 2016)

<<https://theconversation.com/are-robots-taking-our-jobs-56537>>

Verizon, 'The Internet of Things 2015: Discover how IoT is transforming business results' (2015 accessed 26 Mar 2016) [http://www.verizonenterprise.com/resources/reports/rp\\_state-of-market-the-market-the-internet-of-things-2015\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf)

Verizon, '2016: ready, set, go for the Internet of things' (2016 accessed 11 Apr 2016)

<<http://www.verizonenterprise.com/verizon-insights/state-of-market-internet-of-things/2016/>>

Verizon, 'Impact of the Internet of things on Consumers' *Insights podcast with Ohad Zeira* (2016 accessed 11 April 2016) <<http://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf>>

Verizon, 'State of the Market: Internet of Things 2016' (2016 accessed 11 April 2016)

<<http://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf>>

Verizon, 'Value of IoT: The next step for IoT is predictive and prescriptive data analytics', *Insights podcast with Ashok Srivastava* (2016 accessed 11 April 2016)

<<http://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf>>

Verto Analytics, 'The Internet of Things is Here... but Do Consumers Care?' *IOT Watch* (Oct 2015 accessed 29 Mar 2016) <http://www.vertoanalytics.com/2015/12/the-internet-of-things-is-herebut-do-consumers-care/>

Victorian Government, Victorian Government Guide to Regulation (Jul 2014 accessed 20 Apr 2016) *Department of Treasury and Finance* <<http://www.dtf.vic.gov.au/Publications/Victoria-Economy-publications/Victorian-guide-to-regulation>>

Victorian Government, 'Victoria's future industries new energy technologies', *Discussion Paper* (Dec 2016 accessed 2 Feb 2016) [http://yoursay.business.vic.gov.au/futureindustries/application/files/8114/4823/4306/9186\\_dedjtr\\_vfi\\_document\\_new\\_energy\\_technologies\\_web.pdf](http://yoursay.business.vic.gov.au/futureindustries/application/files/8114/4823/4306/9186_dedjtr_vfi_document_new_energy_technologies_web.pdf)

Victorian Law Reform Commission, 'Surveillance in Public Places' Report 18 (12 Aug 2010 accessed 3 Apr 2016) <<http://www.lawreform.vic.gov.au/projects/surveillance-public-places/surveillance-public-places-final-report>>

Vilner, Yoav, 'The Internet of Shopping (IoS) is A Thing, and It's growing' *Forbes* (23 Mar 2016 accessed 8 Apr 2016) <<http://www.forbes.com/sites/yoavvilner/2016/03/23/the-internet-of-shopping-ios-is-a-thing-and-its-growing/print/>>

Vlaskovits, Patrick, 'Henry Ford, Innovation, and that "Faster Horse" Quote' *Harvard Business Review* (29 Aug 2011 accessed 15 Mar 2016) <https://hbr.org/2011/08/henry-ford-never-said-the-fast>

Voas, Jeffrey, 'Networks of "Things" NIST Special Publication 800- 183 (Jul 2016 accessed 2 Oct 2016) <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf>>

Vodafone US Inc. d/b/a Vodafone, 'NTIA Comment' (13 Mar 2017 accessed 25 Mar 2017) <[https://www.ntia.doc.gov/files/ntia/publications/comments\\_vodafone\\_us\\_ntia\\_green\\_paper.pdf](https://www.ntia.doc.gov/files/ntia/publications/comments_vodafone_us_ntia_green_paper.pdf)>

Vogel, 'IoT Privacy Lawsuit- Bose sued for taking headphone data without consent!' *Gardere Blog* (25 Apr 2017 accessed 26 Apr 2017) <<http://www.lexology.com/library/detail.aspx?g=19ce5f62-b7ac-4ba6-83b4-82658f1efddd>>

Voicelabs, 'The 2017 Voice Report' (15 Jan 2017 accessed 2 Mar 2017) <<http://voicelabs.co/2017/01/15/the-2017-voice-report/>>

Volvo, 'Volvo Cars plans to launch China's most advanced autonomous driving experiment' *Press Release* (7 Apr 2016 accessed 15 May 2016) <<https://www.media.volvocars.com/global/en-gb/media/pressreleases/189499/volvo-cars-plans-to-launch-chinas-most-advanced-autonomous-driving-experiment>>

Vulkanovski, Alexander, "'Home, Tweet Home": Implications of the Connected Home, Human and Habitat for Australian Consumers' ACCAN (Feb 2016 accessed 17 Apr 2016) <[http://accan.org.au/files/Reports/HomeTweetHome\\_IoT\\_Report-v2.pdf](http://accan.org.au/files/Reports/HomeTweetHome_IoT_Report-v2.pdf)>

## W

Waddell, Kaveh, 'The privacy problem with digital assistants' *The Atlantic* (24 Mar 2016 accessed 2 Nov 2016) <<http://www.theatlantic.com/technology/archive/2016/05/the-privacy-problem-with-digital-assistants/483950/>>

Wagstaff, Keith 'Out of Milk? LG's new smart fridge will let you know' *NBC News*, (7 May 2014 accessed 4 Mar 2016) < <http://www.nbcnews.com/tech/gift-guide/out-milk-lgs-new-smart-fridge-will-let-you-know-n99531>>

Walker, Kim 'The legal considerations of the internet of things' *Computer Weekly* (July 2014 accessed 19 Nov 2015) <http://www.computerweekly.com/opinion/The-legal-considerations-of-the-internet-of-things>

Walker Smith, Bryant. 'Automated Vehicles Are Probably Legal in the United States' *University of South Carolina - School of Law; Stanford Law School Center for Internet and Society* (2014) 1 *Tex. A&M L. Rev.* 411 (2014) < <http://dx.doi.org/10.2139/ssrn.2303904> >

Waller, Spencer Weber, Jillian G. Brady, R.J. Acosta and Jennifer Fair, 'Consumer Protection in the United States: An Overview' *European Journal of Consumer Law* (May 2011 accessed 20 Feb 2016) <<https://ssrn.com/abstract=1000226>>

Wang, Amy, 'Teens finally understand rights after lawyer translates Instagram terms into plain English' *The Sydney Morning Herald* (9 Jan 2017 accessed 7 Feb 2017) <<http://www.smh.com.au/technology/web-culture/teens-finally-understand-rights-after-lawyer-translates-instagram-terms-into-plain-english-20170108-gtny6d.html>>

Wang, Selina, 'Fitbit's Move Into Medical Gadgets Risks Attracting FDA Scrutiny' *Bloomberg Technology* (15 Apr 2016 accessed 20 Aug 2016) <https://www.bloomberg.com/news/articles/2016-04-15/fitbit-s-move-into-medical-gadgets-risks-attracting-fda-scrutiny>

Wang, Yang, Huichuan Xia & Yun Huang, 'Examining American and Chinese Internet Users' Contextual Privacy Preferences for Behavioural Advertising' *Submission to FTC PrivacyCon 2016* (2016 accessed 6 Apr 2016) < [https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00066-98111.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00066-98111.pdf)>

Waterman, Shaun, 'FTC, reigning in data actions, is urged to drop D-Link case' *cyberscoop* (2 Feb 2017 accessed 20 Feb 2017) <<https://www.cyberscoop.com/ftc-data-actions-ohlhausen-trump-d-link-case/>>

Weber, Rolf H., 'Internet of things - Need for a new legal environment?' (2009 accessed 2 Jan 2016) 25:1 *Computer Law & Security Review* 522- 527

Weber, Rolf H., 'Accountability in the Internet of Things' (Apr 2011 accessed 2 Jan 2016) 27:2 *Computer Law & Security Review* 133- 138 <[http://ac.els-cdn.com/ezproxy.bond.edu.au/S0267364911000069/1-s2.0-S0267364911000069-main.pdf?\\_tid=863bc528-2a16-11e6-bda1-00000aacb361&acdnat=1465018871\\_58a40825974e4ce8329d614bae3e0](http://ac.els-cdn.com/ezproxy.bond.edu.au/S0267364911000069/1-s2.0-S0267364911000069-main.pdf?_tid=863bc528-2a16-11e6-bda1-00000aacb361&acdnat=1465018871_58a40825974e4ce8329d614bae3e0)>

Weber, Rolf H., 'Internet of Things – Governance Quo Vadis?' *Computer Law & Security Review* 29 (2013) 341- 347 <<http://www.sciencedirect.com/science/article/pii/S0267364913001015>>

Weber, Rolf H., 'Internet of Things: Privacy issues revisited' *Computer Law & Security Review*, (October 2015) 31:5, 618-627

Weber, Rolf H. & Evelyn Studer, 'Cybersecurity in the Internet of Things: Legal aspects' *Computer Law and Security Review* 32 (2016) 715 – 728 <<http://ac.els->

cdn.com.ezproxy.bond.edu.au/S0267364916301169/1-s2.0-S0267364916301169-main.pdf?\_tid=abb300f8-0203-11e7-a484-00000aacb35f&acdnat=1488760224\_1022e6aabd3787bcc450c2486e13b688>

Weidersen, Sarah, 'CHOICE takes aim at MILO fitness trackers' AAP (6 December 2016 accessed 24 Mar 2017) <http://www.news.com.au/national/breaking-news/choice-takes-aim-at-milo-fitness-trackers>

Weier, A. and P. Loke, 'Precaution and the Precautionary Principle: two Australian case studies', *Productivity Commission Staff Working Paper*, Melbourne, (Sept, 2007)

Weiner, Gabriel and Bryant Walker Smith, 'Automated Driving: Legislative and Regulatory Action' *Stanford University* (1 Jun 2016 accessed 2 Aug 2016) <[cyberlaw.stanford.edu/wiki/index.php/Automated\\_Driving:\\_Legislative\\_and\\_Regulatory\\_Action](http://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action)>

Weiner, Gabriel and Bryant Walker Smith, 'Automated Driving: Legislative and Regulatory Action' (n.d. accessed 10 Nov 2016) <[cyberlaw.stanford.edu/wiki/index.php/Automated\\_Driving:\\_Legislative\\_and\\_Regulatory\\_Action](http://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action)>

Weins, Kyle, 'We Can't Let John Deere Destroy the Very Idea of Ownership' *WIRED* (21 Apr 2015 accessed 2 Apr 2016) < <http://www.wired.com/2015/04/dmca-ownership-john-deere/>>

Welsh, Jonathan, "Late on a Car Loan? Meet the Disabler" *The Wall Street Journal* (25 Mar 2009 accessed 16 Mar 2016) < <http://www.wsj.com/articles/SB123794137545832713>>

Wheatman, Jeffrey. 'Musings from Def Con 23: Internet of Things Risks Are Bad and Likely to Get Worse' *Gartner* (25 September 2015 accessed 3 Mar 2016) < <https://www.gartner.com/doc/3137426?ref=ddisp>>

Whelan, Robert, 'Insurance council of Australia, Submission to Attorney-General's department as to Privacy Mandatory Data Breach (3 Mar 2016 accessed 10 Apr 2016) [http://www.insurancecouncil.com.au/assets/2016\\_03\\_03\\_Submission\\_Privacy%20breach%20notification.pdf](http://www.insurancecouncil.com.au/assets/2016_03_03_Submission_Privacy%20breach%20notification.pdf)

Whigham, Nick, 'Tesla Autopilot update to improve 'probability of safety,' Musk says' (12 Sept 2016 accessed 12 Sept 2016) < <http://www.news.com.au/technology/innovation/motoring/tesla-autopilot-update-to-improve-probability-of-safety-musk-says/news-story/70cfa99decd5209c4b52b0887a3e3e69>>

Whittaker, Zack, 'Two newly-discovered flaws light fire under IoT security' *ZDNet* (2 Feb 2016 accessed 7 Apr 2016) < <http://www.zdnet.com/article/two-newly-discovered-security-flaws-light-fire-under-internet-of-things-again/>>

Whittington, Jan, & Chris Jay Hoofnagle, 'Free: Accounting for the Costs of the Internet's most Popular price' 61 *UCLA L. Rev.* (2014) 606.

Wiese, Elizabeth, 'Hey Siri and Alexa, Let's talk privacy practices' *USATODAY* (2 Mar 2016 accessed 4 Apr 2016) <<https://consumercal.org/hey-siri-and-alexas-lets-talk-privacy-practices/>>

Wikileaks, 'Vault 7: CIA Hacking Tools Revealed' (7 Mar 2017 accessed 12 Mar 2017) <<https://wikileaks.org/ciav7p1/>>

Williams, Michael, "Protecting Business Data in The Information Age Test" *Gilbert & Tobin* (14 Feb 2016 accessed 8 Aug 2016) <https://www.gtlaw.com.au/?q=protecting-business-data-information-age-test-0>

Wilson Elser, 'The Internet of Things: the inevitable collision with product liability' (2 Feb 2015 accessed 2 Oct 2016) < <http://www.lexology.com/library/detail.aspx?g=d2011572-dd37-4709-a283-0f2171ab7c3d>>

Wilson Elser, 'Defending against Product Liability Down Under Part one' (19 Jun 2016 accessed 2 Jul 2016) <<http://www.productliabilityadvocate.com/2015/06/dealing-with-product-liability-down-under/>>

Wilson Elser, 'Defending against Product Liability Down Under' (20 Jun 2016 accessed 2 Jul 2016) <<http://www.lexology.com/library/detail.aspx?g=ddaaedcc-75d0-43df-ab98-0fc5b671231a>>

Winter, Jennifer Sunrise, 'Surveillance in ubiquitous network societies: normative conflicts related to consumer in-store supermarket experience in the context of the Internet of things' *Ethics Info Technology* (2014) 16:27-41 accessed 3 Aug 2016)  
<http://search.proquest.com.ezproxy.bond.edu.au/docview/1507644277?OpenUrlRefId=info:xri/sid:primo&accountid=26503>

Witt, Terry, Police Beat section of the Florida Levy Journal, < <https://www.levyjournalonline.com/police-beat.html>>

Wolf Thiess, 'WI-FI/Copyright' (12 Oct 2016 accessed 13 Oct 2016) < <http://www.lexology.com/library/detail.aspx?g=0a4ee6ad-a059-492c-9e0b-180b3370519f>>

Wolf, Christopher and Jules Polonetsky, 'An Updated Privacy Paradigm for the Internet of Things' *The Future of Privacy Forum* (19 Nov 2013 accessed 3 Jan 2016) <<https://fpf.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf>>

Wong, Julia Carrie, 'We're just rentals': Uber drivers ask where they fit in a self-driving future', *The Guardian* (19 Aug 2016 accessed 20 Aug 2016)  
<https://www.theguardian.com/technology/2016/aug/19/uber-self-driving-pittsburgh-what-drivers-think>

Wood, Colin, 'Rethinking Privacy: Though Technology has Outpaced Policy, That's No Reason to Give Up' *Government Technology* (2 June 2014 accessed 30 Mar 2015)  
<http://www.govtech.com/data/Rethinking-Privacy-Though-Technology-has-Outpaced-Policy-Thats-No-Reason-to-Give-Up.html>

Woollacott, Emma, 'Building innovation through APIS' *Raconteur, The Times* (28 January 2016 accessed 1st February 2016) <<http://raconteur.net/business/building-innovation-through-apis>>

Wright, David, 'A Framework for the ethical impact assessment of information technology' *Ethics and Information Technology* 13: 3 (2011) 199–226 accessed 3 Mar 2016  
<<http://dl.acm.org/citation.cfm?id=2035938>>

Wroe, David & Nino Bucci, 'Police access phone and internet data 1300 times a week' (14 Jan 2015 accessed 2 Feb 2017) *The Syd Morning Herald* <<http://www.smh.com.au/federal-politics/political-news/police-access-phone-and-internet-data-1200-times-a-week-20150113-12nga3.html>>

## X

Xavier, Patrick, 'Behavioural Economics and Customer Complaints in Communication Markets' A report prepared for the Australian Communications and Media Authority in connection with the public inquiry "Reconnecting the Customer" (May 2011 accessed 4 Jun 2016) <<http://www.acma.gov.au/Industry/Telco/Reconnecting-the-customer/Public-inquiry/communications-behavioural-economics-research-reconnecting-the-customer-acma>>

## Y

Yadron, Danny 'White House seeks its first ever chief information security officer' *The Guardian* (9 Feb 2016 accessed 5 Jun 2016) <<https://www.theguardian.com/technology/2016/feb/09/white-house-seeks-first-chief-information-security-officer-hackers-cybersecurity-hacking>>

Yadron, Danny, 'Facebook, Google and WhatsApp plan to increase encryption of user data' *The Guardian* (14 Mar 2016 accessed 15 Mar 2016) <<https://www.theguardian.com/technology/2016/mar/14/facebook-google-whatsapp-plan-increase-encryption-fbi-apple>>

Yadron, Danny, 'This 26-year-old hacker can make a self-driving car, but can he take on Tesla?' *The Guardian* (6 Apr 2016 accessed 7 Apr 2016) <<https://www.theguardian.com/technology/2016/apr/05/george-hotz-comma-self-driving-car-tesla-elon-musk>>

Yadron, Danny, 'Uber claims US regulators collect too much data on its passengers' *The Guardian* (12 Apr 2016 accessed 12 April 2016) <<https://www.theguardian.com/technology/2016/apr/12/uber-us-regulators-data-passengers-report>>

Yadron, Danny, 'Two years until self-driving cars are on the road – is Elon Musk right?' *The Guardian* (3 Jun 2016 accessed 5 Jun 2016) <https://www.theguardian.com/technology/2016/jun/02/self-driving-car-elon-musk-tech-predictions-tesla-google>

Young, Nora, 'Your Car Can be Held for Ransom', *CBCradio* (22 May 2016 accessed 4 Jun 2017) <<http://www.cbc.ca/radio/spark/321-life-saving-fonts-ransomware-cars-and-more1.3584113/your-car-can-be-held-for-ransom-1.3584114>>

## Z

Zanolli, Lauren, 'Welcome to Privacy Hell, Also Known As The Internet Of Things' *FastCompany* (23 Mar 2015 accessed 6 Apr 2016) < <http://www.fastcompany.com/3044046/tech-forecast/welcome-to-privacy-hell-otherwise-known-as-the-internet-of-things>>

Zetsche, Dieter, 'The Mercedes-Benz F015 Luxury in Motion' (n.d. accessed 6 Jul 2016) <https://www.mercedes-benz.com/en/mercedes-benz/innovation/research-vehicle-f-015-luxury-in-motion/>

Zetter, Kim, 'Hacker Lexicon: What are the Dos and DDOS attacks?' *WIRED* (16 Jan 2016 accessed 22 Oct 2016) <<https://www.wired.com/2016/01/hacker-lexicon-wha-are-dos-and-ddos-attacks/>>

Zhang, Sarah, 'Of course 23andMe's plan has been to Sell your genetic data All along' *Gizmodo* (6 Jan 2015 accessed 15 May 2016) <http://gizmodo.com/of-course-23andmes-business-plan-has-been-to-sell-your-1677810999>

Ziegler, Chris, 'Together, we can mind the hype gap' *The Verge* (19 Feb 2016 accessed 12 Apr 2016) <http://www.theverge.com/2016/2/19/11065044/self-driving-car-technology-hype-gap>

Ziegler, Chris, 'A Google self-driving car caused a crash for the first time' *The VERGE* (29 Feb 2016 accessed 3 Mar 2016) <http://www.theverge.com/2016/2/29/11134344/google-self-driving-car-crash-report>

Ziegler, Chris, Tesla's own Autopilot warnings outlined deadly crash scenario 'THE VERGE' (30 Jun 2016 accessed 2 Jul 2016) <http://www.theverge.com/2016/6/30/12073240/tesla-autopilot-warnings-fatal-crash>

Zion Market Research, 'Smart Home Market (Smart Kitchen, Security & Access Control, Lighting Control, Home Healthcare, HVAC Control and Others): Global Industry Perspective, Comprehensive Analysis and Forecast, 2016-2022' (18 Jan 2017 accessed 2 Mar 2017) <https://www.zionmarketresearch.com/report/smart-home-market>

# Table of Cases

## Australia

### Victorian Civil & Administrative Tribunal (VCAT)

*Aboud v Krystal Limousines Pty Ltd (Civil Claims) [2017] VCAT 459 (3 April 2017)*  
*Barrett v Australian National Car Parks Pty Ltd & Others (Civil Claims) [2015] VCAT 1876 (20 November 2015)*  
*Dharmawardena v Advanced Hair Studio (Civil Claims) [2016] VCAT 1036 (6 July 2016)*  
*Mastos v Advanced Hair Studio (Civil Claims) [2016] VCAT 57 (12 January 2016)*

### Commonwealth & state courts

*Amlink Technologies Pty Ltd and the Australian Trade Commission (2005) AATA 359*  
*ASX Operations Pty Ltd v Pont Data Australia Pty Ltd (No 1) (1990) 27 FCR 460*  
*Attorney General (NSW) v World Best Holdings Ltd [2005] 63 NSWLR 557 (per Spiegelman, J)*  
*Australian Broadcasting Commission v Lenah Game Meats Pty Ltd (2001) 208 CLR 199*  
*Australian Competition and Consumer Commission v. Apple Pty Ltd [2017] FCA 416 (21 April 2017)*  
*Australian Competition and Consumer Commission v. Audi Aktiengesellschaft & Ors Case No NSD 322/2017M NSW Registry, Federal Court of Australia (8 Mar 2017)*  
*Australian Competition and Consumer Commission v. BMW Australia Limited [2003] FCA 727, (2003) ATPR 41-944*  
*Australian Competition and Consumer Commission v. Bunav.it Pty Ltd [2016] FCA 6*  
*Australian Competition and Consumer Commission v. Chrisco Hampers Australia Ltd [2015] FCA 1204 (10 November 2015)*  
*Australian Competition and Consumer Commission v. Coles Supermarkets Australia Pty Ltd [2014] FCA 1405*  
*Australian Competition and Consumer Commission v. Coles Supermarkets Australia Pty Ltd [2014] FCA 1405*  
*Australian Competition and Consumer Commission v. Coles Supermarkets Australia Pty Limited [2015] FCA 330*  
*Australian Competition and Consumer Commission v. Fisher & Paykel Customer Services Pty Ltd [2014] FCA 1393*  
*Australian Competition and Consumer Commission v. Get Qualified Australia Pty Ltd [2016] FCA 976*  
*Australian Competition and Consumer Commission v. Hewlett-Packard Australia Pty Ltd [2013] FCA 653*  
*Australian Competition and Consumer Commission v. Homeopathy Plus! Australia Pty Limited [2014] FCA 1412*  
*Australian Competition and Consumer Commission v. Jetstar Airways Pty Limited (No 2) [2017] FCA 205*  
*Australian Competition and Consumer Commission v. Jones (No 5) [2011] FCA 49*  
*Australian Competition and Consumer Commission v. Jutsen (No 3) (2011) 206 FCR 264 at 287*  
*Australian Competition and Consumer Commission v. Reckitt Benckiser (Australia) Pty Ltd (No 4) [2015] FCA 1408*  
*Australian Competition and Consumer Commission v. Seal-a-Fridge Pty Ltd [2010] FCA 525*  
*Australian Competition and Consumer Commission v. TPG Internet Pty Limited [2013] HCA 54; (2013) 250 CLR640*  
*Australian Competition and Consumer Commission v. Valve Corporation [2015] FCA 721*  
*Australian Competition and Consumer Commission v. Valve Corporation (No. 3) [2016] FCA 196*

Australian Competition and Consumer Commission v. Virgin Australia Airlines Pty Ltd (No 2) [2017] FCA 204.  
*Australian Competition and Consumer Commission v Woolworths Ltd* 2016 FCA 18  
*BMW Australia Limited v Australian Competition & Consumer Commission* [2004] FCAFC 167; 207 ALR 452  
*Bunnings v Laminex* [2006] FCA 682  
*Campomar Sociedad Limitada v Nike International Ltd* [2000] HCA 12 (2000) CLR 45  
*Carey-Hazell v Getz Bros and Co (Aust) Pty Ltd* [2004] FCA 853; [2004] ATPR 42-014  
*Carpet Call v Chan* (1987) ASC 55- 553 (1987) ATPR (Digest) 46-025  
*Centrebet Pty Ltd v Baasland* [2013] NTSC 59 9re when CT in force)  
*Crawford v Mayne Nickless Ltd* (1992) ASC 56-144; (1992) ATPR(digest) 46-091  
*DAB v. Byron Shire Council* [2017] NSW CATAD 104.  
*Desktop Marketing Systems Pty Ltd v Telstra Corporation Limited* [2002] FCAFC 112  
*Director of Consumer Affairs Victoria v The Good Guys Discount Warehouses (Australia) Pty Ltd* [2016] FCA 22  
*Director of Consumer Affairs (Vic) v Scully (No 3)* [20-13] VSCA 292  
*DPN Solutions Pty Ltd v Tridant Pty Ltd* [2014] VSC 511  
*Ebay International AG v Creative Festival Entertainment Pty Ltd* (2006) 170 FCR 450  
*Four Square Stores (Qld) Ltd v ABE Copiers Pty Ltd* [1981] ATPR 40-232  
*Gammasonics Institute for Medical Research Pty Ltd v Comrad Medical Systems Pty Ltd* [2010] NSWSC 267  
*Google Inc. v ACCC* (2013) 249 CLR 435; [2013] HCA 1  
*Graham Barclay Oysters Pty Ltd v Ryan* [2000] FCA 853,  
*Hearne v Street* (2008) 235 CLR 125 at 154-162; [2008] HCA 36)  
*Kakavas v Crown Melbourne Limited* [2013] 250 CLR 392.  
*Jetstar Airways Pty Ltd v Free* [2008] VSC 539  
*Laminex (Aust) v Coe Manufacturing Co* [1999] NSWCA 270  
*Lowery v Insurance Australia Ltd* [2015] NSWCA 303  
*McConnell Dowell Constructors (Aust) Pty Ltd v Santam Ltd & Ors (No 1)* [2016] VSC 723  
*McDermott v Robinson Helicopter Company* [2014] QSC 34.  
*Matthews v AusNet Electricity Services Pty Ltd* [2014] VSC 663  
*Merck Sharpe and Dohme (Australia) Pty Ltd v Petersen* [2011] FCAFC 128; (2011) 196 FCR 145  
*Nine Network Pty Limited v IceTV Pty Limited* [2009] HCA 14.  
*Oster & Houli* [2015] FCCA 398 (25 February 2015)  
*Paciocco v Australia and New Zealand Banking Group Limited* [2015] FCAFC 50 [363] – [364],  
*Parkdale Custom Built Furniture Pty Ltd v Puxu Pty Ltd* [1982] HCA 44.  
*Perpetual Trustee Company v Burniston (No 2)* [2012] WASC 383.  
*Privacy Commissioner v Telstra Corporation Ltd*, No VID 38/2-16  
*Rana v Australian Human Rights Commission* [2014] FCA 1902,  
*Ransley v Black & Decker (A'asia) Pty Ltd* (1977) TPR 138  
*Rowe v Emmanuel College* [2013] FCCA 231  
*Seafolly Pty Ltd v Madden* (2012) 297 ALR 337  
*Smythe v Thomas* (2007) 71 NSWLR 537 [ re when online CT comes into effect)  
*Taco Co of Australia Inc. v Taco Bell Pty Ltd* (1982) 42 ALP 177; [1982] FCA 170 [199].  
*Telstra Corporation Limited & Anor v Phone Directories Company Pty Ltd & Ors* [2010] FCA 44  
*Telstra Corporation Limited v Privacy Commissioner, Decision* [2015] AATA 991 (18 Dec 2015)  
*Vautin v BY Winddown Inc (No 2)* [2016] FCA 1235  
*Video-Ezy International Pty Ltd v Sedema Pty Ltd* [2014] NSWSC 143

## **OAIC Determinations & enforceable undertakings**

'CP' and Department of Defence [2014] AICmr 88 (2 September 2014)  
'DO' and Department of Veterans' Affairs [2014] AICmr 124 (13 November 2014)  
'EQ' and Great Barrier Reef Marine Park Authority [2015] AICmr 11 (2 February 2015)  
Grubb v Telstra Corporation Limited [2015] AICmr 35  
'IY' and Business Services Brokers Pty Ltd t/a TeleChoice [2016] AICmr 44 (30 June 2016)  
'IX' and Business Services Brokers Pty Ltd t/a TeleChoice [2016] AICmr 42 (30 June 2016)  
'IR' and NRMA Insurance, Insurance Australia Limited [2016] AICmr 37 (27 June 2016)  
'JO' and Comcare [2016] AICmr 64 (21 September 2016)

Enforceable Undertaking Under s 33E of the Privacy Act 1988 (Cth), to the Australian Information Commissioner - Avid Life Media Inc. (ALM) (trading as Ruby Corp.) 21 Aug 2015 (the Ashley Madison case)

## **European Union & United Kingdom**

*Patrick Breyer v. Bundesrepublik Deutschland*, Case C-582/14, 19 October 2016  
*Director General of Fair Trading v First National Bank PLC* [2001] UKHL 52; [2002] 1 AC 481  
*Google Inc. v Judith Vidal-Hall and others* [2015] EWCA Civ 311  
*Kásler and Káslerné Rábai/OTP Jelzálogbank Zrt*, CJEU 30 April 2014, case C-26/13, ECLI:EU:C:2014:282 points 73–74  
*McFadden v Sony Music Entertainment Germany GmbH* (C-484/14), Preliminary Opinion, Advocate General of the CJEU  
*Mylcrist Builders Ltd v Buck* [2008] App L. Rev 09/19  
*Office of Fair Trading v Abbey National plc* [2010] 1 All ER 667  
*Schrems v Data Commissioner & Digital Rights Ireland*, Court of Justice of the EU, Case No: C-362/14  
*Vidall-Hall and Ors v Google Inc.* [2014] EWHC QB 13 (QB)

## **United States of America**

*American Civil Liberties Union v Clapper et al*, 785 F 3d. 787 (2<sup>nd</sup> Cir. 2015)  
*Archer-Hayes & Ors v. ToyTalk Inc, Mattel Inc., & Ors, Class Acton Complaint*, Case No. BC 603467 Superior Court of California (Filed 7 Dec 2015)  
*Attorney General of the State of New York, In the Matter of Cardio, Inc.*, Assurance No.: 16-173, Assurance of Discontinuance under Executive Law Section 63, Subdivision 15 (23 Jan 2017) <[https://ag.ny.gov/sites/default/files/cardio\\_aod\\_executed.pdf](https://ag.ny.gov/sites/default/files/cardio_aod_executed.pdf)>  
*Attorney General of the State of New York, In the Matter of Runtastic GmbH*, Assurance No.: 16-174, Assurance of Discontinuance under executive Law Section 63, Subdivision 15 (23 Jan 2017) <[https://ag.ny.gov/sites/default/files/runtastic\\_aod\\_executed\\_0.pdf](https://ag.ny.gov/sites/default/files/runtastic_aod_executed_0.pdf)>  
*Attorney General of the State of New York, In the Matter of Matis Ltd*, Assurance No.: 16-101, Assurance of Discontinuance under executive Law Section 63, Subdivision 15 (13 Feb 2017) <[https://ag.ny.gov/sites/default/files/matis\\_aod\\_executed.pdf](https://ag.ny.gov/sites/default/files/matis_aod_executed.pdf)>  
*Baker v. The ADT Corporation and ADT, LLC d/b/a ADT Security Services*, Case No. 15-cv-02038-CSB-DGB (U.S.D.C. C.D. Illinois)  
*Brickman v Fitbit Inc.*, Class Action Case No. 3:15-cv-2077 (Filed 8 May 2015)  
*Cahen, et al. v. Toyota Motor Corporation, et al.*, U.S. District Court of Northern California, San Francisco Division, Civil Action No. 4:2015cv01104

<<https://dlbjbjzgnk95t.cloudfront.net/0731000/731922/https-ecf-cand-uscourts-gov-doc1-035113610903.pdf>>

*Cheatham & Ors. v. ADT CORP.*, No. CV-15-02137-PHX-DGC, 161 F.Supp.3d 815 (2016)

*DeJohn v The TV Corp International* 245 F Supp 2d 913 (ND Ill 2003),

*Edenborough & Ors., v. ADT, LLC d/b/a ADT Security Services, Inc*, United States District Court, N.D. California (Filed Feb 27, 2017)

*Federal Trade Commission v. Breathometer, Inc., & Ors*, FTC Matter/File Number: 162 3057, Federal Court: Northern District of California, Case No. 3:17-Cv-314-Lb, Stipulated Final Order, Filed 23 Jan 2017 <[https://www.ftc.gov/System/Files/Documents/Cases/170123breathometer\\_Dkt.\\_4-1\\_-\\_Stipulated\\_Order.Pdf](https://www.ftc.gov/System/Files/Documents/Cases/170123breathometer_Dkt._4-1_-_Stipulated_Order.Pdf)>

*Federal Trade Commission v D-Link Corporation and D-Link Systems, Inc.*, Case No: 3:17-cv-00039 filed 5 Jan 2017; United States District Court of California

<[https://www.ftc.gov/system/files/documents/cases/170105\\_d-link\\_complaint\\_and\\_exhibits.pdf](https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf)>

*Federal Trade Commission v. Sitemsearch Corporation, dba LeapLab*, (United States District Court for the District of Arizona, Phoenix Division) FTC Matter/ File No: 142 3192 (23 Dec 2014)

<<https://www.ftc.gov/system/files/documents/cases/141223leaplabcmt.pdf>>

*Federal Trade Commission v. Sequoia One LLC & Ors*, Case No. 2:15-cv-01512, US District Court of Nevada (7 August 2015)

*Federal Trade Commission v. Wyndham Worldwide Corp, et al.*, No. 14-3514, (3rd Cir. Aug. 24, 2015)

*Federal Trade Commission v. Wyndham Worldwide Corp, et al.*, 10 F.Supp.3d 602 (D.N.J. 2014) (No. 2:13-CV-01887-ES-JAD).

*Federal Trade Commission & Ors., v. Vizio Inc. & Ors.*, Case 2:17-cv-00758 (6 Feb 2017)

<<https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc>>

'Complaint for Permanent Injunction and Other Equitable and Monetary Relief '[https://www.ftc.gov/system/files/documents/cases/170206\\_vizio\\_2017.02.06\\_complaint.pdf](https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf)> and

'Stipulated Order for Permanent Injunction and Monetary Judgment'

<[https://www.ftc.gov/system/files/documents/cases/170206\\_vizio\\_stipulated\\_proposed\\_order.pdf](https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf)>

'Concurring Statement of Acting Chairman Maureen K. Ohlhausen In the Matter of Vizio, Inc.'

<[https://www.ftc.gov/system/files/documents/public\\_statements/1070773/vizio\\_concurring\\_statement\\_of\\_chairman\\_ohlhausen\\_2-6-17.pdf](https://www.ftc.gov/system/files/documents/public_statements/1070773/vizio_concurring_statement_of_chairman_ohlhausen_2-6-17.pdf)>

*Federal Trade Commission v. Wyndham Worldwide Corp. et al.*, Civil No. 13-1887 (Dist. Court New Jersey, 7 Apr 2014) <<http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation> [Dist Ct].

*Federal Trade Commission v. Wyndham Worldwide Corporation, Wyndham Hotel Group Llc, Wyndham Hotels and Resorts Llc and Wyndham Hotel Management Incorporated*, United States Court Of Appeals For The 3rd Circuit, Case No. 14-3514 (Filed 24 Aug 2015)

<<https://www.ftc.gov/system/files/documents/cases/151209wyndhamstipulated.pdf>>

*Flynn, Brown et al v. FCA US Llc F/K/A Chrysler Group LLC and Harmon International Industries, Inc*, US Dist Court Sthern Dist Illinois, Case No. 3:15-cv-855, Class Action Complaint

<[https://www.law360.com/dockets/download/55c103f7a36d4660ce000028?doc\\_url=https%3A%2F%2Fecf.ilsd.uscourts.gov%2Fdoc1%2F06913233689&label=Case+Filing](https://www.law360.com/dockets/download/55c103f7a36d4660ce000028?doc_url=https%3A%2F%2Fecf.ilsd.uscourts.gov%2Fdoc1%2F06913233689&label=Case+Filing)>

*Forrest v Verizon Communications Inc* 805 A2d 1007 (DC 2002)

*In the Matter of ASUSTek*, File No. 142 3456, Agreement containing Consent Order (26 Feb 2016)

<https://www.ftc.gov/system/files/documents/cases/160222asusagree.pdf>

*In the Matter of Epic Marketplace Inc. and Epic Media Group LLC*. Docket No. C4389, US Federal Trade Commission, Complaint 13 March 2013

<<http://www.ftc.gov/sites/default/files/documents/cases/2013/03/130315epicmarketplacecmpt.pdf>>

*In the Matter of TRENDnet Inc.*, No. C-4426, 2014 WL 556262 (F.T.C. Jan. 16, 2014) (consent order)

<<http://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf>>

*TRENDNet, Inc.*, No. C-4426 (F.T.C. Feb. 7, 2014), at ¶ 8 (complaint), available at

<http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf>; Case No. C-4482 (F.T.C. Aug.14, 2014) (consent order), available at <http://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf>; HTC America, Inc., C-4406 (F.T.C. June 25, 2013) (decision and order), available at <http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf>.  
In the Matter of Oracle Corporation Docket No. C-4571 File No 132 3115  
'Complaint' <https://www.ftc.gov/system/files/documents/cases/151221oracleorder.pdf> 'Decision and Order' <<https://www.ftc.gov/system/files/documents/cases/160329oracledo.pdf>>  
In re Ashley Madison Customer data security breach, Case No 4:15-md-02669 (filed 9 Dec 2015)  
In Re Facebook Biometric Information Privacy Litigation, US District Court, Northern District of California, Order re Motion to Dismiss and Summary Judgment, Case No. 15-cv-03747-JD <<https://cdn.arstechnica.net/wp-content/uploads/2016/05/Biometric-Ruling.pdf>>  
In Re Order requiring Apple, Inc. to assist in the execution of a search warrant issued by the court, Memorandum and Order, James Orenstein, Magistrate Judge, U.S. District Court, Eastern District of New York (Brooklyn), 1:15-mc-1902 (JO), February 29, 2016  
In Re Target Corp. Data Sec. Breach Litigation, No. 14-2522, 2014 WL 7192478, (18 Dec 2014).  
In Re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp. Microsoft Corp. v. United States, No. 14-2985, 2016 U.S. App. LEXIS 12926 (2d Cir. 2016),  
In the Matter of ScanScout Inc., No. C-4344 (F.T.C. Matter/ File No. 102 3185 (21 Dec 2011) <<https://www.ftc.gov/enforcement/cases-proceedings/102-3185/scanscout-inc-matter>>  
LabMD, Inc. v. The Federal Trade Commission, Petition for review of a decision of the FTC, Case No 16-16270-D, US Court of Appeals for the Eleventh Circuit, (10 Nov 2016) <<http://www.thompsoncoburn.com/docs/default-source/default-document-library/labmddecision8d702626dda26f05acb8ff0000ba5cc9.pdf?sfvrsn=0>>  
Loomis v. Wisconsin, Docket No. 16-6387, (13 July 2016)  
Meyer v. Kalanick, No. 15 Civ. 9796, 2016 WL 4073012 (S.D.N.Y. July 29, 2016).  
McLellan et al., v Fitbit, Inc., Case No. 3:16-cv-00036, US Dist Ct Nthern Dist Calif (5 Jan 2016)  
Complaint < <https://www.documentcloud.org/documents/2675603-1-Main.html>>  
N.P. & Ors v Standard Innovation (US) Corp dba We-Vibe, Case No 1:16-cv-8655, United States District Court of Illinois (Filed 2 Sept 2016) <<https://www.cnet.com/news/internet-connected-vibrator-we-vibe-lawsuit-privacy-data/>>  
Re Zapos.com, Inc 3:12-cv-00325-RCJ-VPC (2012)  
Sgouros v TransUnion Corporation No 15-2015  
Sheikh, Kelner and Milone & Ors v. Tesla, Inc dba Tesla Motors Inc, United States District Court Northern District of California, Case No 5:17- cv -02193 (Filed 19 Apr 2017) Specht v Netscape Communications Corp 2001 WL 755396  
State of Wisconsin v. Eric L. Loomis, Case No.: 2015AP157-CR, Sup Court of Wisconsin < <https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690>>  
United States v. Gen. Motors Corp., 518 F.2d 420, 427 (D.C. Cir. 1975)  
United States of America v Path, Inc. FTC Matter/ File No. 122 3158 (1 Feb 2013) <<https://www.ftc.gov/enforcement/casesproceedings/122-3158/path-inc>>  
USA v Volkswagen AG, Audi AG et al Civil Action, United States District Court for the Eastern District of Michigan, Case No. 2:16-cv-10006 (Filed 01/04/16) <https://www.justice.gov/opa/file/809826/download>  
In re Volkswagen "Clean Diesel" Marketing, Sales Practices, and Products Liability Litigation, Case No. 3:15-md-2672 (N.D. Cal.),  
U.S. v. Volkswagen, 16-CR-20394, Volkswagen Diesel Engine Vehicle Matters, Case No. 2:16-cr-20394-SFC-APP (E.D. Mich.) <<https://www.justice.gov/usao-edmi/us-v-volkswagen-16-cr-20394>>

*Valdez-Marquez, Sinopli, Navarro et al v Netflix, Inc. U.S. District Court for the Northern District of California, San Jose Division, Civil Action No. c09 05903*  
<http://privacylaw.proskauer.com/uploads/file/doe-v-netflix.pdf> (Filed 17 Dec 2009)  
*Zak et al v. Bose Corp., Class Action Complaint, Case No. 17-cv-2928 (Filed 18 Apr 2017) Northern District of Illinois* < <https://assets.documentcloud.org/documents/3673948/Zak-v-Bose.pdf>>

### **Electronic Privacy Information Center (EPIC) Complaint & Amicus Filings**

EPIC, Alleruzzo, et al., v. SuperValu, Inc., et al., Brief of Amicus Curiae Electronic Privacy Information Center in Support of Plaintiffs-Appellants/Cross-Appellees, Case Nos. 16-2378 and 16-2528  
<<https://epic.org/amicus/data-breach/supervalu/EPIC-Amicus-SuperValu.pdf>>

EPIC v. Customs and Border Protection (Analytical Framework for Intelligence) Complaint (Filed 18 Jul 2014) Civil Action No. 14-1217 US District Court for the District of Columbia  
<<https://epic.org/foia/dhs/cbp/afi/>>

EPIC, 'In the Matter of Samsung Electronics Co. Ltd., 'Compliant, Request for investigation, Injunction, and other relief to the Federal Trade Commission' (24 Feb 2015)  
<<https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf>>; Motion to Dismiss The Amended Class Action Complaint, United States District Court for the Southern District of Illinois, Case No. 3:15-Cv-855 (Filed 19 Feb 2016) <<http://www.Liabilitydesk.Com/Wp-Content/Uploads/2016/02/15-Cv-00855-Mjr-Dgw-Document-71-1.Pdf>>

EPIC, 'In the Matter of Genesis Toys and Nuance Communications, 'Complaint and Request for Investigation, injunction, and other relief', Submitted by The Electronic Privacy Information Center, The Campaign for a Commercial Free Childhood, The Center for Digital Democracy and the Consumers Union (6 Dec 2016 accessed 12 Dec 2016) <https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf>

## **Table of Legislation**

### **Australia**

#### **Bills**

Privacy Amendment (Re-identification Offence) Bill 2016

#### **Regulations**

Competition and Consumer Regulations 2010 (Cth).

#### **Commonwealth**

Administrative Decisions (Judicial Review) Act 1977 (Cth)

Administrative Appeals Tribunal Act 1975 (Cth)

Age Discrimination Act 2004 (Cth)

Australian Consumer Law

Australian Information Commissioner Act 2010 (Cth)

Australian Securities and Investments Commission Act 2001 (the ASIC Act)

Competition and Consumer Act 2010 (Cth)

Copyright Act 1968 (Cth)

Corporations Act 2001 (Cth)

Crimes Act 1914 (Cth)

Criminal Code Act 1995 (Cth)

Cybercrime Act 2001 (Cth)

Cybercrime Legislation Amendment Act 2012 (Cth)

Data-matching Program (Assistance and Tax) Act 1990 (Cth)

Disability Discrimination Act 1992 (Cth)

Do Not Call Register Act 2006 (Cth)

Electronic Transactions Act 1999 (Cth)

Electronic Transactions Act 1999 (Cth)

Electronic Transactions (Queensland) Act 2001 (Qld)

Federal Court of Australia Act 1976 (Cth)

Healthcare Identifiers Act 2010 (Cth)

Insurance Contracts Act 1984 (Cth)

National Consumer Credit Protection Act 2009 (Cth).

National Health Act 1953 (Cth)

Personally Controlled Electronic Health Records Act 2012 (Cth)

Personal Property Securities Act 2009 (Cth)

Privacy Act 1988 (Cth)

Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)

Racial Discrimination Act 1975 (Cth)

Sex Discrimination Act 1984 (Cth)

Spam Act 2003 (Cth)

Surveillance Devices Act 2004 (Cth)

Telecommunications Act 1997 (Cth)

Telecommunications (Consumer Protection and Services Standards) Act 1999 (Cth)

Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth)

Telecommunications (Interception and Access) Act 1979 (Cth)

Treasury Legislation Amendment (Small Business and Unfair Contract Terms) Act 2015 (Cth)

Current Commonwealth legislation is found in the Federal Register of Legislation  
<<https://www.legislation.gov.au/>>

### **State**

Anti-Discrimination Act 1977 (NSW)  
Anti-Discrimination Act 1996 (NT)  
Anti-Discrimination Act 1991 (Qld)  
Anti-Discrimination Act 1998 (Tas)  
Discrimination Act 1991 (ACT)  
Equal Opportunity Act 1984 (SA)  
Equal Opportunity Act 2010 (Vic)  
Equal Opportunity Act 1984 (WA)  
Electronic Transactions Act 2001 (ACT)  
Electronic Transactions Act 2000 (NSW)  
Electronic Transactions Act 2000 (SA)  
Electronic Transactions Act 2000 (Tas)  
Electronic Transactions (Victoria) Act 2000 (Vic)  
Electronic Transactions (Northern Territory) Act 2000 (NT)  
Electronic Transactions Act 2003 (WA). Electronic Transactions (Queensland) Act (Qld)  
Fair Trading Act 1989 (Qld)  
Information Privacy Act 2014 (ACT)  
Information Privacy Act 2009 (Qld)  
Criminal Code Act 1899 (Qld)  
Motor Vehicles (Trials of Automotive Technologies) Amendment Act 2016 (SA)  
Public Records Act 2002 (Qld)  
Telecommunications Interception Act 2009 (Qld)

### **New Zealand**

Fair Trading Act 1986 (NZ)

### **United Kingdom & European Union**

Consumer Rights Act 2015 (UK)  
Data Protection Act 1998 (UK)

European Council Data Protection Directive 95/46 EC (to be replaced by GDPR in 2018)  
European Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ 1993, L 095/29.  
EU General Data Protection Regulation (GDPR) 2016/679 (27 Apr 2016)  
EU General Product Safety Directive (GPSD) 2001/95/EC (3 Dec 2001)

### **United States**

Children's Online Privacy Protection Act, 15 USC § 6501 (COPPA)  
Federal Trade Commission Act, 15 U.S.C.

Federal bills:

Autonomous Vehicle Privacy Protection Act of 2015 (HR3876) [Federal bill]  
<<https://www.congress.gov/114/bills/hr3876/BILLS-114hr3876ih.pdf>>

[Defunct] Consumer Privacy Bill of Rights Act of 2015,  
<<https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf>>

Developing Innovation and Growing the Internet of Things (DIGIT) Act,  
<[http://www.fischer.senate.gov/public/\\_cache/files/03de7771-088b-45ac-8552-f82ddc0aa480/digit-2016---final-bill-for-filing.pdf](http://www.fischer.senate.gov/public/_cache/files/03de7771-088b-45ac-8552-f82ddc0aa480/digit-2016---final-bill-for-filing.pdf)>

*State consumer protection legislation example: California\**

Senate Bill 327 (Calif.) ('Teddy Bear & Toaster Act')

Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code  
Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code  
False Advertising Law ("FAL"), Cal. Bus. Prof. Code  
Implied Warranty of Merchantability, Cal. Com. Code  
Song-Beverly Consumer Warranty Act, Cal. Civ. Code

\* Example statutes drawn from California as pleaded in the *Cohen* smart car litigation. Note US state approaches vary, but some have equivalent forms of legislation.

## Schedule 1: ACL unfair terms review

### S1.1 Smart home<sup>1910</sup>

Smart home: potentially applicable device terms <sup>1911</sup>		
GOOGLE 'NEST' <sup>1912</sup>	AMAZON 'ALEXA'	SAMSUNG SMART THINGS HUB 2
<b>UK Terms of Service</b> <sup>1913*</sup> <b>EULA (software) *</b> <b>Terms of Sale*</b> <b>Limited Warranty*</b> <b>Privacy Statement for Nest products*</b> <b>Website Privacy Policy*</b> <b>Privacy Policy for Nest Web Sites</b> <b>Open Source Compliance</b> <b>Sales Terms</b> <b>Intellectual Property and Other Notices</b> <b>Community Forum Agreement</b> <b>FCC Compliance Notice</b> <b>Customer Agreements for Rush Hour Rewards</b> <b>Customer Agreements for Rebates &amp; Safety rewards</b>	Alexa Terms of Use <sup>*1914</sup> Amazon.com Conditions of Use & Sale <sup>*1915</sup> Amazon Device Terms of Use <sup>*1916</sup> Amazon.co.uk Privacy Notice* Amazon.co.uk Conditions of Use (EULA)* PLUS "other applicable rules, policies, and terms posted on the Amazon.co.uk website, available through your Amazon Alexa App, or provided with Alexa Enabled Products" including: <ul style="list-style-type: none"> <li>• Cookies &amp; Internet Advertising*</li> <li>• Amazon Prime Terms and Conditions*</li> <li>• Amazon Music Terms of Use*</li> <li>• Kindle Terms of Use*</li> <li>• Audible Conditions of Use<sup>*1917</sup></li> </ul>	Samsung SmartThings Terms of Use <sup>1918*</sup> Samsung Service Terms and Conditions <sup>1919*</sup> EULA* Privacy Policy* Copyright Dispute Policy* Security policy* LiveTrack EULA* Livetrack Privacy policy" Copyright*

Table S1.1 Smart home: potentially applicable device terms

**Important Reader Note: All comments on these terms are illustrative only and do not imply contravention of the ACL. Terms cited are included for discussion purposes and are not necessarily or impliedly in breach of the provisions against which they are tabulated. Versions used are best available but may not apply to the Australian market. Not all products cited are yet sold in Australia. Terms quoted are copyright their respective owners.**

<sup>1910</sup> Devices reviewed feature regularly on the Amazon.com 'best sellers' list, but are otherwise selected randomly.

<sup>1911</sup> As discerned from web searches and following links within terms. It is difficult to conclude that these are the complete set however. Those asterisked above are expressly incorporated into the 'contract'.

<sup>1912</sup> All appear here (UK): <https://nest.com/uk/legal/privacy-policy-for-nest-web-sites/?from-chooser=true>

<sup>1913</sup> TOS <https://nest.com/uk/legal/terms-of-service/> (10 Mar 2016); Privacy <https://nest.com/uk/legal/privacy-policy-for-nest-web-sites/>; EULA <https://nest.com/legal/eula/> (10 May 2016).

<sup>1914</sup> <https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201809740>

<sup>1915</sup> <https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=1040616>

<sup>1916</sup> <https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=202002080>

<sup>1917</sup> Persons who "use or access" Alexa "agree" to 8 sets of terms plus those who "purchase or register an Amazon device" agree to the Device terms of Use (making 9 all up).

<sup>1918</sup> Samsung, 'SmartThings Terms' (3 Sept 2015) <https://www.smarthings.com/uk/terms> and Privacy (3 Sept 2015) <https://www.smarthings.com/uk/privacy> UK terms are used.

<sup>1919</sup> Samsung, 'Samsung Service Terms and Conditions' <https://account.samsung.com/membership/terms>

**Smart home: selective terms review**

<b>ACL SECTION 25</b> Examples of terms that are likely to be unfair include terms which:	<b>GOOGLE 'NEST'<sup>1920</sup></b>  UK Terms of Service EULA (software)	<b>AMAZON 'ALEXA'<sup>1921</sup></b>  Alexa Terms of Use [TOU] Amazon.com Conditions of Use & Sale [COU] Amazon Device Terms of Use [DTOU]	<b>SAMSUNG SMART THINGS HUB 2<sup>1922</sup></b>  Samsung SmartThings Terms of Use
a) allow only one party to <b>avoid or limit the performance</b> of the contract;		<p>[TOU] 3.2 <b>Functionality; Content.</b> We do not guarantee that Alexa or its functionality or content ... is accurate, reliable, or complete.</p> <p><b>Comment: this clause may mislead consumers as to their rights under the ACL consumer guarantees s 54 acceptable quality and s 55 fit for purpose which are non-excludable: s64. It may also be unfair if for example, marketing and sales techniques represent that product accuracy.</b></p>	<p><b>Preamble: Will these terms ever change?</b>                      We reserve the right to change the Terms at any time...</p> <p><b>Comment: changing terms entitles them to avoid or limit contract performance. There is no equivalent right to the consumer. This clause enables a potential unfair term breach, depending upon the facts as to the nature of the change.</b></p>
b) allow only one party to <b>terminate</b> the contract;	<p><b>1(d) Term and Termination.</b> At any time, Nest may (i) suspend or terminate your rights to access or use the Services, or (ii) terminate these Terms with respect to you if Nest in good faith believes that you have used the Services in violation of these Terms...</p> <p><b>Comment: broad unilateral termination right dependent upon Nest good faith "belief" whether that belief is fair or accurate. Right has low threshold- there are many violations which may be trivial and do not justify termination. No mandated accountability as to 'belief'.</b></p>		<p>SmartThings is also free to terminate (or suspend access to) your use of the Services or your account, for any reason in our discretion...</p> <p><b>Comment: Mutual termination rights exist (elsewhere), but Samsung's unilateral right to determine breach without notice or appeal may be unfair.</b></p>
c) penalise only one party <b>for breach or</b>	<p><b>Preamble: IF YOU DO NOT AGREE WITH ANY OF THE PROVISIONS OF THESE TERMS, YOU</b></p>	<p>[AU] 3.5 [DU d.] <b>Termination.</b> Your rights under this Agreement will automatically terminate without notice if</p>	<p><b>Will these Terms ever change?</b></p>

<sup>1920</sup> The Nest website lists 15 legal 'documents', including those reviewed. Terms cover: Learning Thermostat™, Protect: Smoke + Carbon Monoxide™ Alarm, Cam™, Dropcam™, Works with Nest™, MyEnergy™, and 'other products'.

<sup>1921</sup> Alexa has 9 sets of potentially-relevant terms covering Amazon's Alexa voice services, which "includes Third Party Services, digital content, Software, the Amazon Alexa App, and support and other related services." The UK terms were reviewed: <<https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201566380>>

<sup>1922</sup> Samsung has 9 sets of potentially-relevant terms.

<p>termination of the contract;</p>	<p>SHOULD ... CEASE ACCESSING OR USING THE SERVICES...</p> <p><b>2(b) (b) Automatic Software Updates....</b> You consent to this automatic update. If you do not want such Updates, your remedy is to terminate your Account and stop using the Services and the Product</p> <p><b>Comment: limited remedy without refund may 'penalise' consumer for termination of the contract, so operates as a disincentive to termination. Note however that product updates- especially as to home hubs – are an important security requirement so in the public interest.</b></p>	<p>you fail to comply with any of its terms... Amazon may immediately revoke your access to Alexa without refund of any fees...</p> <p><b>Comment: there is no criteria to determine 'failure', no limit to important terms only nor any requirement that a consumer be notified. There is no equivalent penalty (refund of fees) should Amazon breach terms. Also, no reference to a consumer retrieving their (personally valuable) data which may be lost if the Service is immediately revoked, which denies portability.</b></p>	<p>If you don't agree with the new Terms, you are free to reject them; unfortunately, that means you will no longer be able to use the Services.</p> <p><b>Comment: No overt termination penalty (in the technical sense) but <i>practically</i> penalises consumers if their device (or home system) is useless without services, so they lack bargaining power to reject. No direct court authority on that question; but e.g. traditional approaches may include where the consumer must pay a sum, regardless of who terminates.</b></p>
<p>d) allow only one party to <b>vary</b> the contract;</p>	<p><b>13 (a) Changes to these Terms.</b> Nest reserves the right to make changes to these Terms. We'll post notice of modifications to these Terms on this page. You should ensure that you have read and agree with our most recent Terms when you use the Services. Continued use of the Services following notice of such changes shall indicate your acknowledgment of such changes and agreement to be bound by the revised Terms.</p> <p><b>Comment: unilateral variation rights plus low level notice to consumers. It is arguably unfair to expect consumers to check the website for changes and imposes a grey area as to which terms apply where consumers reasonably have not yet 'seen' a notice online.</b></p>	<p><b>[TOU] 3.3 Changes to Alexa; Amendments.</b> We may change, suspend, or discontinue Alexa, or any part of it, at any time. We may amend any of this Agreement's terms at our sole discretion by posting the revised terms on the Amazon.co.uk website. You will be subject to the terms of this Agreement in force at the time you use Alexa.</p> <p><b>[DTOU] General c. Changes to Services; Amendments.</b> [as above except 'the Services' in lieu of Alexa]</p> <p><b>Comment: unilateral variation rights plus low level notice to consumers. It is arguably unfair to expect consumers to check the website for changes and imposes a grey area as to which terms apply where consumers reasonably have not yet 'seen' a notice online.</b></p> <p><b>[CU] 15. [COS 9] ALTERATIONS TO SERVICE OR AMENDMENTS TO THE CONDITIONS OF USE</b> We reserve the right to make changes to any Amazon Services, policies, terms and conditions ... at any time. You will be subject to the terms and conditions, policies</p>	<p><b>Will these Terms ever change? ...</b>We reserve the right to change the Terms at any time, but if we do, we will bring it to your attention by placing a notice on the Services and/or by sending you an email...</p> <p>If you don't agree with the new Terms, you are free to reject them; unfortunately, that means you will no longer be able to use the Services. If you use the Services in any way after a change to the Terms is effective, that means you agree to all of the changes. ... no other amendment or modification .... will be effective unless in writing and signed by both you and us.</p> <p><b>Comment: unilateral variation rights plus low level notice to consumers. Unclear when which form of notice applies. No remedy if consumers reject a change.</b></p> <p><b>Does SmartThings cost anything?...</b> SmartThings reserves the right to change its price list and to institute new charges at any time, upon ten (10) days prior notice to you, ...by email or</p>

		<p>and Conditions of Use in force at the time that you use the Amazon Services...</p> <p><b>Comment: as above. Use does not equate to acceptance if consumers are unaware of a change, so this clause is potentially unfair, especially as it does not prescribe notice or offer remedy where the consumer does not accept the change.</b></p>	<p>posted on the Services. Use of the Services by you following such notification constitutes your acceptance...</p> <p><b>Comment: While the ACL s 24 does not apply to the 'upfront price payable', this clause allows for subsequent new charges or changes on short notice. Use may be an unfair form of acceptance unless notice is very clear. Question where consumers are no longer able to use their devices due to unreasonable "new charges" on little notice – this could be unfair.</b></p>
<p>e) allow only one party to <b>vary</b> the ... characteristics of the goods or services to be supplied ... under the contract;</p>	<p><b>3(i) Modification.</b> Nest reserves the right, at any time, to modify, suspend, or discontinue the Services or any part thereof with or without notice. You agree that Nest will not be liable to you or to any third party...</p> <p><b>Comment: This confers unfettered rights upon Nest and may be unfair insofar as there is no apparent notice requirement or restriction upon their capacity to modify, suspend or discontinue the Services. This may leave consumers with a useless device, or one so changed from that which they purchased as to be a different product. Depending upon the facts, this is likely to be unfair.</b></p>	<p>[CU] As above.</p>	<p>As above.</p>
<p>g) allow only one party to vary the <b>upfront price</b> payable under the contract without the right of the counterparty to terminate the contract;</p>	<p><b>(d) Temporary Suspension.</b> The Services may be suspended temporarily without notice for security reasons, system failure, maintenance and repair, or other circumstances. You agree that you will not be entitled to any refund or rebate for such suspensions. Nest does not offer any specific uptime guarantee for the Services.</p> <p><b>Comment: This may be unfair, particularly as the decision to terminate can only be exercised once the length of suspension is known. Note however, consumers (largely)</b></p>	<p>[CU] as above</p> <p><b>Comment: as above</b></p>	<p><b>Does SmartThings cost anything?...</b></p> <p>SmartThings reserves the right to change its price list and to institute new charges at any time, upon ten (10) days prior notice to you, ...by email or posted on the Services. Use of the Services by you following such notification constitutes your acceptance...</p> <p><b>Comment: While the ACL s 24 does not apply to the 'upfront price payable', this clause allows for subsequent new charges or changes on short notice. Use may be an unfair form of</b></p>

	tolerate internet dropouts, usually without recompense, so query if this clause would be challenged.		acceptance unless notice is very clear. Question where consumers are no longer able to use their devices due to unreasonable “new charges” on little notice – this could be unfair.
h) allow one party to <b>unilaterally determine</b> whether the contract has been breached or to interpret its meaning;		<p><b>[TOU] 3.5 Termination.</b> Your rights under this Agreement will automatically terminate without notice if you fail to comply with any of its terms. In case of such termination, Amazon may immediately revoke your access to Alexa without refund of any fees...</p> <p><b>Comment: as stated above. Also, note there is no criteria to determined failure to comply nor gradation as to serious breach or minor breach, which may be unfair given the punitive consequence.</b></p>	<p><b>What if I want to stop using the Services?...</b> SmartThings has the sole right to decide whether you are in violation of any of the restrictions set forth in these Terms.</p> <p><b>Comment: unilateral determination lacks reasonable criteria and may be exercised in a manner which renders reliance upon this clause unfair.</b></p>
i) limit one party’s <b>vicarious liability</b> for its agents;	<p><b>2(c)</b> Nest is not responsible for your use of any Third Party Product or Service or any personal injury, death, property damage (including, without limitation, to your home), or other harm or losses arising from or relating to your use of any Third Party Products or Services.</p> <p><b>5(d)</b> Nest is not responsible for your use of any Third Party Product or Service or any personal injury, death, property damage (including, without limitation, to your home), interruption of service, downtime, data loss, or other harm or losses arising from or relating to your use of any Third Party Products or Services.</p> <p><b>Comment: third parties are not necessarily agents but the ACL may view them as such where Nest marketing promotes and recommends ‘Works with Nest’ products to create that perception. Then the exclusion may be unfair. Note given the careful legal contracts surrounding the Works programme, it is unlikely such an argument would succeed.</b></p>	<p><b>[TOU] 2.2 Third Party Alexa Enabled Products.</b> Alexa Enabled Products include third party products that Amazon does not manufacture or develop. Amazon has no responsibility or liability for such products.</p> <p><b>Comment: as per Nest.</b></p>	<p>You agree that SmartThings shall not be responsible or liable for any loss or damage of any sort incurred as the result of any such [third party] dealings.</p> <p><b>Indemnity.</b> You agree to indemnify and hold SmartThings, its affiliates, officers, agents, employees, and partners harmless for and against any and all claims, liabilities, damages (actual and consequential), losses and expenses (including attorneys' fees) arising from or in any way related to any third party claims relating to (a) your use of the Services..., and (b) your violation of these Terms...</p> <p><b>Comment: Very broad clause which imposes an indemnity without tying it to consumer fault. No reciprocity or mutual indemnities suggest this clause may be found to be unfair in the right factual circumstances.</b></p>

<p><b>j) allow one party to assign the contract to the counterparty's detriment without the counterparty's consent;</b></p>	<p><b>(f) Assignment.</b> These Terms ... may not be assigned or otherwise transferred by you without Nest's prior written consent. These Terms may be assigned by Nest without restriction.</p> <p><b>Comment: clear potential breach which seems to lack justification and evidence inequality of bargaining power.</b></p>		<p><b>Assignment.</b> You may not assign, delegate or transfer these Terms or your rights or obligations hereunder ... We may transfer, assign, or delegate these Terms and our rights and obligations without consent.</p> <p><b>Comment: The question is whether 'detriment' can be demonstrated; this is unlikely unless for example, Samsung sold the business to a competitor (who without compensation, bricks their system).</b></p>
<p><b>k) limit one party's rights to sue another party;</b></p>	<p><b>4(g)</b> The Services provide you with information ("Product Information") regarding the Products in your home and their connection with other products and services. All Product Information is provided "as is" and "as available". We cannot guarantee that it is correct or up to date.</p> <p>4(h) You acknowledge that all Content accessed by you using the Services is at your own risk and you will be solely responsible for any damage or loss to any party resulting therefrom... you hereby release us from all liability for you having acquired or not acquired Content through the Services.</p> <p><b>Comment: the application of these clauses in the event of (e.g.) a fire where alarms are controlled through Nest may be unfair – given the product representations and marketing.</b></p> <p><b>5(h) Release Regarding Third Parties.</b> Nest is not responsible for third parties or their products and services, including, without limitation, the App Stores, Third-Party Products and Services, Third-Party Sites, Referred Vendors, Equipment, ISP and Operators. Nest hereby disclaims, and you hereby discharge, waive and release Nest and its licensors and suppliers from any past, present and future claims, liabilities and damages, known</p>	<p><b>[TOU] 3.7 Exclusion of Liability.</b> Without limiting the exclusion of liability in the Amazon.co.uk Conditions of Use and Sale, our or our licensor's aggregate liability to you for compensation under this Agreement with respect to any claim (in addition to any rights to obtain a repair, replacement or refund via your statutory rights) will not exceed fifty pounds sterling (£50.00). Nothing in this paragraph affects your statutory rights as a consumer or any liability for death, personal injury, or fraud.</p> <p><b>Comment: assuming this were modified to meet the ACL s 64 as to non-exclusion of the consumer guarantees, then this clause is acceptable, unless the link other limitations clauses is regarded as lacking in transparency or otherwise 'unfair' given consumers may have difficulty reconciling the two.</b></p> <p><b>[DTOU] General e. Applicable Law.</b> Any dispute or claim arising from or relating to this Agreement, an Amazon Device, the Software, the Digital Content, or the Services is subject to the Applicable Law, liability and all other terms in the Amazon.co.uk Conditions of Use. You agree to those terms by entering into this Agreement, or using an Amazon Device or the Services.</p> <p><b>Comment: again, referral reduces clarity and may expect too much of consumers to cross reference multiple contracts and to adduce what applies in which priority.</b></p>	<p><b>What else do I need to know?</b></p> <p><b>Warranty Disclaimer...</b> THE SERVICES (AND ALL PRODUCTS, SOFTWARE, SERVICES, INFORMATION AND CONTENT) ARE PROVIDED ON AN "AS-IS" BASIS, WITHOUT WARRANTIES OR ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR THAT USE OF THE FOREGOING WILL BE UNINTERRUPTED OR ERROR-FREE. <u>SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.</u></p> <p><b>Comment: may breach ACL s 64 as to non-excludable consumer guarantees and remedies of repair, replacement or refund depending upon whether a failure is major or minor. This may mislead consumers into thinking otherwise. Query whether the underlined portion (my emphasis) overrides the dominant impression of the bulk of the text, as well as whether these carve outs adequately or fairly inform consumers or may mislead or deceive them - this may go to fairness. (Note UK clause terminology 'implied warranty' is relevant to</b></p>

	<p>or unknown, arising out of or relating to your interactions with such third parties and their products and services. ...</p> <p><b>Comment: this broad release may mislead and deceive consumers as to their rights under the ACL, or be unfair under s 24 as too broad, especially as Nest ‘recommends’ certain products and suppliers.</b></p> <p><b>7. Indemnity</b>  You agree to defend, indemnify and hold Nest and its licensors and suppliers harmless from any damages, liabilities, claims or demands (including costs and attorneys’ fees) made by any third party due to or arising out of (i) your use and each Authorized User’s use of the Products or Services, (ii) your or your Authorized Users’ violation of these Terms, (iii) any User Submissions or Feedback you provide; or (iv) your or your Authorized Users’ violation of any law or the rights of any third party.</p> <p><b>Comment: excessively broad indemnity against third party claims (regardless of consumer control over them) may be unfair.</b></p> <p><b>8. Warranty Disclaimers</b>  (a) ...  (b) THE SERVICES ARE PROVIDED FOR YOUR CONVENIENCE, “AS IS” AND “AS AVAILABLE” AND NEST AND OUR LICENSORS AND SUPPLIERS EXPRESSLY DISCLAIM ANY WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, AND NON-INFRINGEMENT.</p>	<p><b>[DTOU] General</b>  <b>f. Exclusion of Liability.</b> Without limiting the exclusion of liability in the Amazon.co.uk Conditions of Use, (1) unless otherwise provided by Amazon, your Amazon Device may be subject to a limited warranty (in addition to any rights to obtain a repair, replacement or refund via your statutory rights); and (2) our or our licensor’s aggregate liability to you for compensation under this agreement with respect to any claim (in addition to any rights to obtain a repair, replacement or refund via your statutory rights) will not exceed the greater of fifty pounds sterling (£50.00) and the amount you paid for your Amazon Device. Nothing in this paragraph affects your statutory rights as a consumer or any liability for death, personal injury, or fraud.</p> <p><b>Comment: clear as to ACL s 64 but again cross referral to another agreement diminishes clarity. Best practice would suggest a link to an explanation of consumer’s statutory rights (which is on the website but not linked)</b></p> <p><b>[COUS] 13. Our Liability</b> ... Amazon will not be responsible for (i) losses that were not caused by any breach on our part, or (ii) any business loss (including loss of profits, revenue, contracts, anticipated savings, data, goodwill or wasted expenditure), or (iii) any indirect or consequential losses that were not foreseeable to both you and us when you commenced using the Amazon Services.</p> <p>We will not be held responsible for any delay or failure to comply with our obligations under these conditions if the delay or failure arises from any cause which is beyond our reasonable control. This condition does not affect your legal right to have goods sent or services provided within a reasonable time or to receive a refund if goods or services ordered cannot be supplied within a</p>	<p><b>Australian common law but not ACL statutory guarantees.)</b></p> <p><b>Limitation of Liability.</b> <u>TO THE FULLEST EXTENT ALLOWED BY APPLICABLE LAW, UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY (INCLUDING, WITHOUT LIMITATION, TORT, CONTRACT, STRICT LIABILITY, OR OTHERWISE) SHALL SMARTTHINGS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR (A) ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING DAMAGES FOR LOST PROFITS, LOSS OF GOODWILL, WORK STOPPAGE, ACCURACY OF RESULTS, OR FAILURE OR MALFUNCTION OF ANY DEVICE CONNECTED TO THE SERVICES, OR (B) ANY AMOUNT, IN THE AGGREGATE, IN EXCESS OF THE GREATER OF (I) \$100 OR (II) THE AMOUNTS PAID BY YOU TO SMARTTHINGS IN CONNECTION WITH THE SERVICES IN THE TWELVE (12) MONTH PERIOD PRECEDING THIS APPLICABLE CLAIM, OR (III) ANY MATTER BEYOND OUR REASONABLE CONTROL. <u>SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF CERTAIN DAMAGES, SO THE ABOVE LIMITATION AND EXCLUSIONS MAY NOT APPLY TO YOU.</u></u></p> <p><b>Comment: as above.</b></p> <p><b>Risk of Loss; Insurance.</b> YOU ACKNOWLEDGE AND AGREE THAT YOUR USE OF THE SERVICES (INCLUDING, WITHOUT LIMITATION, USING THE SERVICES TO SECURE OR OTHERWISE CONTROL ACCESS TO ANY REAL OR PERSONAL PROPERTY) IS SOLELY AT YOUR OWN RISK, AND THAT YOU ACCEPT</p>
--	---	--	--

	<p>(c) NEST AND OUR LICENSORS AND SUPPLIERS MAKE NO WARRANTY THAT DEFECTS WILL BE CORRECTED OR THAT THE SERVICES: (I) WILL MEET YOUR REQUIREMENTS; (II) WILL BE COMPATIBLE WITH YOUR HOME NETWORK, COMPUTER OR MOBILE DEVICE; (III) WILL BE AVAILABLE ON AN UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE BASIS; OR (IV) WILL BE ACCURATE OR RELIABLE. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM NEST OR THROUGH THE SERVICES SHALL CREATE ANY WARRANTY.</p> <p><b>Comment: clauses may breach ACL s 64 as to non-excludable consumer guarantees. The ACL guarantees entitle consumers to a repair, replacement or refund depending upon whether a failure is major or minor. This may mislead consumers into thinking otherwise. ...</b></p> <p><b>9. Limitation of Liability</b> Nothing in these Terms and in particular within this "Limitation of Liability" clause shall attempt to exclude liability that cannot be excluded under applicable law.</p> <p>TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW... IN NO EVENT WILL (A) NEST BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, EXEMPLARY, SPECIAL, OR INCIDENTAL DAMAGES, INCLUDING ANY DAMAGES FOR LOST DATA OR LOST PROFITS, ARISING FROM OR RELATING TO THE SERVICES OR THE PRODUCTS, EVEN IF NEST KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES, AND</p>	<p>reasonable time owing to a cause beyond our reasonable control.</p> <p>The laws of some countries do not allow some or all of the limitations described above. If these laws apply to you, some or all of the above limitations may not apply to you and you might have additional rights.</p> <p>Nothing in these conditions limits or excludes our responsibility for fraudulent representations made by us or for death or personal injury caused by our negligence or wilful misconduct.</p> <p><b>Comment: restrained limitations clause reflecting UK laws which carves out reasonable goods delivery times, refunds and contemplates Amazon responsibility for events within its reasonable control. A good example of the positive effect of regulation. But rather than a general reference to 'other laws', specific reference should be made to countries whose laws differ so that consumers clearly understand if the clause applies or not.</b></p> <p><b>[TOU] 3.6 Applicable Law [COU] 14. APPLICABLE LAW</b> These conditions are governed by and construed in accordance with the laws of the Grand Duchy of Luxembourg, and the application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. We both agree to submit to the non-exclusive jurisdiction of the courts of the district of Luxembourg City, which means that you may bring a claim to enforce your consumer protection rights in connection with these Conditions of Use in Luxembourg or in the EU country in which you live. The European Commission provides for an online dispute resolution platform, which you can access here: <a href="http://ec.europa.eu/consumers/odr/">http://ec.europa.eu/consumers/odr/</a>. If you would like to bring a matter to our attention, please contact us.</p>	<p>RESPONSIBILITY FOR ALL LOSSES, DAMAGES AND EXPENSES ARISING OUT OF SUCH USE.</p> <p><b>Comment: as above. 'Services' are also subject to statutory guarantees and 'software' is defined as 'good' so falls subject to the relevant consumer guarantees for goods.</b></p> <p><b>EULA re Garmin Connect Mobile App™</b> <b>No warranty</b> This application is provided to you 'as it is' and you agree to use it at your own risk. Garmin makes no guarantees...</p> <p><b>Disclaimer of warranty</b> GARMIN... DISCLAIM ANY WARRANTIES, EXPRESS OR IMPLIED, OF QUALITY, PERFORMANCE OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, NO ORAL OR WRITTEN ADVICE OR INFORMATION BY GARMIN SHALL CREATE A WARRANTY, AND YOU ARE NOT ENTITLED TO RELY UPON SUCH ADVICE OR INFORMATION. THIS DISCLAIMER OF WARRANTIES IS AN ESSENTIAL CONDITION OF THIS AGREEMENT. Some regions and countries do not allow certain warranty exclusions, so to the extent the above exclusion may not apply to you.</p> <p><b>Disclaimer of Liability.</b> ... GARMIN AND ITS AFFILIATES SHALL NOT BE LIABLE TO YOU: IN RESPECT OF ANY CLAIM.... Some regions and countries do not allow certain warranty exclusions, so to the extent the above exclusion may not apply to you.</p> <p><b>Comment: The above clauses are problematic potentially in terms of software as 'goods' and the non-excludable consumer guarantees. Whether they are fair given their breadth, the</b></p>
--	--	--	---

	<p>(B) NEST'S TOTAL CUMULATIVE LIABILITY ... EXCEED THE FEES ACTUALLY PAID BY YOU TO NEST OR NEST'S AUTHORIZED RESELLER FOR THE SERVICES OR THE PRODUCT AT ISSUE IN THE PRIOR 12 MONTHS (IF ANY). ..</p> <p><b>Comment: Question if the oft-used lower case initial sentence sufficiently informs consumers or overrides the dominant impression of the capitalised sections above and below. Absent the Regulation 90 statement, this may be sufficient to render this clause unfair as it does not sufficiently alert consumers to their rights.</b></p>	<p><b>Comment: TOU 3.6 is possibly unfair by requiring consumers to link across to other agreements and to locate the relevant term, rather than stating it outright. The EU provision proposed seems fair insofar as while jurisdiction is in one country, consumers may bring claims in their own (EU) country. Best practice would require a similar clause as to an Australian dispute resolution service.</b></p>	<p><b>emphasis of capitals, placement and the relative inconsequence of the carve out, is also an open question.</b></p>
<p>l) restrict one party's <b>right to commence dispute proceedings</b> against another party;</p>	<p><b>Preamble:</b> These Terms "...require the use of binding arbitration to resolve disputes rather than jury trials or class actions. Please follow the instructions ...below if you wish to opt out of this provision." ...</p> <p><b>11. Dispute Resolution and Arbitration</b> PLEASE READ THIS SECTION CAREFULLY. FOLLOW THE INSTRUCTIONS BELOW IF YOU WISH TO OPT OUT OF THE REQUIREMENT OF ARBITRATION ON AN INDIVIDUAL BASIS.</p> <p><b>11(a) Arbitration.</b> Nest and you agree to arbitrate all disputes and claims that arise from or relate to these Terms or the Services in any way, except for claims arising from bodily injury... by entering into this agreement, we are each waiving the right to a trial by jury or to participate in group litigation or collective procedures.</p> <p><b>11(f) 30-Day Opt-Out Period.</b> If you do not wish to be bound by the arbitration and class-action waiver ... you must notify Nest in writing within 30 days of the date that you first accept these Terms (unless a longer period is required by applicable law)... Your written notification must be mailed to Nest ... if you do not notify Nest ... you agree to</p>	<p><b>[TOU] 3.6 Applicable Law.</b> Any dispute or claim arising from or relating to this Agreement, Alexa, the Amazon Alexa App and the Software is subject to the Applicable Law, liability and all other terms in the Amazon.co.uk Conditions of Use. You agree to those terms by entering into this Agreement, or using Alexa.</p> <p><b>COUJ 14. APPLICABLE LAW</b> These conditions are governed by and construed in accordance with the laws of the Grand Duchy of Luxembourg, and the application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. We both agree to submit to the non-exclusive jurisdiction of the courts of the district of Luxembourg City, which means that you may bring a claim ... in Luxembourg or in the EU country in which you live. The European Commission provides for an online dispute resolution platform, which you can access here: <a href="http://...">http...</a></p> <p><b>Comment: Clause proposes a reasonable approach in an EU environment but Australian equivalent would require jurisdiction in Australia with dispute resolution jurisdiction available in the consumer's</b></p>	<p><b>Choice of Law; Arbitration.</b> These Terms are governed by and will be construed under the laws of the State of California... Any dispute arising from or relating to the subject matter of these Terms shall be finally settled in San Francisco County, California, ... by one commercial arbitrator ... (etc.)</p> <p>... the parties consent to exclusive jurisdiction and venue in the state or federal courts located in, respectively, San Francisco County, California, or the Northern District of California.</p> <p><b>Comment: This (clearly US) UK clause restricts certain consumer access to the courts save for injunctive or equitable relief. The UK High Court has found mandatory arbitration to be unfair. The forum and jurisdiction clearly restricts Australian consumers from commencing proceedings for cost and convenience reasons.</b></p>

	<p>be bound by... these Terms, including such provisions in any Terms revised after the date of your first acceptance...</p> <p><b>Comment: This (clearly US) UK clause restricts certain consumer access to the courts and class actions. The UK High Court has found mandatory arbitration to be unfair. Nest carve out certain types of disputes, retain small claims entitlements, pay certain costs, include local venue (US related) and offer a 30 day opt out in specific form. The question is whether their capitalised notice and complex opt out clause remain 'unfair'? Multiple factors: possible transparency issues; questions as to Nest's legitimate interest; party imbalance; consumer detriment legal rights restriction; &amp; US AAA jurisdiction is problematic, as is some confusion as to venue and in-person format. A best practice solution may be an open opt-in with a check box or simple link to a page for completion to overcome rigorous notice requirements. It may be fairer to use arbitration services within consumer jurisdiction not just a US process. Finally, as a practical matter, behavioural economics suggests that consumers are unlikely to opt out within 30 days- so the time limit may seem 'unfairly' self-serving.</b></p>	<p><b>state. An online dispute resolution system may be offered but not as the sole option.</b></p>	
<p>m) <b>limit evidence</b> counterparty can adduce in contract proceedings;</p>	<p>As above.</p> <p><b>Comment: Arbitration rules and (uncertain) forum may restrict consumer rights to adduce evidence.</b></p>		<p>As above.</p> <p><b>Comment: Arbitration rules and (uncertain) forum may restrict consumer rights to adduce evidence.</b></p>
<p>n) impose <b>evidential burden</b> on one party in proceedings re contract.</p>	<p>As above.</p> <p><b>Comment: Arbitration rules and US forum are unlikely to offer consumers the advantageous presumptions such as those within section</b></p>		<p>As above.</p> <p><b>Comment: Arbitration rules and US forum are unlikely to offer consumers the advantageous presumptions such as those within section</b></p>

	24(4) that a term is presumed not to be reasonably necessary to protect the legitimate interests of the party who is advantaged by the term, which in this case would be Nest's burden to rebut.		24(4) that a term is presumed not to be reasonably necessary to protect the legitimate interests of the party who is advantaged by the term, which in this case would be Nest's burden to rebut.
s 24(2) In determining if a term is unfair, court must take into account:			<b>Subjective ratings key</b> ☺ okay    ☺☺ good    ☺☺☺ very good+ ☹ <okay    ☹☹ poor    ☹☹☹ very poor+
<b>reasonably plain language</b>	☺☹☹☹☹ ☺☺ Language moderately plain though very complex in places ☹☹ Very Long: 12107 words to 16308 [including privacy] <b>Comment:</b> ☹☹ Multiple contracts means consumers must read across contracts ☹☹☹ Extensive and (overly) broad & complex indemnities ☹☹☹ Legalese	☺☺☺☹☹ ☺☺☺ Language: reasonably plain, little legalese ☹☹☹ Very long: 30,940 words <sup>1923</sup> <b>Comment:</b> ☹☹☹ Multiple contracts and many links means consumers must read across contracts and terms which creates complexity and reduces clarity. ☹ Legalese	☺☺☹☹☹ ☺☺ Language: initially colloquial and consumer friendly, reverts to legalese for Samsung-significant terms ☹☹ Very long: 4887; to 14182 [including Service Terms & Privacy] <b>Comment:</b> ☹☹ Multiple contracts means consumers must read across contracts and terms which creates complexity and reduces clarity. ☹☹☹ Extensive and (overly) broad & complex indemnities ☹☹ Legalese
<b>Legible</b> <sup>1924</sup>	☺☺☺	☺☺☺	☺☺☺
<b>presented clearly</b> <sup>1925</sup>	☺☹ ☺ Contract follows conventions as to clause placement; clear font and use of capitals attempts to draw consumer's attention to important aspects (though emphases may favour Nest's over consumer interests) ☹☹ BUT consumers must read across multiple contracts AND complexity both within and across these is significant.	☺☹☹ ☺☺ Contract follows conventions as to clause placement; clear font, headings, clause numbers and each is reasonably short form. ☹☹☹ BUT consumers must read across eight sets of terms (excluding links) AND complexity both within and across these is significant. Reduces clarity.	☺☹ ☺☺☺ Contract follows usual conventions as to clause placement; clear font, headings, clause numbers. ☹☹ BUT consumers must read across four contracts ☹ Important terms located mid bulky text reduces clarity

<sup>1923</sup> See <<https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201566380>>

<sup>1924</sup> This is usually defined to mean "clear enough to read": Collins English Dictionary. Interestingly

<sup>1925</sup> While there is no authority on the point, the author infers this means form and layout (i.e. presentation) or else it would be duplicative.

	⊖ Important terms located mid bulky text reduces clarity		
<b>readily available</b> <sup>1926</sup>	<p>⊖⊖⊖</p> <p>☺ Overseas (UK) terms online used for review</p> <p>⊖⊖⊖ No Australian terms online though product is sold in Australia</p>	<p>☺☺☺</p> <p>☺ Overseas (UK) terms online used for review</p> <p>☺ Products not officially sold in Australia yet</p>	<p>☺☺☺</p> <p>☺ Overseas (UK) terms online used for review</p> <p>☺ Products not officially sold in Australia yet</p>
<b>Overall rating:</b>	☺☺ / ⊖⊖⊖⊖⊖	☺☺☺ / ⊖⊖⊖	☺☺☺ / ⊖⊖⊖⊖⊖

Table S1.2 Smart home selective terms review

Source: author

<sup>1926</sup> Accessible via the internet should suffice.

## S1.2 Smart self

### Smart self: potentially applicable device terms

FITBIT Charge 2 Band <sup>1927</sup>	MILO Champions band	GARMIN Vivomove
<p><b>Contract:</b><sup>1928</sup>  <b>Fitbit Website Terms and Conditions</b><sup>*1929</sup> (TOS)  <b>Privacy Policy</b><sup>1930</sup>  <b>Product care;</b>  <b>Safety instructions</b>  <b>Cookie policy</b>  <b>Wellness Community Pledge Premium Membership Terms and Conditions</b>  <b>Community Guidelines</b>  <b>Terms of Sale</b>  <b>Returns and Warranty</b>  <b>Copyright Policy</b>  <b>Feedback and Submission Policy</b></p>	<p><b>Contract:</b>  Terms and conditions of Sale<sup>1931*</sup>  Milo Champions App v 3.3<sup>1932*</sup>  Condensed Privacy Policy**  Full Privacy Policy**  Nestle Website Disclaimer<sup>1933</sup>  FAQs</p> <p><i>**Discussed in Ch. 5</i></p>	<p><b>Contracts:</b>  Terms of Use<sup>1934*</sup>  Garmin Connect App<sup>1935*</sup>  Garmin Important Safety and product information (2016) &amp; Owner's Manual<sup>1936</sup>  Privacy Policy<sup>1937</sup></p>

Table S1.3 Smart self: potentially applicable device terms

Source: author

**Important Reader Note: All comments on these terms are illustrative only and do not imply contravention of the ACL. Terms cited are included for discussion purposes and are not necessarily or impliedly in breach of the provisions against which they are tabulated. Versions used are best available but may not apply to the Australian market. Not all products cited are yet sold in Australia. Terms quoted are copyright their respective owners.**

<sup>1927</sup> Derived randomly from Amazon Best Sellers, <<https://www.amazon.com/Best-Sellers-Sports-Outdoors-Fitness-Trackers/zgbs/sporting-goods/5393958011>> Note Fitbit Alta came third but is not included as its terms are the same as those for the Charge 2.

<sup>1928</sup> Fitbit's Legal Policy page <<https://www.fitbit.com/au/legal>>

<sup>1929</sup> <https://www.fitbit.com/au/legal/terms-of-service> Last update 22 Oct 2015.

<sup>1930</sup> <https://www.fitbit.com/au/legal/privacy>

<sup>1931</sup> <<https://shop.milo.com.au/terms-conditions>>

<sup>1932</sup> <https://app.milo.com.au/champ-squad>; in iTunes linked to <<https://itunes.apple.com/au/app/milo-champions-anz/id1049268402>>

<sup>1933</sup> <http://www.nestle.com.au/info/disclaimer>

<sup>1934</sup> <http://www.garmin.com/en-AU/legal/terms-of-use> (updated 3 Apr 2014)

<sup>1935</sup> <https://connect.garmin.com/en-US/privacy>> Note there is a privacy statement on the Au website but it refers users of Garmin Connect App to this US policy in lieu.

<sup>1936</sup> These appear online here: <https://support.garmin.com/support/manuals/searchManuals.faces?refresh=true>> Note the device box contains the Information but not the Manual which is here:

[http://static.garmin.com/pumac/vivomove\\_OM\\_EN.pdf](http://static.garmin.com/pumac/vivomove_OM_EN.pdf)

<sup>1937</sup> Privacy Statement is here: <<http://www.garmin.com/en-AU/legal/privacy-statement>> but a link in this directs users of Garmin Connect products to this document: <<https://connect.garmin.com/en-US/privacy>>

Smart self: selective terms review

<p><b>ACL SECTION 24</b> Examples of terms that are likely to be unfair include terms which:</p>	<p><b>FITBIT Charge 2 Band</b>  Fitbit Website Terms and Conditions (TOS) Privacy Policy</p>	<p><b>MILO Champions band</b>  Terms and conditions of Sale Milo Champions App v 3.3</p>	<p><b>GARMIN Vivomove</b>  Terms of Use Garmin Connect App Garmin Important Safety and product information (2016) &amp; Owner's Manual</p>
<p>a) allow only one party to avoid or limit the performance of the contract;</p>	<p><b>TOS. Changes to the Fitbit Service.</b> Fitbit may change or discontinue, temporarily or permanently, any feature or component of the Fitbit Service at any time without notice. Fitbit is not liable to you or to any third party for any modification, suspension or discontinuance of any feature or component of the Fitbit Service.</p> <p><b>Comment: unilateral variation of contract without reference to customer right to terminate. [Note however customers may terminate through ceasing device use at any time, but are left with a redundant product, and may not have retrieved data for portability purposes]</b></p>	<p><b>APP 8. Termination</b> ... Nestle also reserves the right to stop supporting the App and may terminate use of it at any time without giving notice to you.</p> <p><b>Comment: consumers who buy the fitness band want the App analytics; cessation of support or Service by Nestle avoids or limits contract performance as analytics and stored data history are a part of the services integral to the device purchase. Arguably, the App should be available for a reasonable period, perhaps consistent with the reasonable device life cycle (by analogy to ACL's spare parts requirements). Failure to do so may lead to an action under ACL section 18 such that any inconsistent term enabling App termination might in that context, be found to be unfair.</b></p>	<p><b>TOU Accounts</b></p> <p>...We may suspend or terminate your account and your ability to use any Garmin Site or portion thereof for failure to comply with these Terms of Use or any special terms related to a particular service.</p> <p><b>Comment: suspicion of account may limit Garmin's performance of its contract as to provision of the App services. As the basis for suspension is so broad (even for minor breach) this term may be unfair in certain circumstances.</b></p>
<p>b) allow only one party to terminate the contract;</p>		<p>As above.</p>	<p>TOU as above.</p> <p><b>Comment: No criteria are provided as to the determination which may render the clause unfair in certain factual situations.</b></p>
<p>c) penalise only one party for breach or termination of the contract;</p>	<p><b>Termination</b> If you violate these Terms, we reserve the right to deactivate your account or terminate these Terms, at our sole discretion, at any time and without notice or liability to you. Upon any such termination, we may delete Your Content and other information related to your account.</p> <p><b>Comment: there is no equivalent provision should Fitbit breach or terminate the contract – save for the consumer's right to cancel their account.</b></p>		

<p><b>d) allow only one party to vary the contract;</b></p>	<p><b>These Terms May Change</b>          These Terms will change over time. If we make minor changes to the Terms without materially changing your rights, we will post the modified Terms on www.fitbit.com. We will notify you by email, through the Fitbit Service, or by presenting you with a new Terms of Service to accept if we make a modification that materially changes your rights.</p> <p><b>Comment: unilateral as to changes. Unilateral determination as to “materiality” and therefore whether notified directly to consumers or otherwise</b></p>	<p><b>APP TERMS</b>  <b>7. Changes</b> Nestle reserves the right to make changes to these terms of use. Please refer to this page from time to time to review these terms of use and any new information.</p>	<p><b>TOU ...</b>We may suspend or terminate your account and your ability to use any Garmin Site or portion thereof for failure to comply with these Terms of Use or any special terms related to a particular service.</p>
<p><b>e) allow only one party to vary the ... characteristics of the goods or services to be supplied ... under the contract;</b></p>	<p><b>Changes To The Fitbit Service</b>          Fitbit may change or discontinue, temporarily or permanently, any feature or component of the Fitbit Service at any time without notice. Fitbit is not liable to you or to any third party for any modification, suspension or discontinuance of any feature or component of the Fitbit Service.</p> <p><b>Comment: unilateral variation of contract without reference to customer right to terminate. [Note however customers may terminate through ceasing device use at any time, but are left with a redundant product, and may not have retrieved data for portability purposes]</b></p>		<p><b>TOU Garmin's Liability</b>          ... Garmin makes no representations or warranties about the accuracy, reliability, completeness, or timeliness of the Content or about the results to be obtained from using the Garmin Sites and the Content. Any use of the Garmin Sites and the Content is at your own risk. Changes are periodically made to Garmin Sites and may be made at any time.</p>
<p><b>h) allow one party to unilaterally determine whether the contract has been breached or to interpret its meaning;</b></p>	<p>See (d) above</p> <p>We reserve the right (but are not required) to remove or disable access to the Fitbit Service, any Fitbit Content, or Your Content at any time and without notice, and at our sole discretion, if we determine that the Fitbit Content, Your Content, or your use of the Fitbit Service is objectionable or in violation of these Terms.</p> <p><b>Comment: unilateral determination permitted at any time, without notice and Fitbit determine standard as to breach by “objectionable” use. This may be unfair depending upon how it is applied on given facts.</b></p> <p>It is Fitbit’s policy to terminate in appropriate circumstances account holders who repeatedly infringe the rights of copyright holders.</p>		<p><b>TOU Accounts</b></p> <p>...We may suspend or terminate your account and your ability to use any Garmin Site or portion thereof for failure to comply with these Terms of Use or any special terms related to a particular service.</p> <p><b>Comment: unilateral determination permitted at any time, without notice and Garmin (it seems) determine standard as to breach of their Terms, without criteria or notice requirements. This may be unfair depending upon how it is applied on given facts.</b></p>

	<p><b>Comment: there is no consultation or appeals process; Fitbit is the sole determinant. This may be unfair depending upon how it is applied on given facts.</b></p> <p>If you violate these Terms, we reserve the right to deactivate your account or terminate these Terms, at our sole discretion, at any time and without notice or liability to you. Upon any such termination, we may delete Your Content and other information related to your account...</p> <p><b>Comment: unilateral determination as to "violation" and potentially unreasonable right to delete account information without a right for consumers to retrieve data. This may be unfair depending upon how it is applied on given facts.</b></p>		
<p>i) limit one party's vicarious liability for its agents;</p>			<p><b>TOU Garmin's Liability</b>  ... Some Content on the Garmin Sites may be provided by third parties and Garmin will not be held responsible for any such Content provided by third parties.</p> <p><b>Comment: are these entities agents at law – may depend on the facts.</b></p>
<p>j) allow one party to assign the contract to the counterparty's detriment without the counterparty's consent;</p>	<p><b>General Terms ...</b> You may not assign or transfer these Terms, by operation of law or otherwise, without Fitbit's prior written consent. Any attempt by you to assign or transfer these Terms, without such consent, will be null. Fitbit may freely assign or transfer these Terms without restriction.</p> <p><b>Comment: this clause clearly enables such an assignment, by unilateral right favouring Fitbit.</b></p>		
<p>k) limit one party's rights to sue another party;</p>	<p>We are not responsible for the accuracy, reliability, effectiveness, or correct use of information you receive through the Fitbit Service...If you rely on any Fitbit Content or the Fitbit Service, you do so solely at your own risk.</p> <p><b>Comment: seeks to limit consumer rights to sue where the device is inaccurate, unreliable or ineffective. May potential breach the consumer guarantee non-exclusion under s. 64</b></p>	<p><b>APP 5. Liability</b> While Nestle uses all reasonable efforts to ensure the accuracy of materials on our App and to avoid disruptions, we are not responsible for inaccurate information, disruptions, discontinuance of other events which may cause you damage, either direct (e.g. computer failure) or indirect (e.g. loss of profit). Any reliance upon materials on this App shall be at your own risk...</p> <p><b>Comment: this clause attempts to exclude liability which may potentially conflict with the ACL obligations as to</b></p>	<p><b>TOU Use of Content</b>  ... UNLESS OTHERWISE SPECIFICALLY AND EXPRESSLY STATED ELSEWHERE, GARMIN HEREBY DISCLAIMS ALL WARRANTIES WITH REGARD TO THE SOFTWARE, INCLUDING WITHOUT LIMITATION ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, WHETHER SUCH WARRANTIES ARE EXPRESS, IMPLIED OR STATUTORY... (etc.)</p>

You acknowledge sole responsibility and assume all risk arising from your use of any Third-Party Services.

**Comment: while commonplace, this clause may not apply if ACL s. 18 is breached where the provider may be recommending the services.**

#### Disclaimers

THE FITBIT SERVICE AND FITBIT CONTENT ARE PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND. WITHOUT LIMITING THE FOREGOING, WE EXPLICITLY DISCLAIM ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUIET ENJOYMENT OR NON-INFRINGEMENT, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. We make no warranty that the Fitbit Service or Fitbit Content will meet your requirements or be available on an uninterrupted, secure, or error-free basis. We make no warranty regarding the quality, accuracy, timeliness, truthfulness, completeness or reliability of the Fitbit Service or any Fitbit Content. You acknowledge and agree that if you rely on any Fitbit Content or the Fitbit Service, you do so solely at your own risk.

**Comment: this clause may breach ACL section 64 as to non-exclusion of consumer guarantees. It may also infringe ACL sections 18 and 29 if the product marketing (etc.) conveys a different impression to consumers as to product performance.**

#### Indemnity

You will indemnify and hold harmless Fitbit and its officers, directors, employees and agents, from and against any claims, disputes, demands, liabilities, damages, losses, and costs and expenses, including, without limitation, reasonable attorneys' fees arising out of or in any way connected with (i) your access to or use of the Fitbit Service, (ii) Your Content, or (iii) your breach of any warranties made by you hereunder or your violation of any other provision of these Terms. We reserve the right to assume control of the defense of any third-party claim that is subject to indemnification by you, in which event you will cooperate with us in asserting any available defenses.

**software being fit for purpose and of acceptable quality. Query whether the overall product marketing and representations align to the product "Purpose" clause 1: "The App is intended to impart information of a general nature only and all calculations are approximate". In that context liability exclusions as to accuracy seem reasonable- unless overall impressions created elsewhere in marketing, etc. override that., rendering it potentially an unfair term and also, in breach of sections 18 and 29 (quality standard etc.).**

#### MILO Sale Terms:

8.1 [Regulation 90 statement]

8.2 To the extent permitted by law, Nestlé's only liability is as expressly stated in these terms and in the Australian Consumer Law and all other guarantees, warranties and conditions are excluded.

8.3 To the extent permitted by law, then except as provided under the Australian Consumer Law, Nestlé will not be liable to you (whether in contract, tort, or otherwise) for any consequential, special, incidental or indirect loss or damage including loss of profit.

**Comment: these terms reflect ACL rights, exclude any other warranty & perhaps evidence the efficacy of legislation to compel compliance.**

#### 9. INDEMNITY

9.1 You indemnify and must keep Nestlé, its officers, employees and agents indemnified against all reasonable damages, losses, costs and expenses suffered by them arising out of any breach by you of these terms or arising out of your use, possession or sale of the Goods or Services, or the use, possession or sale of the Goods or Services by someone with your authority or permission.

...

10.7 These terms are governed by and must be construed in accordance with the laws of New South Wales.

**Comment: as these terms also apply to NZ consumers, this clause may limit NZ rights to sue based upon cost and inconvenience, and so be unfair.**

.... IF ANY OF THE ABOVE PROVISIONS ARE VOID UNDER APPLICABLE LAW, GARMIN'S LIABILITY SHALL BE LIMITED TO THE FULL EXTENT PERMITTED BY LAW.

*(author emphasis)*

**Comment: The presentation and placement of the underlined portion may obscure its impact and is not transparent, especially after provisions which may mislead consumers as to the existence and effect of non-excludable consumer guarantees s 64 as to 'software' which is a defined 'good'. Reg 90 para does not appear to clarify Australian rights.**

#### TOU Garmin's Liability

Garmin makes no representations or warranties about the accuracy, reliability, completeness, or timeliness of the Content or about the results to be obtained from using the Garmin Sites and the Content. Any use of the Garmin Sites and the Content is at your own risk. ... THE GARMIN SITES AND CONTENT ARE PROVIDED ON AN 'AS IS' BASIS WITHOUT ANY WARRANTIES OF ANY KIND. GARMIN, TO THE FULLEST EXTENT PERMITTED BY LAW, DISCLAIMS ALL WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT OF PROPRIETARY OR THIRD PARTY RIGHTS, AND THE WARRANTY OF FITNESS FOR PARTICULAR PURPOSE.

#### Disclaimer of Certain Damages

Your use of the Garmin Sites is at your own risk. If you are dissatisfied with any of the Content or other contents of the Garmin Sites or with these Terms and Conditions, your sole remedy is to discontinue use of the Garmin Sites. IN NO EVENT WILL GARMIN OR ANY THIRD PARTIES MENTIONED AT THE GARMIN SITES BE LIABLE FOR ANY DAMAGES WHATSOEVER ... SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO

**Comment: broad indemnity applies to consumer warranties even where Fitbit disclaim their (statutory) warranties.**

**Limitation of Liability**

...SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

**Comment: above clause appears after an extensive limitation clause in capitals, merges into the text and is not transparent as to whether it applies. As these terms appear on the Australia website, they should not mislead consumers as to the applicable law or confuse them as to what applies.**

YOU, IN WHICH CASE SUCH EXCLUSION OR LIMITATION APPLIES TO THE FULLEST EXTENT ALLOWABLE UNDER THE APPLICABLE LAW.  
(author emphasis)

**Comment: The presentation and placement of the underlined portion may obscure its impact and is not transparent, especially after provisions which may mislead consumers as to the existence and effect of non-excludable consumer guarantees s 64**

**TOU Indemnity**

You agree to defend, indemnify, and hold harmless Garmin, its officers, directors, employees and agents, from and against any claims, actions or demands, including without limitation reasonable legal and accounting fees, alleging or resulting from your breach of these Terms of Use.

**DEVICE BOOKLET July 2016**

**Limited Warranty<sup>1938</sup>**

**One Year Consumer Products Limited Warranty**

Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

The benefits under our Limited Warranty are in addition to other rights and remedies under applicable law in relation to the products....

[then cites manufacturer's limited warranty... concluding with exclusions cited above again]

THE WARRANTIES AND REMEDIES CONTAINED HEREIN ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES EXPRESS, IMPLIED, OR

<sup>1938</sup> Under Support on the AU website: <<http://www.garmin.com/au/support/warranty>>

			<p>STATUTORY, INCLUDING ANY LIABILITY ARISING UNDER ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, STATUTORY OR OTHERWISE. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. IN NO EVENT SHALL GARMIN BE LIABLE FOR ANY INCIDENTAL, SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES... <u>SOME STATES DO NOT ALLOW THE EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.</u> <i>(author emphasis)</i></p> <p><b>Comment: multiple conflicting sources and content is potentially problematic. This statement potentially confuses the Reg 90 requirements and effect of consumer guarantees with the limited warranty, through placement and content. The heading and capitalised sections (of the LW) may dominate in impression and override the ACL requirements or at least, the conflicting information without distinguishing the difference, may confuse consumers. As such it is potentially misleading and may be unfair as well.</b></p>
<p><b>l) restrict one party's right to commence dispute proceedings against another party;</b></p>	<p><b>Governing Law:</b> The Terms of Service and the resolution of any Disputes shall be governed by and construed in accordance with the laws of the State of California without regard to its conflict of laws principles. <b>Comment: this may restrict Australian consumer's rights to institute due to cost barriers.</b></p> <p><b>We Both Agree To Arbitrate:</b> You and Fitbit agree to resolve any Disputes through final and binding arbitration, except as set forth under Exceptions to Agreement to Arbitrate below.</p> <p><b>Opt-out of Agreement to Arbitrate:</b> You can decline this agreement to arbitrate by contacting legal@fitbit.com within 30 days of first accepting these Terms of Service and</p>	<p><b>APP Governing Law &amp; Jurisdiction.</b> You and Nestle agree that any claim or dispute relating to the App shall be governed by the law of New South Wales and brought before the courts of New South Wales.</p> <p><b>Comment: From an Australian and NZ consumer perspective (the target markets) home purchase jurisdiction and law would better facilitate the right to commence proceedings, due to cost or inconvenience; this especially applies as Nestle is in multiple locations across both countries.</b></p>	<p><b>TOU General</b> Except to the extent provided below in this paragraph, all legal issues arising from or related to the use of any Garmin Site will be construed in accordance with and determined by the laws of the State of Kansas applicable to contracts entered into and performed within the State of Kansas without respect to its conflict of laws principles. By using a Garmin Site, you agree that the exclusive forum for any claims or causes of action arising out of your use of the Garmin Site is the United States District Court for the District of Kansas, or any Kansas State court sitting in Johnson County. You hereby irrevocably waive, to the fullest extent permitted by law, any objection which you may now or hereafter have to the laying of the venue of any such proceeding brought in</p>

stating that you (include your first and last name) decline this arbitration agreement.

**No class actions:** ...Class arbitrations, class actions, private attorney general actions, and consolidation with other arbitrations aren't allowed under our agreement.

**Comment: Two potential concerns: (1) Terms imposing arbitration have been found to be unfair in the UK in *Mylcris Builders Ltd v Mrs G Buck*. While the UK statute contains an express 'good faith' requirement unlike Australia's, other ACL factors requiring consideration are similar and if a court agrees a short opt out of otherwise mandatory 'arbitration' (save for small claims) restricts the right to commence proceedings, then the term may be unfair. The opt out clause may overcome that analysis unless a court were of the view that its (unnecessary) limited time frame and the inconvenient actions required (in lieu of a simple check box for example) constitutes a restriction. (2) Terms imposing foreign arbitration (and choice of law) may be void to the extent they exclude restrict or modify statutory guarantees: ACL s 64(1).**

**Judicial Forum for Disputes:** In the event that the agreement to arbitrate is found not to apply to you or your claim, you and Fitbit agree that any judicial proceeding (other than small claims actions) will be brought in the federal or state courts of San Francisco County, California. Both you and Fitbit consent to venue and personal jurisdiction there. We both agree to waive our right to a jury trial.

**Limitation on Claims:** Regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to your use of the Fitbit products or Fitbit Service must be filed within one (1) year after such claim or cause of action arose, or else that claim or cause of action will be barred forever.

**Comment: Both clauses may have the effect of restricting an Australian consumer's rights (which otherwise exist) to institute proceedings, so may be unfair.**

such a court and any claim that any such proceeding brought in such a court has been brought in an inconvenient forum.

**Comment: practically such a provision entails expense which could not be justified by an Australian litigant and may unfairly have the effect of limiting the consumer's right to sue. Note may conflict with ACL ss. 64 and 68 and the Valve decision.**

<p><b>m) limit the evidence that the counterparty can adduce in proceedings relating to the contract</b></p>	<p><b>Arbitration Procedures:</b> The American Arbitration Association (AAA) will administer the arbitration under its Commercial Arbitration Rules and the Supplementary Procedures for Consumer Related Disputes. The arbitration will be held in the United States county where you live or work, San Francisco, California, or any other location we agree to.</p> <p><b>Comment:</b> the AAA Rules may limit evidence which may be adduced. The unilateral right of Fitbit to decide forum may also limit consumer capacity to present evidence due to time, cost, inconvenience reasons; depending upon arbitration terms and conduct.</p>		<p>Above re General.</p> <p><b>Comment: US (Kansas) jurisdiction may entail limitations upon evidence a consumer may adduce depending upon Kansas rules.</b></p>
--	--	--	--

<p>s 24(2) In determining if a term is unfair, court must take into account:</p>	<p><b>Subjective ratings key</b></p> <p>😊 okay    😊😊 good    😊😊😊 very good+</p> <p>😞 &lt;okay    😞😞 poor    😞😞😞 very poor+</p>
--	--

<p><b>reasonably plain language</b></p>	<p>😊😊😊😊</p> <p>😊😊 Language plain and mostly clear          😞😞 Very Long: 7397 [incl privacy]</p> <p><b>Comment:</b>          😞😞 Multiple contracts mean consumers must read across contracts though Website Terms and privacy cover most aspects          😞😞😞 Extensive, broad &amp; complex indemnities          😞 Legalese</p>	<p>😊😊😊😊</p> <p>😊😊😊 Language: plain, little legalese          😞 Long 5,500 (approx. incl privacy)</p> <p><b>Comment:</b>          😞😊 Simpler terms as warranty/ guarantee and liability is limited to ACL requirements (though these are not explained)          😞 Multiple contracts and some links means consumers must read across contracts and terms, which creates complexity and reduces clarity.          😞 Legalese</p>	<p>😊😊😊😊</p> <p>😊 Language is plain but some legalese          😞 Very long: 7834 words [incl privacy]</p> <p><b>Comment:</b>          😞😞 Contracts and terms across multiple locations may affect their efficacy legally, and for consumers, creates confusion, complexity and reduces clarity.          😞😞😞 Extensive, broad &amp; complex indemnities          😞😞 Legalese</p>
<p><b>Legible<sup>1939</sup></b></p>	<p>😊😊😊</p>	<p>😊😊😊</p>	<p>😊😊😊</p>
<p><b>presented clearly<sup>1940</sup></b></p>	<p>😊😊😊</p> <p>😊😊😊 Contract follows conventions as to clause placement; clear font, layout and use of capitals attempts to draw consumer's attention to the liability limitation clause          😞😊😊 headings simple and easy to locate</p>	<p>😊😊😊😊</p> <p>😊😊 Contract follows conventions as to clause placement; clear font, headings, clause numbers and each (excluding privacy policy) is relatively short form.          😞😞😞 BUT privacy policy is long and condensed policy contains potential inconsistency with long form policy as to</p>	<p>😞😞😞</p> <p>😞😞😞 Organisation of all relevant terms is unclear and quite difficult to locate          😞 Contracts do not follow usual formats and overall organisation across website pages may prejudice meaning/ consistency in some contexts</p>

<sup>1939</sup> This is usually defined to mean “clear enough to read”: Collins English Dictionary.

<sup>1940</sup> While there is no authority on this, the author infers this means form and layout (i.e. presentation) or else it would be duplicative.

	☹️☹️ BUT consumers must read across multiple contracts and links which increases complexity and decreases clarity	children's private information which may confuse consumers. (See Sched. 2.2 for details)	☹️ Multiple terms and conditions are very difficult to locate: e.g. the website refers to TOU and privacy; then TOU refer to Connect App terms and privacy; but consumers must go to Support (without prompt) for product manuals (which contain EULA) and Important Information, both of which contain significant clauses.
<b>readily available</b> <sup>1941</sup>	☹️☹️ ☹️ US terms apply as per Australian website: <a href="https://www.fitbit.com/au/legal/terms-of-service">https://www.fitbit.com/au/legal/terms-of-service</a>	☹️☹️☹️ Website and app store. Note app terms are not available online – only via mobile phone which limits screen size and readability.	☹️☹️☹️☹️ ☹️ Australian web pages and App but some terms appear US in origin
<b>Overall rating:</b> <sup>1942</sup>	☹️☹️ / ☹️☹️☹️	☹️☹️☹️ / ☹️☹️	☹️ / ☹️☹️☹️

Table S1.4 Smart self selected terms review

Source: author

<sup>1941</sup> Accessible via the internet should suffice.

<sup>1942</sup> This rating is subjective but attempts to address questions of overall contract content, length, complexity, organisation, legalise, layout, legal accuracy, clarity and overall consumer friendliness; under the headings contained within section 25 of the ACL.

## Schedule 2: Privacy

### S2.1: Australian Privacy Principles

## Australian Privacy Principles — a summary for APP entities

from 12 March 2014

Australian Government  
Office of the  
Australian Information Commissioner

**APP 1 — Open and transparent management of personal information**  
Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

**APP 2 — Anonymity and pseudonymity**  
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

**APP 3 — Collection of solicited personal information**  
Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

**APP 4 — Dealing with unsolicited personal information**  
Outlines how APP entities must deal with unsolicited personal information.

**APP 5 — Notification of the collection of personal information**  
Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

**APP 6 — Use or disclosure of personal information**  
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

**APP 7 — Direct marketing**  
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

**APP 8 — Cross-border disclosure of personal information**  
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

**APP 9 — Adoption, use or disclosure of government related identifiers**  
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

**APP 10 — Quality of personal information**  
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

**APP 11 — Security of personal information**  
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

**APP 12 — Access to personal information**  
Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

**APP 13 — Correction of personal information**  
Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

[www.oaic.gov.au](http://www.oaic.gov.au)

For private sector organisations,  
Australian Government  
and Norfolk Island agencies  
covered by the Privacy Act 1988

Graphic S2.1: Australian privacy principles – a summary for APP entities  
Source: OAIC

## S2.2: Global consumer internet of things privacy sweep

International Results Summary: 314 CIOT devices	
Indicator	International Outcome "NO"(unless specified)
Indicator 1: Do privacy communications adequately explain how personal information is collected, used and disclosed?	59%
Are privacy communications specific to the device?	69%
Do privacy communications mention disclosure to other companies?	48%
Is the user told which companies?	76%+
Do privacy communications match the user experience?	62% (24% don't know)
<b>Does the company collect the following information?</b>	
- Location	68% YES
- Photo/video/audio files	41% YES
- Date of birth	64% YES
<b>Does the company explain why the device collects certain information? (+Canada response only)</b>	
- Location	47%+
- Photo/video/audio files	75%+
- Date of birth	89%+
Indicator 2: Are users fully informed about how personal information collected by the device is stored and safeguarded	68%
Indicator 3: Do privacy communications include contact details for individuals wanting to contact the company about a privacy-related matter?	38%
Indicator 4: Do privacy communications explain how a user can delete their information?	72%
Indicator 5: Did the company provide a timely, adequate and clear response to follow up questions?	43%

Table S2.2 International consumer internet of things privacy sweep  
Source: Author using Office of the Privacy Commissioner of Canada data<sup>1943</sup>

<sup>1943</sup> Office of the Privacy Commissioner of Canada, 'Results of the 2016 Global Privacy Enforcement Network Sweep' (22 Sept 2016 accessed 25 Sept 2016) <[https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/bg\\_160922/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/bg_160922/)>

## Schedule 3: Australian software-related recalls<sup>1944</sup>

### S3.1 Vehicle recalls: 2014- Mar 2017<sup>1945</sup>

Brand/ vehicle	Software defect	Dealer software update fix	Consumer hazard/ risk Vehicle damage (V) personal injury (PI)
Subaru Impreza PRA2017/15954	Reverse camera screen may freeze misrepresenting view, deceiving driver & endangering road users	✓	✓
Maserati Quattroporte PRA 2017/1593022	Gearshift may misrepresent the vehicle is in park when it is in drive	✓	✓
VW Golf/ Passat PRA 2017/15890	Software error may cause inoperative lights & indicator bulb warning-lights so driver is misled	✓	✓
Chevrolet Silverado & GMC Sierra PRA 2017/15825	Sensing and diagnostic module control software defect may prevent front airbag deployment	✓	PI
Mercedes-Benz GLE/GLS PRA 2016/15819	Incorrect software coding may prevent front passenger seat occupancy-recognition control unit from working resulting in airbag not deploying.	✓	PI
Mercedes-Benz "S" Class PRA No: 2016/15792	"Incorrect software coding" may impair front seatbelt operation and expose sharp edges.	?	PI
Suzuki Vitara PRA 2016/15747	Ambient Temperature Sensor Malfunction Indicator Light may not illuminate	✓	ADR breach (emissions)
Peugeot 4008 PRA 2016/15716	Transmission may delay acceleration (unexpectedly).	✓	✓
Ford Mondeo PRA 2016/15710	Headlamps may switch off.	✓	✓
Mitsubishi Lancer, ASX and ZK Outlander	CVT may delay acceleration (unexpectedly).	✓	✓
Mercedes-Benz GLE PRA 2016/15488	Engine may stall when braking at low speed.	?	✓
Mitsubishi i-MiEV PRA 2016/15469	Brake booster vacuum may fall, diminishing brakes and increasing stopping distance.	✓	✓
Hyundai Elantra PRA 2016/15385	Unnecessary front airbags unnecessarily including at zero or low speeds.	✓	✓
Jeep Renegade PRA 2016/15169	Park Assist Mode may not stop vehicle as intended. <sup>1946</sup>	✓	✓
Mercedes-Benz S63	Engine may stall when coasting to a stop.	✓	✓

<sup>1944</sup> Raw data from <https://www.productsafety.gov.au/> Software defect descriptions reflect manufacturer notices.

<sup>1945</sup> There are 81 software-based recalls cited; by manufacturer these are - Chrysler (15), Mercedes-Benz (12), Peugeot (11), Volvo (7), Other brands (5), Jaguar (4), Audi, Citroen (3) Volkswagen, Honda, Hyundai, Landrover, Mitsubishi, Nissan, Subaru, Suzuki, Toyota (2), Fiat, and Ford (1). Note: the only Tesla recall was not software-related.

<sup>1946</sup> NHTSA assert that 266 crashes had injured 68 people as at June 2016. In May 2016, a software update "no later than July or August" was promised, illustrating that defects may lack immediate fixes.

PRA 2015/15065			
Honda City & Jazz PRA 2015/14908	CVT programming may stress & break drive shaft, causing loss in acceleration or front wheel lock-up.	✓	✓
Hyundai Elantra & i30	Unexpected loss of power steering reduces control	?	✓
Toyota Prius V	ECU software may overheat sensors causing vehicle to stop unexpectedly.	✓	✓
Honda Accord & CR-V PRA 2015/14764	Collision Mitigation Braking System (CMBS) may unexpectedly activate while driving & misinterpret roadside objects, such as metal fences or guardrails, as obstacles requiring emergency braking.	✓	✓
Subaru Liberty and Outback PRA 2015	Brake lamp switch (BLS) software failure may compromise brakes	✓	✓
Land Rover Discovery PRA No. 2015/14651	ABS Software may falsely detect a fault, lowering suspension & disabling stability and maximum speed systems	✓	✓
Mercedes-Benz C200	Engine may stall in warm up phase.	✓	✓
Chrysler Jeep Cherokee PRA No. 2015/14575	Occupant Restraint Control Module software may activate unwanted airbag deployment.	✓	✓
Mahindra XUV500 PRA 2015/14564	Side curtain airbag may not deploy.	✓	✓
Jaguar XK PRA 2015/14526	Front park lights turn off without warning.	✓	✓
Chrysler Jeep PRA 2014/14439	"A loss of ESC function during certain driving conditions could cause a crash without warning."	✓	✓
Nissan Infiniti PRA 2014/14335	Unexpected acceleration.	✓	✓
Infiniti V37 Q50 PRA 2014/14333	Software error may cut power to electric vehicle.	✓	✓
Chrysler Jeep PRA 2014/14284	Rear turn lamp outage detection system may not work.	✓	✓
Jaguar F-Type PRA 2014/14250	Software fails to restrict road speed if deployable rear spoiler (DRS) fails to deploy, compromising stability and control.	✓	✓
Chrysler Jeep PRA 2014/14139	Unprompted acceleration may result in "very high vehicle speeds and make it difficult to stop or slow the vehicle".	✓	✓
Volvo V40	Rear light may fail due to a software failure posing a traffic hazard due to reduced visibility.	✓	✓
Toyota Prius PRA 2014/13991	Software defect may cause hybrid system shut down causing the vehicle to stop unexpectedly.	✓	✓

Table S3.1 Vehicle recalls: software defects 2014- 2016

Source: author using Australian government data

### S3.2 Smart self recalls: software defects 1998- 2016

Product	Software defect	Action proposed
Medtronic insulin pumps PRA 2017/15938	Charging issue may stop therapy after alarm. "If the alarm is ignored and no action is taken to correct the problem, the user could develop dangerously high blood sugar levels (hyperglycaemia) which can cause serious health problems." <sup>1947</sup>	Letter to customers and advice to call Helpline if error appears.
GolfBuddy GPS Wristband PRA No.2016/15241	Sweat may result in a skin burn between the wrist and the unit due to a firmware issue.	Customer to upgrade firmware via weblink
Acauanaut Suunto Diving Instruments  PRA 2006/8580	A software bug may result in incorrect tracking of dive time, resulting in a drowning risk.	Nil. Return to retailer.
Scubapro-Uwatec Dive Computers  PRA 2003/6335	A software programming error in these computers may stop alert signals and/ or freeze the screen, showing inaccurate information as to water depth, tank pressure, ascent rate etc.	Nil. Return to retailer.
Citizen Eco-Drive Watches PRA 1998/3746	Software defect may result in incorrect depth indicator readings.	Nil. Return to retailer.

Table S3.2 Australian smart self product recalls: software defects 1998- 2016  
Source: author using Australian government data

<sup>1947</sup> Ibid.

## Annexure A Thesis scope

### A1 Research outline

#### A1.1 Research questions

This thesis is designed to investigate the following:

**How can Australian regulators and policy makers best fulfil the objectives of the Australian Consumer Policy Framework to improve consumer wellbeing through empowerment and protection, cognisant of Australian consumer laws and privacy principles, while fostering the twenty-first century consumer internet of things, as exemplified by smart cars, homes and self?**

#### A1.2 Research purpose

This thesis was undertaken to:

- stimulate discussion amongst government, industry and stakeholders as to consumer IOT issues;
- review certain regulation, identify gaps based upon the policy objective, key issues and to provide options for evaluation;
- respond to public reviews, with respect to the CIOT as an “emerging technology”;
- provide a range of complementary recommendations or more broadly, principles, respecting the policy objective.

#### A1.3 Content scope & exclusions

CIOT legal and policy issues are voluminous. This thesis illustrates many of these in an Australian consumer law context, using the smart car, home and self as illustrative examples. It does not consider other significant areas, such as extant technical constraints, the (massive) industrial IOT, smart retail, health, cities, and so on. The constraints of topic and word limit guided this excision, together with a focus upon applications most proximate to Australian consumers.

This paper *excludes*:

- **Legal areas** including certain federal and state laws pertaining to discrimination,<sup>1948</sup> surveillance,<sup>1949</sup> intellectual property, telecommunications,<sup>1950</sup> common and criminal law aspects,

---

<sup>1948</sup> For a summary, see AHRC, above n 779. For legislation, see above n 777.

<sup>1949</sup> See VLRC, above n 1480.

<sup>1950</sup> Telecommunications Act 1997 (Cth); Telecommunications (Interception and Access) Act 1979; and Radiocommunications Act 1992 (Cth) for example. CIOT providers are not defined carriers or carriage services so are not

and international trade instrument implications.<sup>1951</sup> Many of these are flagged as issues are discussed, and are important topics for future work, such as that underway by the Australian IOT Alliance;<sup>1952</sup> and

- **Competition policy** issues arise given the emerging CIOT-dominance of companies such as Apple, Google, Microsoft and Samsung. While fascinating, this is particularly complex to assess at this early stage of market development.

The paper also does not discuss the following areas, many of which absent government intervention or technical evolution, will impact CIOT delivery and impose consumer access constraints:

- **Internet capacity:** the IOT will add significantly to consumer demand, through the connection of billions of networked devices. This steep demand escalation, combined with the interconnected nature of internet architecture and physical spectrum limits, threatens future congestion and other management issues.
- **General technical issues:** Network neutrality, wider network access (increased connection points in more widespread locations, IPv6; spectrum management; etc.) are all salient issues well-ventilated by the Communications Alliance Report.<sup>1953</sup>
- **IOT (technical) standards** are necessary to ensure that connected devices ‘talk’ to each other; that is, exhibit interoperability and interconnectivity. While discussed broadly if consumers are misled or to exemplify takeover-related obsolescence, the thesis excludes the currently vexed technical questions surrounding network, communication and sensor standards. Suffice to say the industry are active: numerous international bodies are working on standards,<sup>1954</sup> and reputable private industry consortiums have already developed their own ecosystems and frameworks,<sup>1955</sup> which enables consumers to ‘buy’ interoperable ‘works-with’ devices, although may create lock-in as an ongoing consumer issue, which is briefly discussed.

---

under the telecommunications regime – CIOT communications usually pass over public fixed or cellular networks of mobile carriers. But this may evolve: Baker, above n 776.

<sup>1951</sup> Baker, *Ibid.*

<sup>1952</sup> The author is a member of Working Party 3 as to data and privacy matters.

<sup>1953</sup> Above n 119.

<sup>1954</sup> For example, the Internet Engineering Taskforce (IETF), International Telecommunications Union (ITU) and Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA).

<sup>1955</sup> For example, Thread, Apple HomeKit, Apple HealthKit and the Open Internet Consortium.

- **Other consumer-related issues** such as power consumption costs, environmental implications of device power consumption and sustainability (disposal, lifecycle and the like) are not considered.

#### **A.1.4 Disclaimer**

The author is a lawyer and does not purport to evidence technical expertise in the IOT, consumer IOT or computing or information technology, beyond that of an average Australian consumer. Errors in these areas are intended to be avoided, but may be inevitable.

## A2 Methodology & research design

This thesis employs six main research methods: a desktop literature review, impacts assessments, a framing methodology, theoretical perspectives, validation, risk and solutions scenario verification through selected key stakeholder interviews, author participation in the lead Australian IOT-related group, and doctrinal legal analysis by reference to legislative criteria and international cases.

### A2.1 Background research (Comparative literature review)

A desktop literature review process was undertaken to broadly scope the state of the art as to evaluating the consumer IOT in Australia from 2010- (late) 2016. Due to a paucity of Australian CIOT-specific legal literature, this led to an expanded international review, with selective emphasis upon the United States and the European Union. The search was restricted to English and utilised search terms for IOT literature from science, industry, legal and policy-based fields, including research publications from government, industry, analysts, consumer groups and the specialist and lay media.

The initial review yielded voluminous results so was refined through a *Rapid Evidence Assessment* process<sup>1956</sup> with a focus upon the 'internet of things' (or name variants) and all or any of 'consumer law', 'privacy', 'security', 'regulation', 'policy' and 'ethics', confined to law, peer reviewed articles and selected jurisdictions. The search strategy then followed a simplified *Systematic Literature Search* technique, which included identifying and further refining search terms (and combinations thereof) through sequential variation, based upon refining result outcomes and a review of scholarly and other bibliographies. The process was augmented by a more traditional broad search, especially as to news-related articles online.

Resources reviewed (on an ongoing basis) included:

- Research databases in law (Westlaw, Austlii, Lexis Nexis, Lexology, Google Scholar and Mondaq) and scientific databases such as J-Stor and IEEE;
- Australian government websites were monitored manually throughout 2016;
- Regulator websites such as the ACCC, OAIC, US FTC, *Oftcom* and *Digital Europe* were (where possible) subscribed to and monitored;
- Research bodies such as the Productivity Commission, were also manually monitored;

---

<sup>1956</sup> UK Civil Service, 'What is Rapid Evidence Assessment' (2014 accessed 2 Feb 2016)  
<<http://webarchive.nationalarchives.gov.uk/20140305122816/http://www.civilservice.gov.uk/networks/gsr/resources-and-guidance/rapid-evidence-assessment/what-is>>

- Australian industry IOT-stakeholder websites were also monitored including those of the *Communications Alliance, the Australian IOT Alliance, the ADMA, ACMA, and ACCC Product Recall*;
- International entities were monitored including the US National Security Telecommunications Advisory Committee, the FTC, NTIA, EPIC, UK's Ofcom, the European *Research Cluster of the Internet of Things* and *Working Party 29*, and the (EU) Alliance IOT;
- Submissions to relevant Australian enquiries were reviewed;
- Leading Australian law firm sites, such as those of G+T, as well as industry analysts such as Deloitte and Accenture, and consumer bodies such as the US Consumer Reports, the EU's BUEC and Australia's CHOICE were monitored; and
- *Google* was also used as a search back-up.

Given the rapidly evolving and technical nature of the CIOT, the technical media and lay media were monitored through web searches, online email-subscribed updates and direct searches for articles of relevance, including in *WIRED, Mashable, and ComputerWorld*. Lay media CIOT articles were searched weekly using the leading online news resources.

The systematic review process generated the thesis bibliography of approximately 1500 documents.<sup>1957</sup>

## **A2.2 Framing method**

Consistent with other IOT studies,<sup>1958</sup> it was necessary to examine the “self and co-regulatory nature of IOT governance”,<sup>1959</sup> as well as formal regulation. The study was thus framed using a stakeholder analysis to identify key IOT entities including both formal<sup>1960</sup> and informal<sup>1961</sup> regulatory groupings (**Annex. B2**).

In analysing stakeholder literature, policy positions and (where applicable) ‘soft law’ instruments,<sup>1962</sup> it was necessary to consider it:

- may or may not fulfil public policy objectives where stakeholders have competing or conflicting purposes;

---

<sup>1957</sup> The thesis was delayed months into 2017 to await various Australian enquiries and reports; as such it contains those selective updates which also appear in the bibliography.

<sup>1958</sup> EC, above n 52.

<sup>1959</sup> *Ibid.*

<sup>1960</sup> For example, government, regulators, standards bodies, etc.

<sup>1961</sup> For example, industry groups, lobbyists, alliances, etc.

<sup>1962</sup> For example, non-mandatory standards, codes of practice, etc.

- may devise solutions which serve other overriding (for example, industry-based) objectives or may be designed to (tactically) avoid imposed regulation;
- may rely upon members' voluntary, self-audited, "self-interested" participation and compliance behaviours, which may lack the authority, resources and effectiveness of formal regulatory interventions;
- may lack exclusive power and so compete, overlap or collaborate with other entities; and
- may be shaped by political or other institutional power influences.

As such, the research was framed to analyse the literature and to understand the stakeholders' market role and to interpret the likely influences upon them, within the IOT policy landscape.

### **A2.3 Theoretical perspectives**

The thesis uses a range of theoretical perspectives to liberate ideas as to CIOT public policy approaches. It employs a 'reform-oriented' research approach,<sup>1963</sup> that is, it intensively evaluates existing rule adequacy and recommends changes to better achieve certain legal or policy objectives. To establish those objectives, it adapts the Australian Consumer Policy Framework,<sup>1964</sup> to analyse whether the CIOT presents public policy issues requiring regulatory solutions.

The thesis also utilises selected multi-disciplinary theoretical frameworks to analyse certain aspects of Australian law and public policy relevant to the CIOT. These include:

- the normative approaches to Australian consumer policy gleaned from the Australian Government companion guide to the OECD Consumer Policy Toolkit;<sup>1965</sup>
- aspects of behavioural economic theory to enhance the Ch. 5 analysis; and
- regulatory policy options are considered drawing upon the precautionary principle, privacy/security by design, Thierer's 'permissionless innovation', and command and control versus alliance or self-regulatory theories.

The thesis concludes by employing a principles-based regulatory approach,<sup>1966</sup> in attempting to identify certain broadly-accepted norms to promote fundamental consumer protective obligations relevant to the consumer IOT.

---

<sup>1963</sup> Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' *Deakin Law Review* 17: 1 (2012) <https://ojs.deakin.edu.au/index.php/dlr/article/view/70>

<sup>1964</sup> Australian Government, above n 501.

<sup>1965</sup> Australian Government, above n 501.

<sup>1966</sup> J Black, above n 1788, cited at ALRC, above n 1480: 'Regulating Privacy'.

## **A2.4 Additional validation**

A series of unstructured interviews were conducted by telephone and email with experts in a range of fields and from a range of organisations. The interviewees were derived from selected key stakeholders, and are identified in the **Introduction**.

## **A2.5 Legal analysis**

This research strategy was complemented by using legal profession doctrinal research methods.<sup>1967</sup> An analysis of relevant Australian consumer and privacy legislation and case law, was undertaken within the context of the political and institutional enforcement practices, to locate possible CIOT 'gaps'. This included reviewing cases from federal and state courts and statutory-based enforcement actions of the ACCC and OAIC, and determinations of the Privacy Commissioner. Further, international CIOT product 'defect' case reports (some un-litigated) were used to evidence key CIOT problem themes, through a snapshot of smart cars, homes and self.

Identified CIOT issues are analysed and linked to the known body of Australian consumer, privacy and contract law.<sup>1968</sup> This informed an analysis of unfair contract terms law and privacy laws, to illustrate potentially infringing terms and privacy statement attributes. CIOT-related recall activity was also evaluated to assess (largely) software-based product issues in Australia.

In summary, an overview of Australian legislation relevant to the CIOT, together with its application to CIOT cases and risk scenarios (identified by mostly international cases and examples) is provided. Gaps or potential deficiencies in the law are identified. Related international jurisprudence or policy approaches that may be of relevance to Australia or of use in assessing its policy options, is discussed and evaluated where relevant.

## **A2.6 Impact assessment**

Non-quantitative impacts were assessed using analyses drawn from the scholarly literature and the ACPF, consultation with expert interviewees and expert industry literature.

Absent examples of clear consumer detriment in Australia, this assessment is largely subjective insofar as it assesses 'potential' impacts. However, its strength is bolstered by utilising international examples to project those potential Australian issues and impacts, and by interview findings. Those interviews

---

<sup>1967</sup> This term may be defined as a systematic exposition of the normative rules and principles governing consumer law as a legal category, analysing the relationship between rules, explaining areas of difficulty ('gaps') and predicting future developments: Dennis Pearce, Enid Campbell and Don Harding, 'Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission', AGPS, 1987 ('Pearse Committee') cited in Terry Hutchinson, *Researching and Writing the Law* (Reuters Thomson, 3<sup>rd</sup> ed, 2010): 7.

<sup>1968</sup> Terry Hutchinson, above n 1963: 113.

confirmed research findings of a lack of Australian federal policy, differing state-related actions, and a general lack of Australian research, consumer education or other engagement with respect to CIOT issues as at 2016.

### **A3. Conclusion**

In summary, this research is extensive in a rapidly-developing area. Its contents relate to the consumer IOT generally, the challenges it presents, its costs and benefits and how these are to be appraised, together with related issues such as big data, privacy, security, consumer 'consent' and regulation, and all relevant Australian governmental and industry reports, and selected international offerings. Utilising the research framework above, the thesis provides a discussion of key CIOT problems and risks in Australia, extant Australian legislative approaches, gap assessment and potential regulatory options to enhance consumer protection in a CIOT context, together with a narrative summary of the political and public policy environment, and recommended approaches, including draft CIOT policy principles to address the key issues identified.

Unless references reveal otherwise, the research as presented is accurate to 2016 end.

## Annexure B Background

### B1 Literature review

*"When we look overseas ... it is utterly evident that they are more advanced in their IOT narrative and strategy than we are. You can read it, you can see it, and here you don't read about it... There is nothing..."<sup>1969</sup>*

An Australian CIOT literature and policy review supports this contention. Aside from excellent but non-CIOT specific work into the internet,<sup>1970</sup> 3D printing,<sup>1971</sup> privacy<sup>1972</sup>, talent analytics,<sup>1973</sup> drones,<sup>1974</sup> big data<sup>1975</sup> and consumer regulation,<sup>1976</sup> Australian legal research, reports and scholarly articles on this topic are few.<sup>1977</sup> Fortunately, 2016 has seen several scholarly articles and multiple potentially-related enquiries emerge, as well as the first signs of regulatory interest in a topic which has engaged overseas regulators for some years. However, there remains no other scholarly consideration of how Australian consumer protection laws respond to the CIOT at present. This thesis seeks to help fill that gap.

European legal research into the internet of things is voluminous, and its policy work, world leading. United States regulators are playing a rapid catch-up since 2014, while Australian literature has only just emerged in 2016.<sup>1978</sup> It seems probable that factors such as CIOT inexperience, definitional difficulties and genuine uncertainties as to scope and content, as well as a slower purchase and implementation rate, few (if any) practical complaints and no litigation, together with lesser mainstream media interest, and inadequate academic research funding, may form the basis for this temporary vacuum.

---

<sup>1969</sup> Frank Zeichner cited in Stuart Comer, 'Australian government set to tackle the Internet of things' *ZDNet* (21 Aug 2015 accessed 13 Apr 2016) <<http://www.zdnet.com/article/australian-government-set-to-tackle-internet-of-things/>> A Department of Communications website search on 13 April 2016 revealed "no results" for 'internet of things' or variants, other than two externally-uploaded non-government submissions.

<sup>1970</sup> See for example, Forder, above n 148.

<sup>1971</sup> <<http://www.utas.edu.au/law-and-genetics/research-and-projects/3d-printing-research>>

<sup>1972</sup> See for example, a critique of the Privacy Commissioner's weak enforcement practices (which this author has also argued previously): Siganto above n 1529. See also the *SalingerPrivacy* blog: <<https://www.salingerprivacy.com.au/blog/>>

<sup>1973</sup> An analysis of talent analytics (predictive recruiting) recommends that "snapshots, insights ... into the behavioural existence of individuals which can be used for infer predictions of future behaviours" be treated as 'personal information; and should be protected in anti-discrimination law: Burdon, above n 336.

<sup>1974</sup> Des Butler, 'The Dawn of the Age of Drones: An Australian Privacy Law Perspective' 37:2 (2014) UNSWLJ 434- 470 <[http://www.unswlawjournal.unsw.edu.au/sites/default/files/g2\\_butler.pdf](http://www.unswlawjournal.unsw.edu.au/sites/default/files/g2_butler.pdf)> In 2002, Australia was the first country to formally regulate drones for commercial and civilian use, and new reduced-red-tape regulations commence at September 2016.

<sup>1975</sup> M. De Zwart, Sal Humphreys and Beatrix van Dissel, 'Surveillance, Big data and democracy: Lessons for Australia from the US and UK', *University of NSW Law Journal*, (2014) 37:2: 713-747.

<sup>1976</sup> Justin Malbon & Luke Nottage (eds) 'Consumer Law & Policy in Australia & New Zealand', The Federation Press, 2013. The Introduction discusses policy from behavioural economics, rights-based approaches, fairness and social psychology perspectives.

<sup>1977</sup> One interesting IT privacy study of 24 individuals emerged post 2016: above n 1817.

<sup>1978</sup> Australia's major IOT-specific papers include: Communications Alliance, above n 119 and ACMA, 'The Internet of Things and the ACMA's areas of focus: Emerging issues in media and communications' Occasional Paper (Nov 2015 accessed 26 Nov 2015) file:///C:/Users/Kate/Desktop/ACMA%20Internet%20of%20Things\_occasional%20paper%20pdf.pdf> CIOT-specific papers include: Vulkanovski, above n 110; Manwaring, above n 88 and n 836; Leonard, above n 98.

Structurally, this literature review has three sections: Australian work is considered in detail, then a briefer overview is conducted as to the main institutional European Community and United States CIOT literature, and other selected resources. While differing in their approaches, these jurisdictions were considered for reasons of socio- cultural similarity, (some) legal similarity and for their internationally-significant role in IOT policy leadership. Reference is also made to selected Canadian privacy studies which reflect their privacy regulator's international standing.

## **B1.1 Australia**

Categories of literature reviewed are as follows:

- Australian statutes, rules and regulations;
- Government and regulator reports and enquiries;
- Stakeholder submissions to public enquiries, and related materials;
- Peer-reviewed academic journals;
- Private sector and consumer/ privacy body reports;
- Industry analytical or stakeholder reports;
- International case law or (non-litigated) case reports; and
- Specialist and lay media reports.

### *B1.1.1 Scholarly (peer reviewed) Papers*

There are no scholarly legal books and few peer-reviewed journal papers expressly directed toward the consumer IOT in Australia as at late 2016. Of the few, one disclaims legal analysis, but uses a selective literature review process to consider the extent to which Australia's *Privacy Principles* protect CIOT data from a thematic perspective.<sup>1979</sup> The paper concludes that the Privacy Act will be deficient in ensuring privacy in an CIOT context. Another is a 2015 article by Manwaring and Clarke, which identifies key IOT attributes and proposes a research framework for "eObjects".<sup>1980</sup> The paper identifies the certain core

---

<sup>1979</sup> Caron, above n 1466; and Richardson, above n 1817.

<sup>1980</sup> Manwaring, above n 88.

attributes,<sup>1981</sup> and coupled with a 2015 working paper,<sup>1982</sup> proposes a legal analysis of the socio-technological change and attribute-related harms. This work continues, as does other PhD work on autonomous vehicles (smart cars) at QUT and extensive industry-connected work at UNSW. Queensland state accident liability and criminal laws regarding smart cars have also been studied,<sup>1983</sup> with the conclusion that most laws are adaptable to tackle the issues as to “operation” and “control”, though certain anomalies requiring reform exist. It specifically excludes privacy concerns, which this thesis addresses.

It is important to clarify that there is significant Australian work in related or overlapping areas, but which does not mention the CIOT. While this review excludes scholarly security, discrimination, consent and privacy law papers,<sup>1984</sup> some are analogously used to support various arguments. For example, an Australian (medical) Consent Study<sup>1985</sup> is referenced to identify low prose-literacy levels which implies, even disregarding the ‘signing-without-reading’ problem,<sup>1986</sup> that almost half of Australians may have difficulty in providing informed consent to CIOT data collection and use. This study is cited in chapter 6 to evidence certain contentions from behavioural economics. Similarly, reliance was also placed upon (for example) Australian textbooks such as Miller<sup>1987</sup> and Malbon & Nottage on consumer law<sup>1988</sup> and a 2014 UNSW journal edition on ‘big data’ and privacy featuring respected Australian academic writers. Professor Greenleaf writes that all contributors are “united in pessimism” showing “little enthusiasm for [its] promises ... many concerns about its dangers and shared dismay at the inadequacy of privacy laws to deal with the problems raised by big data, or by surveillance practices.”<sup>1989</sup> This paper largely concurs but in a CIOT context, and in chapter 5, justifies the call for the concerted effort to which Professor Greenleaf refers:

---

<sup>1981</sup> Ibid: 2- 3. These include (technically) volatility and vulnerability, and (functionally), factors such as greater object/ people mobility, changed geographical extent, the rise of contextually-aware and autonomous decision-making technology and the “decreased visibility” of implicit human: computer interaction.

<sup>1982</sup> Manwaring, above n 836.

<sup>1983</sup> Kieran Tranter, ‘The Challenges of Autonomous Motor Vehicles for Queensland Road and Criminal Laws’ 16:2 (2016) *QUT Law Review* 59- 81 < <https://lr.law.qut.edu.au/article/view/626/591>>

<sup>1984</sup> See for example, ALRC, above n 1235; Megan Richardson and Andrew Kenyon, ‘Privacy Online: Reform Beyond Law Reform’ in Normann Witzleb et al (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014); Graham Greenleaf, ‘Is it too late to protect privacy? Pessimism reigns over big data and the law’ *UNSWLJ* (15 Sept 2014 accessed 8 Aug 2016) <<http://newsroom.unsw.edu.au/news/law/it-too-late-protect-privacy-pessimism-reigns-over-big-data-and-law>>; Angela Adrian, ‘Has a digital civil society evolved enough to protect privacy?’ *Alternative Law Journal*, 37:3 (Jul 2012 accessed 2 Mar 2016) 183-185.

<sup>1985</sup> McWhirter above n 1644.

<sup>1986</sup> Michael G. Faure, & Hanneke A. Luth, ‘Behavioural Economics in Unfair Contract Terms: Cautions and Considerations’ *J Consum Policy* (2011) 34:337 358.

<sup>1987</sup> Miller, above n 1071.

<sup>1988</sup> Malbon, above n 1976.

<sup>1989</sup> Greenleaf, above n 1984.

“The prevailing US model of an internet where the user is the product is not necessarily permanent. However, to stop it becoming so, it will take either a second internet bubble to burst, or a concerted effort by the rest of the world to reject privacy-invasive business practices... Neither is impossible, nor likely to occur rapidly.”<sup>1990</sup>

### B1.1.2 Law firm outputs

Searches of law firm article repositories such as *Lexology* revealed only seven brief Australian CIOT-related articles by mid-2016, although these have increased after the NTC Enquiry was announced. All are largely descriptive, ‘newsy’ and reflect overseas client-focussed commentary of similar ilk. There are four more scholarly papers from larger firms: *Baker and McKenzie*<sup>1991</sup> issued a broad overview of various CIOT issues, though with little consumer law analysis. In August, *Clayton Utz* released a specific report as to smart cars, which, reflecting their business client base, identified “... an urgent need to address the issue of a legal framework [citing liability, insurance and federal minimum safety standards] that supports the testing, introduction and safe operation of driverless vehicles”.<sup>1992</sup> In contrast to the many NTC submissions which (without evidence) assert that Australia’s privacy regime is adequate for the smart car future, the Report also warns:

“Given the technology involved, consideration also needs to be given to how the law deals with issues around access to data generated by automated and driverless vehicles, privacy, and of course, the very real concern of cybersecurity.”<sup>1993</sup>

G+T’s Peter Leonard also issued a brief IOT paper in August 2016, dealing with business risk and opportunities, but which also flags greater consumer interest in transparency and data privacy management practices.<sup>1994</sup> Finally, *Minter Ellison* released a cyber security report which outlines best practice compliance approaches, many of which are relevant to the CIOT.<sup>1995</sup>

### B1.1.3 Australian Government Research and Enquiries

There are only two reports referencing the IOT by government or statutory bodies – the ACMA and the Productivity Commission (PC).<sup>1996</sup> In late 2015, ACMA’s 2015 ‘The Internet of Things and the ACMA’s

---

<sup>1990</sup> Ibid: *Foreword*.

<sup>1991</sup> Baker, above n 776; Clayton Utz, above n 1743; Leonard, above n 98.

<sup>1992</sup> Utz, Ibid.

<sup>1993</sup> Ibid.

<sup>1994</sup> Leonard, above n 98.

<sup>1995</sup> Minter Ellison, ‘Perspectives on cyber risk’ (Jan 2016. accessed 10 Mar 2016) <

[http://www.minterellison.com/files/uploads/documents/publications/newsletters/15%200189%20Cyber%20Report\\_Final%20v1.pdf](http://www.minterellison.com/files/uploads/documents/publications/newsletters/15%200189%20Cyber%20Report_Final%20v1.pdf)>

<sup>1996</sup> This excludes technical research reports from CSIRO’s *Data61* collaboration with National ICT Australia.

area of focus<sup>1997</sup> was released, but (perhaps) reflective of low IOT awareness, received only three (brief) industry-based submissions.<sup>1998</sup> In terms of IOT security, the Australian Cyber Security Centre's 2015 'Threat Report'<sup>1999</sup> cited the IOT as a new risk factor and part of escalating critical infrastructure threats; a factor potentially addressable though not mentioned, in the Commonwealth's *Cyber-Security Strategy 2016*.<sup>2000</sup>

There are no government enquiries, research or papers, explicitly considering the IOT by Terms of Reference. Two are important as to consumer protection: the ACL review<sup>2001</sup> focussed upon ACL legal efficacy, the extent to which it satisfies the National Consumer Policy Framework and most relevantly, "...the flexibility of the ACL to respond to new and emerging issues to ensure that it remains relevant into the future as the overarching consumer policy framework in Australia".<sup>2002</sup> Few submissions mentioned CIOT issues at all, and none comprehensively.<sup>2003</sup> The complementary PC review titled 'Consumer Law Enforcement and Administration' is also to (inter alia) report on overseas models seeking improvements to ensure Australian consumer protection remains "...flexible and responsive in addressing new and emerging issues".<sup>2004</sup> CAANZ reported in December 2016 and the PC, in April 2017, and those reports were reviewed for this thesis, although neither contained CIOT-specific recommendations.

In 2016, the following potentially CIOT- relevant enquiries were announced:

Entity	Enquiry	Papers	Dates
National Transport Commission	<i>Regulatory Options for Automated vehicles (smart car enquiry)</i>	Issues Paper	Feb 2016
		Discussion Paper	May 2016
		Draft Report due	Nov 2016
		Final report	April 2017

<sup>1997</sup> ACMA, above n 1978.

<sup>1998</sup> Of these, two were from Telstra and NBN Co., both urged resolution of technical (spectrum) issues and little (or no) comment as to CIOT issues.

<sup>1999</sup> ACSC, above n 559.

<sup>2000</sup> Australian Government, above n 316.

<sup>2001</sup> Intergovernmental Agreement for the Australian Consumer Law (IGA), 2 Jul 2009 provides for a CAANZ review after 7 years.

<sup>2002</sup> Above n 496.

<sup>2003</sup> Submissions closed in June 2016, and 180 were publicly available in late August: very few deal with the IOT or with the question of "future threats".

<sup>2004</sup> Scott Morrison & Kelly O'Dwyer, 'Productivity Commission to examine arrangements supporting Australian Consumer Law' (29 Apr 2016 accessed 3 May 2-16) <<http://kmo.ministers.treasury.gov.au/media-release/048-2016/>>; Productivity Commission, *Consumer Law Enforcement and Administration (May 2016)* <<http://www.pc.gov.au/inquiries/current/consumer-law/terms-of-reference>>

Consumer Affairs Australia and New Zealand	<i>Australian Consumer Law Review</i>	Issues Paper Interim report Final report	May 2016 Dec 2016 March 2017
Productivity Commission (PC)	<i>Digital disruption: What do government's need to do?</i>	Research Paper (self-initiated)	June 2016
PC	<i>Consumer Law Enforcement and Administration</i>	Issues Paper Submissions Draft Report Final Report	15 July 2016 30 Aug 2016 Nov 2016 Mar 2017
PC	<i>Data Availability and Use</i>	Issues Paper Draft Report Report	18 Apr 2016 Nov 2016 Mar 2017
House of Representatives Standing Committee	<i>Social Issues relating to Land-based Driverless Vehicles in Australia</i>	Submissions	June 2017

Table B1.1 Australian enquiries 2015- 7

Source: author

Other than those concerning smart cars, the only enquiry to reference the IOT is the PC's concluded *Digital Disruption Report*,<sup>2005</sup> and then, in an infrastructure or manufacturing context.<sup>2006</sup> It refers to vehicle telematics and its relation to the IOT briefly, and *Case Study E* references transport technologies, but overall, the report does not identify or analyse CIOT issues. That may reflect the research purpose and methodology: it was informed by government and industry roundtables only, so the critical economic question identified by the Chair is left unanswered:

*"... whether the current economic lassitude is primarily a delay before the onset of significant social and economic changes driven by digital disruption; **whether government policies (or lack of them) might themselves be frustrating the realization of the benefits**; or whether the effects of this disruption are less fundamental than initially thought."*<sup>2007</sup> [author emphasis]

<sup>2005</sup> PC, above n 680.

<sup>2006</sup> See passing references at pages 14, 16, 25, 39, 58, 103, 119, 163. Page 164 cites an IOT definition; others relate to size, standards, interconnectivity, security and improved monitoring capacity of the industrial IOT.

<sup>2007</sup> PC, above n 680 Foreword.

While labelling Australian government as “reactive” to digital technologies and Australians, as “unremarkable” adopters, the Chair pointedly disclaims the Report findings’ accuracy, saying: “...absence of conjecture in this space would be both timid and unhelpful to the development of a productivity policy agenda.”<sup>2008</sup> He concludes (beyond scope):

**Broader protections for an individual's rights** (such as with control of personal information) and **to support society's moral and ethical mores** (relevant to ...artificial intelligence, remote sensing...) will require ongoing government attention...<sup>2009</sup> [author emphasis]

In framing the consumer IOT policy discussion, the 2011 Australian Government ‘companion’<sup>2010</sup> was used, which adopts the more detailed OECD Toolkit<sup>2011</sup> and outlines policy review process, assessing “consumer detriment” and regulatory policy<sup>2012</sup> (**Annex C**). Together with specific OECD recommendations<sup>2013</sup> and the behavioural economics articles discussed below, these papers provided the framework to consider the CIOT from a policy perspective.

#### *B1.1.4 Industry groups*

The *Communications Alliance* aims to be the leading ICT-industry initiative shaping the CIOT regulatory framework and released a comprehensive 2015 report entitled ‘Enabling the Internet of Things for Australia’. It is a very useful overview resource and makes numerous recommendations from a (predominantly) industry or technical perspective. ADMA have also produced its ‘2016 Regulatory Landscape’<sup>2014</sup> which briefly addresses IOT data use in an advertising context. In February 2016, the ACCAN released an entertaining 2016 intern’s paper on the CIOT which is the first Australian report to scope the potential issues, but is largely descriptive and does not undertake legal analysis.<sup>2015</sup> As such, a ‘gap’ in the literature remains.

#### *B1.1.5 Regulators*

---

<sup>2008</sup> Ibid.

<sup>2009</sup> Ibid.

<sup>2010</sup> Australian Government, above n 499.

<sup>2011</sup> OECD, above n 505.

<sup>2012</sup> Lunn, above n 1659.

<sup>2013</sup> OECD, above n 523.

<sup>2014</sup> Association for Data-driven Advertising and Marketing, ‘2016 Regulatory Landscape’ (1 Mar 2016 accessed 2 Mar 2016) <<http://www.adma.com.au/comply/regulatory-newsletter/2016-regulatory-landscape/>>

<sup>2015</sup> Vulkanovski, above n 110.

The *Australian Competition and Consumer Commission* (ACCC) has no explicit CIOT policy, but will continue to “concentrate on emerging systemic issues”<sup>2016</sup> in the online marketplace.<sup>2017</sup> There is no explicit reference to the CIOT, but absent consumer complaints or obvious detriment, this seems justifiable. The author found the Deputy Chair very concerned about the topic and it seems likely that the ACCC is monitoring overseas developments.

The *Office of the Australian Information Commissioner* (OAIC) has produced little on the IOT,<sup>2018</sup> despite significant international regulator interest since (at least) 2014.<sup>2019</sup> In September 2016, it participated in a Global Privacy Enforcement Network sweep of 314 CIOT devices internationally. The OAIC examined 45 fitness and health monitors, thermostats and smart travel locks and found that 71% of them “did not adequately explain how privacy is managed”.<sup>2020</sup> The OAIC cautioned that businesses should adopt privacy-by-design practices to protect personal information and promised resources to help start-ups “shortly”.<sup>2021</sup> The Privacy Commissioner has previously foreshadowed guidance as to big data, data de-identification and the IOT within the 2016-17 financial year, but its zeal may be dampened by the recent *Grubb*<sup>2022</sup> metadata decision, which is arguably suggestive of the courts taking a narrow approach to defining “personal information” unresponsive to modern technology, nor reflective of broader European and other international approaches. Further while greater OAIC action would be privacy positive, the regulator must overcome its apparent reluctance to take proactive regulatory action, which would influence its efficacy and industry compliance practices in a CIOT (and many other) contexts.<sup>2023</sup>

---

<sup>2016</sup> Corporate plan or priorities 2015- 2016.

<sup>2017</sup> ACCC, ‘ACCC and AER Corporate Plan 2015- 16’ <<https://www.accc.gov.au/publications/corporate-plan-priorities/corporate-plan-priorities-2015-16>> This includes examining sharing economy regulation and promoting informed consumer purchasing through big data (e.g. by comparator tools).

<sup>2018</sup> The OAIC has released a data breach guide: above n 577. An OAIC website search reveals only a passing mention of IOT in Privacy Commissioner speeches.

<sup>2019</sup> ICPEN, above n 736.

<sup>2020</sup> Office of the Privacy Commissioner of Canada, ‘Global Internet of Things Sweep finds connected devices fall short on privacy’ News Release (22 Sept 2016 accessed 23 Sept 2016) <[https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/nr-c\\_160922/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/nr-c_160922/)>

<sup>2021</sup> OAIC, ‘Privacy shortcomings of Internet of Things businesses revealed’ *OAIC News* (23 Sept 2016 accessed 25 Sept 2016) <<https://www.oaic.gov.au/media-and-speeches/news/privacy-shortcomings-of-internet-of-things-businesses-revealed>> Oddly the author was told the OAIC does not have a “position” on the IOT yet. Note that the promised materials were not released as at April 2017.

<sup>2022</sup> The original determination: *Ben Grubb v Telstra Corporation Limited* [2015] AICmr 35 went to the AAT on appeal by Telstra and was then unsuccessfully appealed by the Privacy Commissioner in January 2016.

<sup>2023</sup> The author has criticised the OAIC in this regard as to online behavioural advertising: above n 185; as have others: Siganto, above n 1529. Note however that the OAIC experienced several years of budgetary and organisational uncertainty due to government decisions. However, its press release did not suggest it was taking any action after the Sweep.

### B1.1.6 *Private Sector Analysis*

Australian-specific CIOT analytics reports are few. Telsyte,<sup>2024</sup> has produced several market reports, covering smart home, smart selves (wearables) and consumer digital, which assert a positive picture as to increased Australian interest and adoption practices. Others may be commercially available, but were not accessible to the author. Other valuable resources used are (mostly) international private-sector research or white papers, marketing documents and statistical and predictive research, discussed below.

## B1.2 International materials

This section considers *selected* international literature, with a focus upon the OECD, EU, UK, Canada and the USA. This was undertaken to augment the Australian literature search, choosing jurisdictions or organisations with a similarity in consumer law provisions,<sup>2025</sup> and/ or public policy positioning, and with similar types of consumer issues to be addressed.

International group reports such as the OECD on consumer policy and UN as to its consumer protection guidelines<sup>2026</sup> and privacy<sup>2027</sup> were also considered. An April 2016 Consumers International report<sup>2028</sup> provides a comprehensive international analysis of CIOT and foreshadows broad regulatory issues, and as such, is the first of its kind internationally and a valuable contribution to the literature.

Literature produced by regulators as to the IOT has been extensive in the EU since (at least) 2008, and since 2014, is growing in the US. The IOT is policy-ingrained in the EU *Digital Agenda for Europe 2020* and coordinated high quality research occurs via the *European Research Cluster of the Internet of Things*,<sup>2029</sup> and the independent *Article 29 Data Protection Working Party (WP29)*.<sup>2030</sup> Reports cover all

---

<sup>2024</sup> Telsyte, above n 300; Telsyte, 'Cut through: how the Internet of things is sharpening Australia's competitive edge' (Feb 2015 accessed 17 Mar 2016) <[http://mscorpnews.blob.core.windows.net/ncmedia/2015/02/Microsoft\\_IoT\\_Whitepaper.pdf](http://mscorpnews.blob.core.windows.net/ncmedia/2015/02/Microsoft_IoT_Whitepaper.pdf)>

<sup>2025</sup> Corones, above n 845.

<sup>2026</sup> United Nations, 'Guidelines on Consumer Protection' Resolution 70/186 on Consumer Protection, adopted by the General Assembly on 22 December 2015 (2015 accessed 26 Jun 2016) <[http://unctad.org/meetings/en/SessionalDocuments/ares70d186\\_en.pdf](http://unctad.org/meetings/en/SessionalDocuments/ares70d186_en.pdf)>

<sup>2027</sup> United Nations Human Rights Council, 'The right to privacy in the digital age' *Report of the Office of the United Nations High Commissioner for Human Rights* (30 Jun 2014 accessed 13 Apr 2016) [http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37\\_en.pdf](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf)

<sup>2028</sup> Above n 44.

<sup>2029</sup> For example, as to the IOT, see Ian G Smith et al (eds), 'The Internet of Things 2012 New Horizons' *Internet of Things European Research Cluster* <[http://www.internet-of-things-research.eu/pdf/IERC\\_Cluster\\_Book\\_2012\\_WEB.pdf](http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf)> There are many other papers also here: <http://www.internet-of-things-research.eu/>

<sup>2030</sup> There is a plethora of other EU materials, which perhaps reflects the long-standing EU commitment to digitisation, data protection and to consumer privacy – all of which are amplified in the IOT context.

IOT aspects, with a global implementation view: including technical, public policy, industrial and consumer issues and the data economy. Selected recent reports considered include the Cluster's 'Internet of Things' (2013),<sup>2031</sup> the Rand policy options report (2015),<sup>2032</sup> 'IOT opportunities and challenges' (2015),<sup>2033</sup> and 'Opinion 8/ 2014'<sup>2034</sup> - all of which evaluate the policy complexities and seek solutions respectful of European values. WP29's Opinion also sought to locate "high level" protections against the "many privacy and security challenges" presented by the IOT.<sup>2035</sup> In the UK, national strategy, initiatives and financial support<sup>2036</sup> for IOT development and realisation followed the excellent 2014 *Blackett Report*<sup>2037</sup> and OFCOM's 2015 enquiry.<sup>2038</sup> In the US, NSTAC's 2014 Presidential Report<sup>2039</sup> warned of a convergence, if not "collision", between IT and IOT, with resulting governance and security implications, and urged policy action warning that time to influence IOT governance was short. The FTC has been especially active since that time: conducting a CIOT workshop,<sup>2040</sup> issuing a Staff Report<sup>2041</sup> and industry guidance, entitled 'Careful Connections Building Security into the Internet of Things'.<sup>2042</sup> Since then, US government enquiries and related testimony have accelerated, including relevantly:

- US Senate *Committee* "The Connected World: Examining the Internet of Things"<sup>2043</sup> (Feb 2015);
- House of Representatives *Committee*, 'IOT hearing'<sup>2044</sup> (Mar 2015);
- Senate IOT resolution passed (23 June 2015);<sup>2045</sup>

---

<sup>2031</sup> Above n 103.

<sup>2032</sup> EC, above n 52.

<sup>2033</sup> European Parliamentary Research Service, 'The Internet of things: opportunities and challenges' (May 2015 accessed 2 Jan 2016) [http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS\\_BRI\(2015\)557012\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf)

<sup>2034</sup> EU, above n 103. (Art 29)

<sup>2035</sup> Ibid.

<sup>2036</sup> IOTUK has set aside £40 million (AUD83million) in an 'integrated' three-year programme seeking to advance the UK as a global IOT leader and to increase technology and service adoption in both business and the public sector. In January 2016, the PETRAS Consortium, set up nine universities to work on significant IOT issues such as ethics, privacy, trust, security, acceptability, and reliability.

<sup>2037</sup> Above n 19. (Blackett Review)

<sup>2038</sup> OFCOM, 'Promoting investment and innovation in the Internet of Things: Summary of responses and next steps' (27 Jan 2015 accessed 23 Feb 2016) <<http://stakeholders.ofcom.org.uk/binaries/consultations/IOT/statement/IOTStatement.pdf>>

<sup>2039</sup> NSTAC, above n 66.

<sup>2040</sup> FTC, above n 449.

<sup>2041</sup> Ibid.

<sup>2042</sup> FTC, above n 118; FTC, 'Start with Security: A Guide for Business' <[https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business?utm\\_source=govdelivery](https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business?utm_source=govdelivery)>

<sup>2043</sup> US Senate Committee of Commerce, Science and Transportation 'The Connected World: Examining the Internet of Things' (11 Feb 2015 accessed 7 Mar 2016) <<http://www.commerce.senate.gov/public/index.cfm/2015/2/the-connected-world-examining-the-internet-of-things>>

<sup>2044</sup> United States House of Representatives, Committee on Energy and Commerce, 'Examining Ways to Improve Vehicle and Roadway Safety' *Commerce, Manufacturing, and Trade Sub-Committee* (114th Congress) (21 Oct 2015 accessed 29 May 2016) < <https://energycommerce.house.gov/hearings-and-votes/hearings/examining-ways-improve-vehicle-and-roadway-safety>>

<sup>2045</sup> Senator Deb Fischer, 'Senate passes 'The Internet of Things' Resolution' (24 May 2015 accessed 3 Jun 2016) < [http://www.fischer.senate.gov/public/\\_cache/files/6c5693ae-dc0c-448b-ae9a-12e2eb154804/internet-of-things-bill-](http://www.fischer.senate.gov/public/_cache/files/6c5693ae-dc0c-448b-ae9a-12e2eb154804/internet-of-things-bill-)

- Senators' GAO request to study interoperability and other IOT standards;<sup>2046</sup>
- House of Representatives, *Subcommittee* hearing on the challenges facing the Internet of Things,<sup>2047</sup> (29 Jul 2015);
- NTIA on "the benefits challenges and potential roles for government in fostering the advancement of the Internet of Things' (April 2016); and 2017 green paper.<sup>2048</sup>

These resulted in testimony, reports and other literature, adding to available IOT materials, including the Markey Report as to smart cars.<sup>2049</sup> Similarly, The Canadian Privacy Commissioner has released several excellent studies providing stern warnings as to adverse privacy implications of smart cars,<sup>2050</sup> smart self<sup>2051</sup> and smart home devices,<sup>2052</sup> which are very useful in the case study context.

Non-governmental groups producing relevant high quality reports, include the *IEEE*,<sup>2053</sup> the Internet Society,<sup>2054</sup> and the International Telecommunications Union.<sup>2055</sup> Interestingly, the literature is also enhanced by groups such as 'I Am the Cavalry',<sup>2056</sup> 'BuildITSecurely'<sup>2057</sup> and other expert volunteer initiatives. DEFCON have also highlighted CIOT security issues through widely-publicised "white hat" hacking,<sup>2058</sup> which has informed manufacturers and consumers of apparently latent vulnerabilities, but

---

language.pdf> Note the resolution refers to consumers only as empowered by the CIOT and as recipients of cost savings. It does not mention consumer protection.

<sup>2046</sup> United States Government Accountability Office, (GAO) 'Intelligent transportation Systems: vehicle-to-vehicle technologies Expected to offer Safety benefits, but a Variety of Deployment challenges exist' GAO-14-13, Report to congressional requesters <<http://www.gao.gov/products/GAO-14-13> >

<sup>2047</sup> US Subcommittee on Courts, Intellectual Property, and the Internet, 'IOT Hearing - U.S. House of Representatives Judiciary Committee' (29 Jul 2015 accessed 3 Mar 2016) < [http://judiciary.house.gov/\\_cache/files/5378eb3d-fc2a-48e6-b45d-0a7ff050ec3d/114-38-95686.pdf](http://judiciary.house.gov/_cache/files/5378eb3d-fc2a-48e6-b45d-0a7ff050ec3d/114-38-95686.pdf)>

<sup>2048</sup> NTIA, above n 48.

<sup>2049</sup> Edward Markey, "Tracking and Hacking: Security and Privacy Gaps Put American Drivers at Risk' (Feb 2015 accessed 16 Mar 2016) < [http://www.markey.senate.gov/imo/media/doc/2015-02-06\\_MarkeyReport-Tracking\\_Hacking\\_CarSecurity%202.pdf](http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf)>

<sup>2050</sup> Lawson, above n 36.

<sup>2051</sup> Hilts, above n 204; Canada, above n 340.

<sup>2052</sup> Canadian Privacy Commission, 'An introduction to privacy issues with a focus on the retail and home environments', *Research paper prepared by the Policy and Research Group* (February 2016 accessed 16 Aug 2016) < [https://www.priv.gc.ca/media/1808/IOT\\_201602\\_e.pdf](https://www.priv.gc.ca/media/1808/IOT_201602_e.pdf)>

<sup>2053</sup> IEEE, above n 87.

<sup>2054</sup> ISOC, above n 10.

<sup>2055</sup> ITU, above n 175.

<sup>2056</sup> It corroborated to produce: Atlantic Council, above n 211.

<sup>2057</sup> BuildITSecurely, 'Our Goals for the Internet of things' (n.d. accessed 7 Apr 2016) <<https://builditsecure.ly/>>

<sup>2058</sup> DEFCON is one of the oldest annual hacking conventions. See Daron Pauli, 'DEFCON 23 to host Internet of Things Slaughterfest' *The Register* (6 May 2015 accessed 3 Mar 2016) <[http://www.theregister.co.uk/2015/05/06/defcon\\_23\\_to\\_host\\_internet\\_of\\_things\\_slaughterfest/](http://www.theregister.co.uk/2015/05/06/defcon_23_to_host_internet_of_things_slaughterfest/)>; and Anderson, above n 391.

also provided the technical information and alert for regulator prosecutions, such as the first smart home case, *ASUSTek*.<sup>2059</sup>

There is a plethora of high quality research-based, private-industry reports, most of which support the view that the CIOT has enormous potential for social and economic benefit, but also carries consumer costs which require resolution. Starting with McKinsey's oft-cited 2015 report, 'The Internet of things: Mapping the Hype',<sup>2060</sup> other lengthy and scholarly reports of value include (for example) Lux Research (2015),<sup>2061</sup> Accenture Digital/ Fjord's 'The Era of Living Services' (2015),<sup>2062</sup> Verizon (2016)<sup>2063</sup> - all of which tackle hard questions as to the nature of the potentially adverse consumer impacts. Symantec,<sup>2064</sup> GSMA<sup>2065</sup> and others authoritatively report on security vulnerabilities. Research reports also reveal some serious adverse implications for consumers:<sup>2066</sup> for example, Acquity Group<sup>2067</sup> has reported negative survey results as to consumer trust. Cisco and Intel,<sup>2068</sup> as potentially major IOT suppliers, has also produced a range of largely pro-enablement reports, suiting their marketing focus,<sup>2069</sup> whereas Intel have taken a pro-policy approach.<sup>2070</sup> In terms of market analytics, Gartner,<sup>2071</sup> ABI research,<sup>2072</sup> Statista<sup>2073</sup>

---

<sup>2059</sup> File No. 142 3456, Agreement containing Consent Order (26 Feb 2016) <<https://www.ftc.gov/system/files/documents/cases/160222asusagree.pdf>>

<sup>2060</sup> McKinsey, above n 22.

<sup>2061</sup> Lux, above n 26.

<sup>2062</sup> Accenture, above n 24.

<sup>2063</sup> Verizon, above n 312.

<sup>2064</sup> M. Barcena, & Candid Wueest, 'Insecurity in the Internet of Things' *Symantec* (12 Mar 2015 accessed 23 Mar 2016) <[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/insecurity-in-the-internet-of-things.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/insecurity-in-the-internet-of-things.pdf)>

<sup>2065</sup> GSMA, above n 583; and above n 113.

<sup>2066</sup> See Accenture, above n 1.

<sup>2067</sup> Acquity, above n 46.

<sup>2068</sup> Intel, 'Internet of Things (IoT) Policy (n.d. accessed 2016) <http://www.intel.com/content/www/us/en/policy/policy-internet-of-things-iot.html>; Intel, 'Policy framework for the Internet of things (IoT)' (2014 accessed 2 Jan 2016) <<http://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-iot-framework.pdf>>; Intel, 'The Internet of things (IoT) and Automotive and Transport Policy Principles' (2014 accessed 2 Jan 2016) <<http://www.intel.com/content/www/us/en/policy/policy-iot-automotive-transportation.html>>

<sup>2069</sup> See for example, Cisco, above n 98; 13 and 106.

<sup>2070</sup> Intel, above n 2068.

<sup>2071</sup> Gartner, 'Gartner Says Worldwide IOT Security Spending to Reach \$348 Million in 2016' (25 Apr 2016 accessed 30 Apr 2016) <<http://www.gartner.com/newsroom/id/3291817>> ; Gartner, 'Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015' Press Release (11 Nov 2014 accessed 5 Mar 2016) <http://www.gartner.com/newsroom/id/2905717>; Gartner, "Gartner Says Worldwide Wearable Devices Sales to Grow 18.4 Percent in 2016" Press Release (2 Feb 2016 accessed 29 Mar 2016) <<http://www.gartner.com/newsroom/id/3198018>>; Gartner, above n 273.

<sup>2072</sup> For example: ABI Research, 'The Internet of Things will drive Wireless Connected devices to 40.9 Billion in 2020' Press Release (20 Aug 2014 accessed 26 Mar 2016) <https://www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect/>; ABI, above n 275.

<sup>2073</sup> For example: Statista, above n 273; Statista, 'Projected size of the global connected car market in 2016 and 2021, by segment (in billion euros)' (2016 accessed 20 Jun 2016) <http://www.statista.com/statistics/297816/connected-car-market-size-by-segment/>; Statista, above n 276; Statista, 'Percentage of car customers in selected countries willing to share connected car data as of August 2015, by country and application type' (2016 accessed 20 Jun 2016) <http://www.statista.com/statistics/256157/drivers-willing-to-share-connected-car-data-with-oems-and-dealers/>

and others provide exponential projections with varying assumptions, although Accenture's recent analysis suggests that the IOT market is not growing sufficiently to meet many of these.<sup>2074</sup>

In the US, scholarly legal articles as to CIOT (alone) as distinct from the IOT remain relatively few. In 2014, FTC Commissioner Julie Brill has published several articles<sup>2075</sup> which are a valuable contribution to the CIOT privacy discussion, and spawned articles from two fellow commissioners contesting her precautionary principle approach.<sup>2076</sup> Adam Thierer has also written extensively and thoughtfully on CIOT regulatory policy, privacy and security, from a pro-innovation or "permissionless innovation" perspective.<sup>2077</sup> In 2015, Scott Peppet published a now widely-cited article as to the CIOT, which he describes as the "first [US CIOT] legal work"<sup>2078</sup> and addresses CIOT discrimination, privacy, security and consent issues. He suggests that it continues the initiation of "...a conversation that is already overdue".<sup>2079</sup> Other US academic literature, as to general privacy, security, product liability and the difficult legal questions surrounding (for example) smart cars is voluminous and often context-specific,<sup>2080</sup> so is consulted very selectively, with a focus upon practical case studies.<sup>2081</sup> There are also several UK articles of relevance to smart homes and privacy terms by Walden et al,<sup>2082</sup> which were also consulted.

Research for specific chapters has also involved selected literature as to the case studies,<sup>2083</sup> regulatory approaches and behavioural economics (BE), which is foundational to the OECD consumer policy toolkit, as well as useful in understanding why informed consent in an CIOT context is highly problematic.

---

<sup>2074</sup> Accenture, above n 427.

<sup>2075</sup> Brill, above n 446.

<sup>2076</sup> Maureen K. Ohlhausen, 'The Internet of Things and the FTC: Does Innovation Require Intervention?' *Remarks before the US Chamber of Commerce* (18 Oct 2013 accessed 1 Mar 2016) <

<http://www.ftc.gov/speeches/ohlhausen/130725section5speech.pdf>>; FTC, 'How to Regulate the Internet of Things Without Harming its Future: Some Do's and Don'ts', *Remarks of Joshua D Wright, Commissioner FTC at the US Chamber of Commerce* (21 May 2015 accessed 2 Jan 2015) <

[https://www.ftc.gov/system/files/documents/public\\_statements/644381/150521IOTchamber.pdf](https://www.ftc.gov/system/files/documents/public_statements/644381/150521IOTchamber.pdf)>

<sup>2077</sup> See for example Thierer, above n 161.

<sup>2078</sup> Peppet, above n 283. There are older articles of peripheral relevance cited in Manwaring, above n 88: 587 [footnote 8].

<sup>2079</sup> Peppet, above n 283: 96.

<sup>2080</sup> See for example, the bibliographies of Tranter, above n 73; Adam Thierer & Ryan Hagemann, 'Removing Roadblocks to Intelligent Vehicles and Driverless Cars' *Mercatus Center* (17 Sept 2014 accessed 3 Mar 2016) <

<http://mercatus.org/sites/default/files/Thierer-Intelligent-Vehicles.pdf>>

<sup>2081</sup> As to smart cars: Thierer, *Ibid*; Brendan Gogarty and Meredith Hagger, 'The Laws of Man Over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air' (2008) 19 *Journal of Law, Information and Science* 73, 124–32; Muhammad Usman Iqbal and Samsung Lim, 'Privacy Implications of Automated GPS Tracking and Profiling' (2010) 29 *Technology and Society Magazine*, IEEE 39; Nick Belay, 'Robot Ethics and Self-Driving Cars: How Ethical Determinations in Software Will Require a New Legal Framework' (2015) 40 *Journal of the Legal Profession* 119.

<sup>2082</sup> La Diega, above n 328.

<sup>2083</sup> Atlantic Council, above n 211; Morley Strengers, Nichols & Hazas, 'The hidden cost of smart homes' (13 Jun 2016 accessed 23 Jun 2016) *The Conversation* <<http://theconversation.com/the-hidden-energy-cost-of-smart-homes-60306>>; Ibrahim, above n 334; IEEE, 'Wearfit: Security Design Analysis of a Wearable Fitness Tracker' (2016 accessed 29 Apr 2016) <http://www.computer.org/cms/CYBSI/docs/Wearfit.pdf>; Hilts, above n 204; Anderson, above n 391; Mark Rechlin, 'Early build Tesla Models face quality issues' *ConsumerReports* (19 Apr 2016 accessed 21 Apr 2016) <<http://www.consumerreports.org/tesla/tesla-model-x-quality-issues/>>

Explanatory materials such as the *OECD Toolkit* and articles explaining the policy influence of BE on the policy were reviewed,<sup>2084</sup> together with more general economics articles as to consumer law,<sup>2085</sup> privacy<sup>2086</sup> and those finding flaws with 'notice and choice' such as Friedman,<sup>2087</sup> and Hoofnagle, using a transaction cost economics analysis.<sup>2088</sup> BE analyses as to unfair contract terms<sup>2089</sup> were all also useful and include Bailey's 2016 article as to IOT 'privacy-trading'.<sup>2090</sup>

Finally, preparing the draft principles required consideration of a broad range of recommendations. Taking the security context alone, that included analyses of 'security by design',<sup>2091</sup> the OTA 'IOT Trust framework' (2016)<sup>2092</sup> creating a human centred IOT<sup>2093</sup> and its early 2017 revision, as well as approaches proposed by government bodies such as the FTC,<sup>2094</sup> NIST,<sup>2095</sup> NHTSA,<sup>2096</sup> DOT,<sup>2097</sup> GSMA<sup>2098</sup> and the FBI;<sup>2099</sup> industry offerings;<sup>2100</sup> as well as private groups such as OWASP,<sup>2101</sup> the EWF,<sup>2102</sup> OTA,<sup>2103</sup> I Am the Calvary,<sup>2104</sup> research papers;<sup>2105</sup> security update practices,<sup>2106</sup> academic contributions<sup>2107</sup> and so on.

---

<sup>2084</sup> Lunn, above n 1659; Maria Lissowska, 'Overview of Behavioural Economics Elements in the OECD Consumer Policy Toolkit' 34 *J Consum Policy* (2011): 393- 398;

<sup>2085</sup> Alain Samson (ed), *The Behavioural Guide*, behaviouraleconomics.com (2016 accessed 16 Apr 2016); Hans-W. Micklitz, Lucia A. Reisch and Kornelia Hagen, An Introduction to the Special Issue on "Behavioural Economics, Consumer Policy, and Consumer Law" *Journal of Consumer Policy* (September 2011) 34(3): 271-276.

<sup>2086</sup> Acquisti, above n 579.

<sup>2087</sup> David Adam Friedman, 'Free Offers: A New Look' (2008) 38 *N.M. L. Rev.* 49.

<sup>2088</sup> Whittington, above n 55.

<sup>2089</sup> Bar-Gill, above n 51; Faure, above n 1986.

<sup>2090</sup> Bailey, above n 51.

<sup>2091</sup> Cavoukian, above n 1319; Deloitte, 'Privacy by Design: setting a new standard for privacy certification' <<https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF>>; Louise Taylor, 'Privacy by design – essential for the growth of the Internet of Things?' *Taylor Wessing* (Feb 2014 accessed 19 Nov 2015) <[http://united-kingdom.taylorwessing.com/download/article\\_privacy\\_design.html](http://united-kingdom.taylorwessing.com/download/article_privacy_design.html)>

<sup>2092</sup> OTA, above n 1857.

<sup>2093</sup> EU, above n 49.

<sup>2094</sup> FTC, above n 2042.

<sup>2095</sup> NIST, above n 587.

<sup>2096</sup> Above n 399. (Best practices).

<sup>2097</sup> DOT, above n 716.

<sup>2098</sup> GSMA, above n 113.

<sup>2099</sup> FBI, above n 554.

<sup>2100</sup> Auto Alliance, above n 399; ADMA, 'Best Practice Guideline: Big Data' (2013 accessed 2 Jan 2016) <<https://www.adma.com.au/sites/default/files/Big%20Data%20Best%20Practice%20Guidelines%20%5BADMA%202013%5D.pdf>>

<sup>2101</sup> OWASP above n 558.

<sup>2102</sup> Alta, above n 1224.

<sup>2103</sup> OTA, 'Diffusing-the-IoT-Time-Bomb-Security-and-Privacy Trust Code of Conduct' (3 Jan 2016 accessed 3 Mar 2016) (RSAC 2016 Deck from Panel Session) <[https://otalliance.org/system/files/initiative/documents/ast2-w02-diffusing-the-iot-time-bomb-security-and-privacy\\_trust\\_code\\_of\\_conduct\\_v3.pdf](https://otalliance.org/system/files/initiative/documents/ast2-w02-diffusing-the-iot-time-bomb-security-and-privacy_trust_code_of_conduct_v3.pdf)>

<sup>2104</sup> Above n 586.

<sup>2105</sup> Above n 1692.

<sup>2106</sup> FTC, above n 138, 139 and 2042.

<sup>2107</sup> Daniel Castro and Joshua New, '10 Policy Principles for Unlocking the Potential of the Internet of things' *Information Technology and Innovation Foundation* (4 Dec 2014 accessed 2 Jan 2016) <<http://www2.datainnovation.org/2014-IOT-policy-principles.pdf>>

### B1.3 Case law

There is no explicitly CIOT-related case in Australia,<sup>2108</sup> although the ACCC has instituted proceedings against Volkswagen, Audi and SKODA over its (alleged) diesel emissions software fraud and a related private class action has commenced.<sup>2109</sup> These cases arguably illustrate a smart car case or at least, an example of how manufacturers may leverage information asymmetry, lack transparency and deceive consumers by product complexity and (latent) software. There are also of course, several OAIC cases of note in relation to data security, but few cases of direct relevance. ASIC approaches to directors' duty to address cybersecurity,<sup>2110</sup> perhaps presage potential ACCC action in this area; which in turn would reflect relatively recent FTC cases focussing upon security as a compliance obligation.<sup>2111</sup>

In the US, there are a range of IOT-relevant cases: the first so-called CIOT case concerned security. *TRENDnet*,<sup>2112</sup> involved internet-connected SecurView cameras sold for smart home security and baby monitor purposes – but which used defective software enabling hackers to post nearly 700 live feeds on the internet. Another recent FTC settlement is *AsusTek Computer Inc. (2016)*<sup>2113</sup> in which ASUS were alleged to have failed to secure its home routers and cloud service, such that thousands were compromised, smart homes became hackable and consumers suffered detriments including disclosure of personal information, financial fraud and identity theft. The case also illustrates inadequate security by design, and flawed post-sales service - Asus failed to react to defect warnings and to provide timely software updates as well.

Others are at class action stage, such as *Cahen*,<sup>2114</sup> alleging that smart cars are hackable, and *McLellan* arguing that fitness devices are inaccurate;<sup>2115</sup> but both are meeting defences that no detriment has been shown entitling redress, which raises the US *Spokeo* question as to “injury in fact”,<sup>2116</sup> and for Australians, the question of whether IOT device accuracy or security flaws alone – without more, such as false representation – is actionable at law. Other potential examples of consumer detriment are found in formal

---

<sup>2108</sup> IOT is not a commonly-used court-room term so cases are not readily searchable. The author has searched the main manufacturers as defendants, as well as a range of smart device names, permutations and combinations.

<sup>2109</sup> ACCC, 'ACCC takes action against Volkswagen over diesel emission claims' *Press Release* (1 Sept 2016 accessed 4 Sept 2016) < <https://www.accc.gov.au/media-release/accc-takes-action-against-volkswagen-over-diesel-emission-claims>>

<sup>2110</sup>The Australian Securities and Investments Commission (ASIC) considers board participation important to a strong cyber resilience culture, and that director/ officer failure to manage cyber risks may be disqualifying: ASIC, *Cyber resilience: Health Check' Report No. 429* (Mar 2015 accessed 4 Jan 2016) < <http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf>>

<sup>2111</sup> ASIC's approach reflects *FTC V Wyndham*, above n 656.

<sup>2112</sup> *TRENDnet*, above n 629.

<sup>2113</sup> *ASUSTek*, above n 635.

<sup>2114</sup> *Cahen* above n 688.

<sup>2115</sup> *McLellan*, above n 898.

<sup>2116</sup> *Spokeo v Robins*, 136 S.Ct. 1540 (2016)

requests for FTC investigation filed by groups such as EPIC, which include Samsung's smart TV which allegedly 'eavesdrops' on consumers in their smart homes.<sup>2117</sup>

There are a range of other data breach cases which propose obligations to secure data, including *Wyndham*,<sup>2118</sup> together with numerous data breach examples, many of which affected Australians – including the *Home Depot* (50 million credit cards) and *Target* cases (40 million credit card numbers and 70 million customer's data) and the recent *Yahoo* case (half a billion email addresses). There are also cases concerning data brokers on-selling data without consumer authorisation,<sup>2119</sup> and undisclosed online tracking,<sup>2120</sup> which have analogous relevance to CIOT. Others concern unauthorised data collection: for example, *Path*<sup>2121</sup> involved an app which collected data from mobile phone address books without consent – which has obvious implications for any CIOT device.

There are also a wide range of media-reported issues and hacks, which are cited to illustrate alleged smart car, home or self device defects, and to illustrate potential sources of consumer detriment. Novel studies undertaken by the author include a hypothetical adaption of the 2016 Tesla fatality, a review of selected terms from an unfair contract terms perspective, a review of software recalls in Australia, and a review of the Nestle Milo kid's fitness band app v1.0, using the Australian privacy regime.

## **Conclusion: Literature Review**

This literature review captures the state of Australian CIOT research, cases and materials as to consumer laws as at 2016 end. It does not capture the vast array of international research, reports and many articles which discuss the IOT in non-consumer specific contexts. Rather it identifies the main reports and those which more holistically consider the CIOT from a legal perspective. In summary, at this point, while the EU has a comprehensive research framework and strategy, it seems that the US is playing a rapid catch-up as to its regulatory and public policy position, while Australian policy work is really, just starting out.

---

<sup>2117</sup> *In the Matter of Samsung Electronics Co. Ltd.*, Complaint, Request for Investigation, Injunction and Other Relief Submitted by the Electronic Privacy Information Center, Case, (24 Feb 2015 accessed 10 May 2016) <<https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf>> Note this allegation is supported by Wikileaks' 2016 dump as to CIA hacking capacities.

<sup>2118</sup> *Wyndham*, above n 656.

<sup>2119</sup> *FTC v. Sitemsearch Corporation, Doing Business as LeapLab, et al* (United States District Court for the District of Arizona, Phoenix Division) FTC Matter/ File No: 142 3192 (23 Dec 2014) <<https://www.ftc.gov/system/files/documents/cases/141223leaplabcmt.pdf>>

<sup>2120</sup> *In the Matter of ScanScout Inc.*, No. C-4344 (F.T.C. Matter/ File No. 102 3185 (21 Dec 2011) <<https://www.ftc.gov/enforcement/cases-proceedings/102-3185/scanscout-inc-matter>>

<sup>2121</sup> *United States of America v Path, Inc.* FTC Matter/ File No. 122 3158 (1 Feb 2013) <<https://www.ftc.gov/enforcement/casesproceedings/122-3158/path-inc>>

## B2 Key stakeholder identification

### B2.1 Key sectoral players

Consumer IOT stakeholders were identified to map the key Australian IOT players, as well as current and potential regulatory or governance bodies. Selected key international stakeholders and regulatory or governance bodies were also searched to facilitate comparative literature analysis.

<p><b>Australia</b>          Australian Communications Media Authority          Australian Communications Consumer Action Network          Australian Competition and Consumer Commission          Australian Cyber Security Centre          Austroads &amp; state roads bodies          Association for Data-driven Advertising and Marketing          Australian Federal Police          ALRC          CAF (Legislative and Governance Forum on Consumer Affairs)          CHOICE          Commonwealth Consumer Affairs Advisory Council          Consumer Affairs Australia and New Zealand          (Former) Department of Broadband Communications &amp; the Digital Economy          Department of Communications and the Arts          Department of Prime Minister and Cabinet          Federal Chamber of Automotive Industries (FCAI)          Insurance Council of Australia          Law Council of New South Wales          National Transport Commission          Office of the Australian Information Commissioner (OAIC)          Productivity Commission          State Motoring Clubs (RACV, RACQ, NRMA etc.)          State and Territory governments</p>	<p><b>Private sector research/ analysts/ industry entities</b>          ABI Research          Accenture Digital          Acquity Group          Alliance of Automobile Manufacturers Inc          Association of Global Automakers, Inc          Automotive information Sharing and Analysis Center (Auto-ISAC)          Baker &amp; McKenzie          CEDA          Clayton Utz          Center for Data Innovation          Cisco          Communications Alliance          Davies Collison Cave          Deloitte          DLA Piper          EY          Ferrier Hodgson          Fortinet          Gartner          G+T          Griffith Hack          Hewlett Packard          IBM Institute          IDC          IDG          IEEE          Intel          IOTUK          ISACA          Lloyds  <i>King &amp; Wood Mallesons</i>  <i>McKinsey</i>  <i>Mason Hayes and Curran</i>          Online Trust Alliance          OWASP (Open Web Application Security Project)          Oxford Economics          Philips Fox          Privacy Impact Assessment Project          Rand Corporation          SAE International          Stuart Corner, IOT Alliance website          Sweeney Research</p>
<p><b>Canada</b>          Canadian Privacy Commission</p>	
<p><b>Europe (EU)/ International other</b>          Commission for the Protection of Privacy (BE)          Consumers International          Director-General for Internal Policies          European Commission          European Commission Article 29 Working Group          European Court of Human Rights          European Data Protection Commissioner          European Research Cluster on the Internet of Things          European Union Agency for Network and Information Security (ENISA)          Europol</p>	

GSMA (Groupe Spécial Mobile) IEEE Computer Society International Consumer Protection and Enforcement network (ICPEN) International Telecommunications Union (ITU) OECD The Internet Society (ISOC) United Nations Human Rights Council	SYMANTEC Taylor Wessing Telsyte Verizon Verto Analytics Wilson Elser
<b>United States</b> Consumer Federation of America Consumer Reports [US] EPIC - Electronic Privacy Information Center Executive Office of the President Federal Bureau of Investigation (FBI) Federal Communications Commission (FCC) Federal Trade Commission Department of Commerce Department of Transportation International Transport Forum (US) National Safety Council (NSC) National Highway Traffic Safety Administration (NHTSA) National Institute of Standards and Technology (NIST) National Security Telecommunications Advisory Committee (NSTAC) National Telecommunications Information Administration (NTIA) National Transport Safety Board US Chamber of Commerce Foundation United States Government Accountability Office (GAO) United States Senate <i>Committee on Commerce, Science and Transportation</i> United States House of Representatives, <i>Committee on Energy and Commerce</i>	<b>United Kingdom</b> Competition and Markets Authority Dept of Business, Innovation and Skills Information Commissioner's Office OFCOM

Table B2.1 Key sectoral players  
Source: author

## B2.2 Key Australian IOT stakeholders

Table B2.2 below represents a non-exhaustive, high-level overview of the principal Australian entities relevant to IOT regulation, together with consumer and industry group stakeholders. It identifies their role, work and relationship to other bodies in the IOT ecosystem.

Public Sector	Regulatory role or other objective	IOT Objectives	Relationships
Australian Communications Media Authority	Regulator Licensing Research	Telecommunications Spectrum Devices (smart TVs) Consumer protection (communications)	Impacts retail residential or wholesale business consumers, and telecommunications industry groups and government
Australian Competition and Consumer Commission	Regulator Strategy Education	IOT consumer protection IOT consumer product safety Promote competition and education	Independent Cth statutory authority engages across consumers, industry, government and representative bodies
Austrroads & state roads bodies	Policy development Research (ARRB) Guides	Smart car enablement C-ITS planning Infrastructure development Transport system management	Represents Australasian (govt) road transport and traffic agencies.
Australian Government  Department of Communications and the Arts	National Policy Regulatory Statutory legislation (e.g. privacy, consumer law)	No public IOT policy Innovation economy policy Open government data policy ? permissionless innovation approach	National and international, industry and consumer liaison
Consumer Affairs Forum (Legislative and Governance Forum on Consumer Affairs)	Policy Regulatory strategy	Consumer protection law implementation Strengthen consumer protection framework Education and information Compliance and dispute resolution National product safety consistency	Commonwealth, State, Territory and New Zealand Ministers responsible for fair trading and consumer protection laws
National Transport Commission	Policy Research	Smart car promotion Regulatory strategy for testing Promote IOT for productivity and efficiency	Independent statutory inter-governmental

	Implementation Planning		agency reporting to Transport & Infrastructure Council
Office of the Australian Information Commissioner (OAIC)	Regulator Strategy Dispute resolution	None known IOT position will be consistent with the Privacy Act 1988 (Cth)	Independent Cth statutory authority engages across consumers, industry, government and representative bodies
Productivity Commission	Public inquiries Research studies Self-initiated research Annual reports Competitive neutrality complaints	No IOT-specific policy or research Digital Disruption (self-initiated) (2015) Data availability and Use Inquiry (2016) Consumer Law Enforcement and Administration Review (2016)	Advice and research for government and public policy purposes
State and territory governments	Policy Regulatory Statutory legislation (e.g. road laws as to smart car testing)	Various approaches	National and international, industry and consumer liaison
<b>CONSUMER GROUPS</b>	<b>Regulatory role or other objective</b>	<b>IOT Objectives</b>	<b>Relationships</b>
Australian Communications Consumer Action Network	Advocacy Policy Research	Focus on goods and services in the internet, telecommunications, broadcasting, online services	Liaises with govt to promote interests of individuals, small businesses and not-for-profits to policy makers. Funded by statutory scheme.
CHOICE	Product testing/ review Consumer advocacy Investigation	IOT product testing/ reviews Consumer advocacy to government Consumer complaints	Not for profit with consumer membership, consumer bodies, industry and government
Consumers' Federation of Australia	Advocacy Policy Standards inputs	Consumer policy	Consumer organisations body liaises across consumer

			groups, industry, government and internationally
<b>INDUSTRY GROUPS</b>	<b>Regulatory role or other objective</b>	<b>IOT Objectives</b>	<b>Relationships</b>
IOT Alliance Australia	Advocacy Policy development Regulatory recommendations Lobbying	IOT acceleration, promotion, enablement Promoting enabling evidence-based policy and regulation Promoting government action for enablement	Cross business, industry, academic, business and government liaison – OAIC and ACCC observer status
Association for Data-driven Advertising and Marketing	Soft-law regulator (Codes) Lobbying Education	Promotes data-driven advertising/ marketing Data security and privacy	Industry body liaises with members, industry and government
Communications Alliance	Policy Advocacy	Represents all IOT players IOT growth Consumer interests Promotes soft law self-governance	Powerful consumer industry advocacy and policy body - liaises across all sectors
Federal Chamber of Automotive Industries (FCAI)	Policy Industry advocacy	Facilitate introduction of C-ITS and autonomous vehicle testing in Australia.	Represents companies wholly owned by global manufacturers - liaison government and consumer groups
Insurance Council of Australia	Policy Advocate Soft law regulator (Codes of Practice)		Insurance industry representative liaised with government and consumer groups
<b>OTHER</b>	<b>Regulatory role or other objective</b>	<b>IOT Objectives</b>	<b>Relationships</b>
Standards Australia	Peak non-government national standards body	Responsible for standards (if any) pertaining to IOT devices – for example under the Motor Vehicle Standards Act (Cth)	Cooperative MOU with the ACCC
<b>OTHER: CANADA</b>	<b>Regulatory role or other objective</b>	<b>IOT Objectives</b>	<b>Relationships</b>

Canadian Privacy Commission	Regulator	IOT privacy and data security	Government, industry and consumer
<b>OTHER: EUROPE</b>	<b>Regulatory role or other objective</b>	<b>IOT Objectives</b>	<b>Relationships</b>
BEUC the European consumer organisation  (Bureau Européen des Unions de Consommateurs)	Consumer protection	Consumer policy review Consumer protection	Influential EU-funded, consists of 43 independent national consumer organisations from 31 European countries.
European Commission	Promotional Regulatory Statutory legislation (privacy, etc.)	Rapid advance to stimulate economy Relationships national and international	Promotes cooperative work of member States, EU and globally
European Data Protection Commissioner	Monitoring Privacy policy Independent EU authority	Data protection Privacy IOT policy guidance  <a href="https://secure.edps.europa.eu/EDPSWEB/edps/EDPS">https://secure.edps.europa.eu/EDPSWEB/edps/EDPS</a>	Influential; works with EU institutions, Member States, non EU countries and other national or international organisations.
European Research Cluster on the Internet of Things (Art 29 WP)	Independent Advisory Opinions/ recommendations	IOT impacts on data  <a href="http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm">http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm</a>	Works across EU states, authorities and with an EC representative
European Union Agency for Network and Information Security (ENISA)	Recommendations Policy-making	IOT security Privacy Network and information security	Works with member States & private sector
ITU-T	Regulation standards	Working groups technical)	Works with tech bodies internationally
National EU member states	Regulatory	Rapid advance to stimulate economy Relationship with EC and states	Rule makers for State market
<b>OTHER: USA</b>			
Consumer Reports	Product testing/ review Consumer advocacy	IOT product testing/ reviews Consumer advocacy to government Consumer complaints	Liaises with govt to promote interests of individuals, small

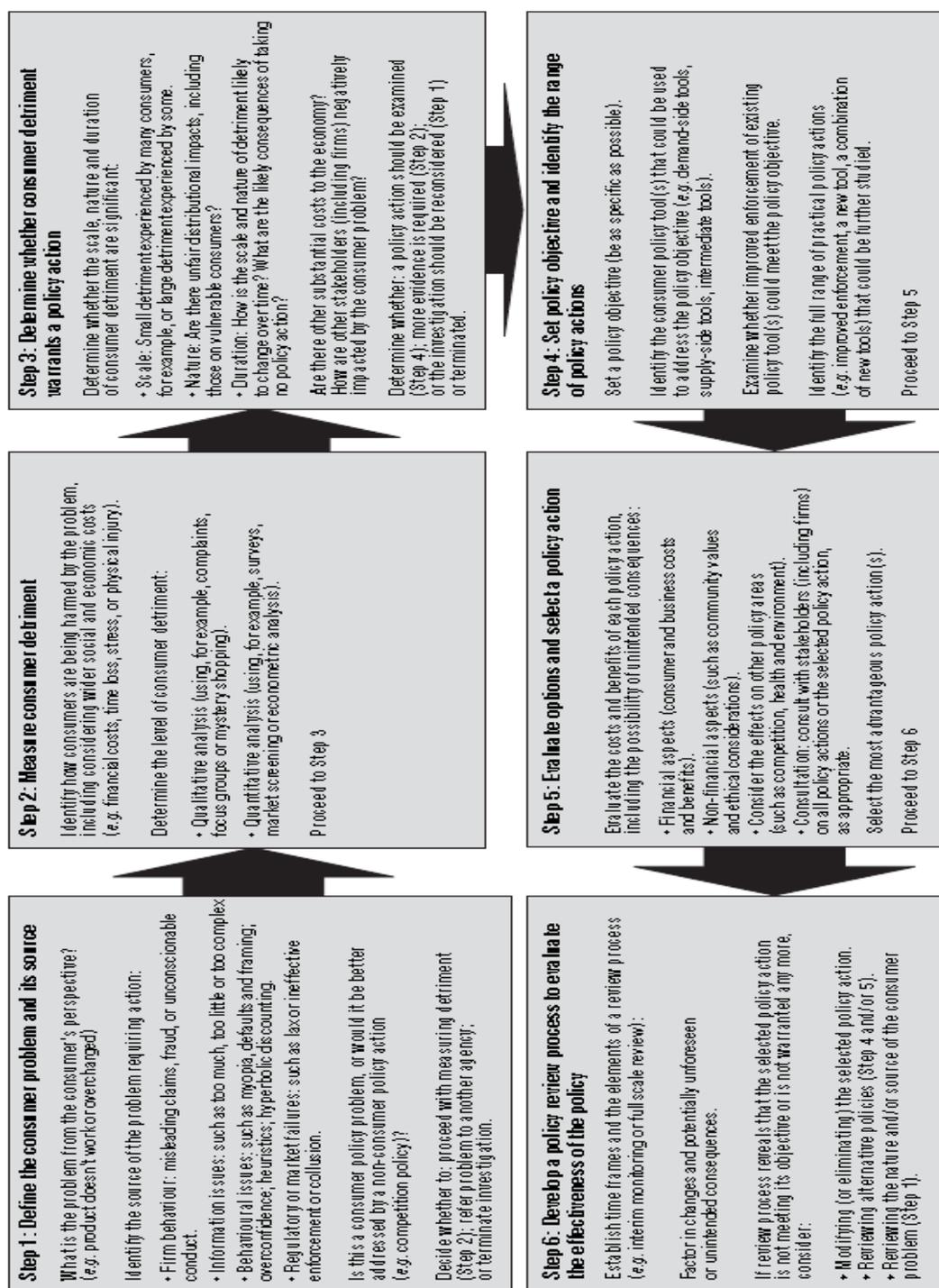
	Investigation		businesses and not-for-profits to policy makers.
Federal Communications Commission	Regulator – spectrum, ISP privacy	Internal US policy-maker Positions may influence other states	Works with all entities
Federal Trade Commission	Independent administrative agency Regulator Educator	Consumer protection incl. privacy and data security Competition regulation Consumer choice and education	Works with consumer, government and private sector
NHTSA, US Department of Transport	Promotional Regulator	Safety performance standards Investigator Researches traffic safety and driver behaviour Consumer information	Works with industry and government and consumers
Department of Commerce, National Telecommunications and Information Administration (NTIA)	Executive adviser Policy maker	Telecommunications adviser Information policy adviser Promotes internet access, spectrum & internet growth and innovation	Executive branch agency Advises president Works across agencies

Table B2.2 Key IOT stakeholders  
Source: author

# Annexure C Consumer policy diagrams

## C1 OECD Consumer Policy Toolkit process

Figure 5.1. Consumer policy making steps



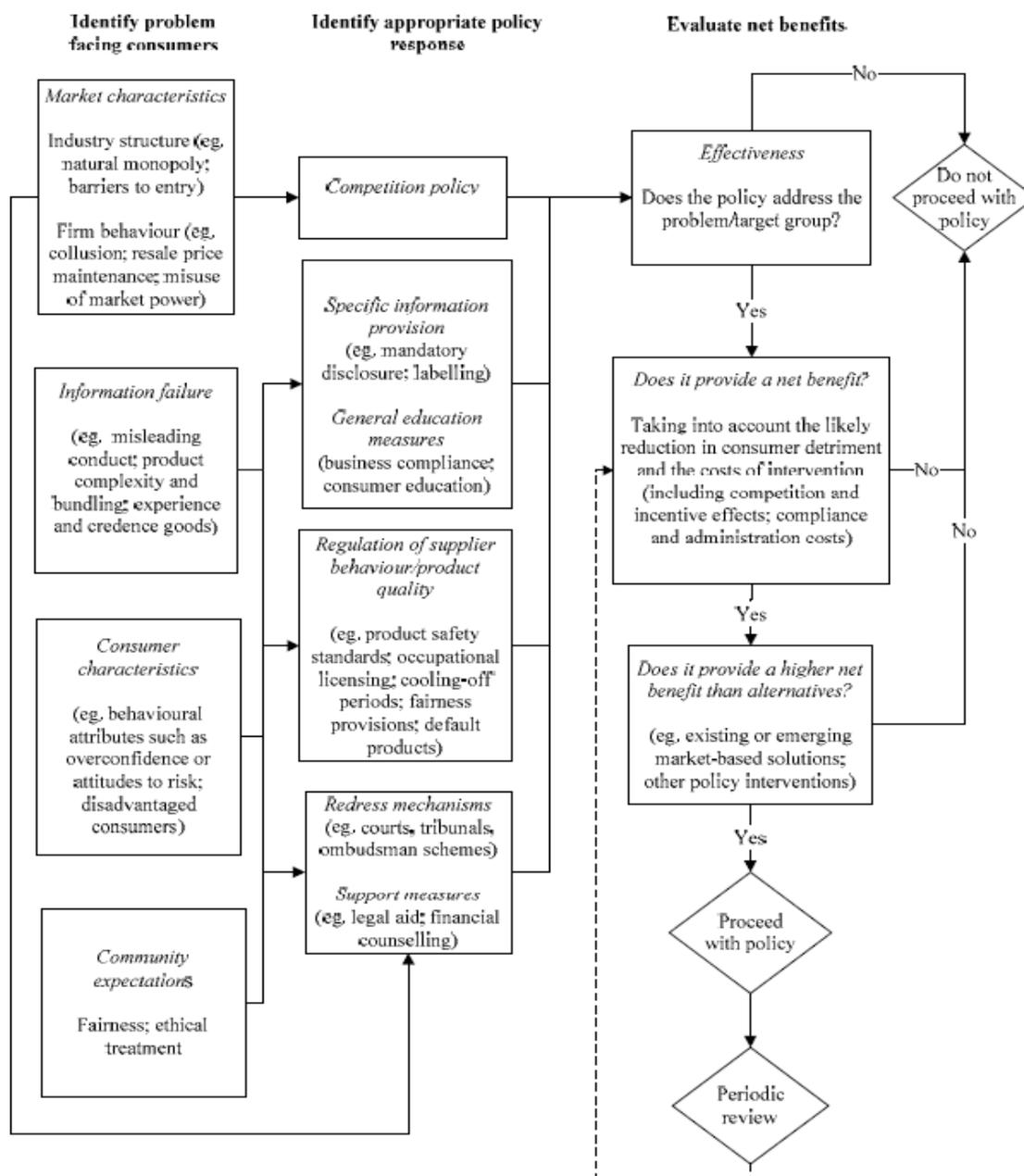
Graphic C1.1 Consumer policy making steps

Source: OECD<sup>2122</sup>

<sup>2122</sup> Above n 505. Licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 IGO (CC BY-NC-SA 3.0 IGO) licence.

## C2 Productivity Commission Policy Flowchart

Figure 3.1 Identifying and evaluating policy instruments



Graphic C1.2 Identifying and evaluating policy instruments

Source: OECD<sup>2123</sup> Licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 IGO (CC BY-NC-SA 3.0 IGO) licence.

<sup>2123</sup> PC, above n 531.

## Annexure D OTA & OWASP consumer guidance

### D1 Online Trust Alliance CIOT Consumer Checklist



## Enhancing the Security, Privacy & Safety of Connected Devices



Addressing cyber threats, identity theft and personal safety risks	
<input type="checkbox"/>	Inventory all devices within your home and workplace that are connected to the Internet and network. Router reports can help determine what devices are connected to your network. Disable unknown and unused devices.
<input type="checkbox"/>	Contact your Internet Service Provider (ISP) to update routers and modems to the latest security standards. Change your router service set identifier (SSID) to a name which does not identify you, your family or the device.
<input type="checkbox"/>	Check that contact information for all of your devices are up-to-date including an email address regularly used to receive security updates and related notifications.
<input type="checkbox"/>	Confirm devices and their mobile applications are set for automatic updating to help maximize protection. Review their sites for the latest firmware patches and updates.
<input type="checkbox"/>	Review all passwords creating unique passwords and user names for administrative accounts and avoid using the same password for multiple devices. Delete guest codes no longer used. Where possible implement multi-factor authentication to reduce the risk of your accounts being taken over. Such protection helps verify who is trying to access your account—not just someone with your password.
<input type="checkbox"/>	Review the privacy policies and practices of your devices, including data collection and sharing with third parties. Your settings can be inadvertently changed during updates. Reset as appropriate to reflect your preferences.
<input type="checkbox"/>	Review devices' warranty and support policies. If they are no longer supported with patches and updates, disable the device's connectivity or discontinue usage of the device.
<input type="checkbox"/>	Before discarding, returning or selling any device, remove any personal data and reset it to factory settings. Disable the associated online account and delete data.
<input type="checkbox"/>	Review privacy settings on your mobile phone(s) including location tracking, cookies, contact sharing, bluetooth, microphone and other settings. Set all your device and applications to prompt you before turning on and sharing and data.
<input type="checkbox"/>	Back up your files including personal documents and photographs to storage devices that are not permanently connected to the Internet.

<https://otalliance.org/loTconsumer>

R 10-3

Graphic D1.1 Enhancing the Security, Privacy & Safety of Connected Devices  
Source: OTA<sup>2124</sup>

<sup>2124</sup> OTA, above n 1885.

## D2 OTA IOT Trust Framework minimum requirements

No	Title	Description
1	Privacy policy	The privacy policy must be readily available to review prior to product purchase, download or activation and be easily discoverable by the user. Such policies should disclose the consequences of opting in or out of policy elements.
2	Privacy policy reading	Display of the privacy policy should be optimised for the reading device to ensure maximum readability.
3	Disclosure	Manufacturers must conspicuously disclose all personally identifiable data types and attributes collected.
4	Personal data sharing	Default personal data sharing must be limited to third parties who agree to confidentiality and limitation of use.
5	Data retention	The term of data retention should be disclosed.
6	Sanitisation	The manufacturer should provide a means of sanitising devices when they use is discontinued.
7	Encryption	Personal data at rest and in motion must be encrypted using industry best standards.
8	Default password	Default passwords must be changed on first use.

9	SSL <sup>4</sup> best practices	All device sites must adhere to SSL best practices using industry standard testing mechanisms.
10	HTTPS	All device sites and cloud services must employ HTTPS encryption by default.
11	Penetration testing	Manufacturers must conduct penetration testing for devices, applications, and services.
12	Vulnerabilities	Manufacturers must have capabilities to remediate vulnerabilities in a prompt and reliable manner either through remote updates and/or consumer notifications. <sup>5</sup>
13	Data breach	Manufacturers must have an up-to-date breach response plan and consumer safety notification plan.
14	Password recovery	Manufacturers must provide secure recovery mechanisms for passwords.
15	Pairing indicator	Devices must provide a visible indicator when they are pairing with another device.
16	Signed updates	All patches, updates, etc. need to be signed and verified.
17	Profiles	For products and services which collect personal information and are designed to be used by multiple users, manufacturers need to incorporate the ability to create and manage personal profiles and/or have parental controls.
18	Contact	Manufacturers must publish and provide a mechanism for users to contact the company regarding issues including but not limited to the loss of the device, device malfunction, device compromise, etc.
19	Transfer of ownership	Manufacturers must provide a mechanism for transfer of ownership including providing updates for consumer notices and access to documentation and support.
20	Manage privacy	The device must have controls and/or documentation enabling the consumer to set, revise, and manage privacy and security preferences including what information is transmitted via the device.
21	Support	Manufacturers must publish to consumers a time frame for support after the device/app is discontinued or replaced by a newer version.
22	Disabling smart functions	Manufacturers must disclose what functions will work if smart functions are disabled or stopped.
23	Email authentication	Configure all security and privacy related email communications to adopt email authentication protocols.

Graphic D2.1 OTA IOT Trust framework

Source: IOTAA<sup>2125</sup>

<sup>2125</sup> Extract from Australian IOT Alliance, 'IoT Security Guideline V1.0' (Feb 2017 accessed 2 Mar 2017): 17- 18 excluding two technical notes.

## D3 OWASP Consumer IOT Security Guidance

“...The goal of this section is help consumers purchase secure products in the Internet of Things space. The guidance below is at a basic level, ...[but]... will greatly aid the consumer in purchasing a secure IoT product.”

Category	IOT Security Consideration
<b>1: Insecure Web Interface</b>	<ul style="list-style-type: none"> <li>• If your system has the option to use HTTPS, ensure it is enabled</li> <li>• If your system has a two factor authentication option, ensure that it is enabled</li> <li>• If your system has web application firewall option, ensure that it is enabled</li> <li>• If your system has a local or cloud-based web application, ensure that you change the default password to a strong one and if possible change the default username as well</li> <li>• If the system has account lockout functionality, ensure that it is enabled</li> <li>• Consider employing network segmentation technologies such as firewalls to isolate IoT systems from critical IT systems</li> </ul>
<b>2: Insufficient Authentication/ Authorization</b>	<ul style="list-style-type: none"> <li>• If your system has a local or cloud-based web application, ensure that you change the default password to a strong one and if possible change the default username as well</li> <li>• If the system has account lockout functionality, ensure that it is enabled</li> <li>• If the system has the option to require strong passwords, ensure that is enabled</li> <li>• If the system has the option to require new passwords after 90 days for example, ensure that is enabled</li> <li>• If your system has a two factor authentication option, ensure that it is enabled</li> <li>• If your system has the option to set user privileges, consider setting user privileges to the minimal needed for operation</li> <li>• Consider employing network segmentation technologies such as firewalls to isolate IoT systems from critical IT systems</li> </ul>
<b>3: Insecure Network Services</b>	<ul style="list-style-type: none"> <li>• If your system has a firewall option available, enable it and ensure that it can only be accessed from your client systems</li> <li>• Consider employing network segmentation technologies such as firewalls to isolate IoT systems from critical IT systems</li> </ul>
<b>4: Lack of Transport Encryption</b>	<ul style="list-style-type: none"> <li>• If your system has the option to use HTTPS, ensure it is enabled</li> </ul>
<b>5: Privacy Concerns</b>	<ul style="list-style-type: none"> <li>• Do not enter sensitive information into the system that is not absolutely required, e.g. address, DOB, CC, etc.</li> <li>• Deny data collection if it appears to be beyond what is needed for proper operation of the device (If provided the choice)</li> </ul>
<b>6: Insecure Cloud Interface</b>	<ul style="list-style-type: none"> <li>• If your system has the option to use HTTPS, ensure it is enabled</li> <li>• If your system has a two factor authentication option, ensure that it is enabled</li> <li>• If your system has web application firewall option, ensure that it is enabled</li> <li>• If your system has a local or cloud-based web application, ensure that you change the default password to a strong one and if possible change the default username as well</li> <li>• If the system has account lockout functionality, ensure that it is enabled</li> <li>• If the system has the option to require strong passwords, ensure that is enabled</li> </ul>

	<ul style="list-style-type: none"> <li>• If the system has the option to require new passwords after 90 days for example, ensure that is enabled</li> </ul>
<b>7: Insecure Mobile Interface</b>	<ul style="list-style-type: none"> <li>• If the mobile application has the option to require a PIN or password, consider using it for extra security (on client and server)</li> <li>• If the mobile application has the option to use two factory authentication such as Apple's Touch ID, ensure it is enabled</li> <li>• If the system has account lockout functionality, ensure that it is enabled</li> <li>• If the system has the option to require strong passwords, ensure that is enabled</li> <li>• If the system has the option to require new passwords after 90 days for example, ensure that is enabled</li> <li>• Do not enter sensitive information into the mobile application that is not absolutely required, e.g. address, DOB, CC, etc.</li> </ul>
<b>8: Insufficient Security Configurability</b>	<ul style="list-style-type: none"> <li>• If your system has the option, enable any logging functionality for security-related events</li> <li>• If your system has the option, enable any alert and notification functionality for security-related events</li> <li>• If your system has security options for passwords, ensure they are enabled for strong passwords</li> <li>• If your system has security options for encryption, ensure they are set for an accepted standard such as AES-256</li> </ul>
<b>9: Insecure Software/Firmware</b>	<ul style="list-style-type: none"> <li>• If your system has the option to verify updates, ensure it is enabled</li> <li>• If your system has the option to download updates securely, ensure it is enabled</li> <li>• If your system has the ability to schedule updates on a regular cadence, consider enabling it</li> </ul>
<b>10: Poor Physical Security</b>	<ul style="list-style-type: none"> <li>• If your system has the ability to limit administrative capabilities possible by connecting locally, consider enabling that feature</li> <li>• Disable any unused physical ports through the administrative interface</li> </ul>

#### “General Recommendations

If you are looking to purchase a device or system, consider the following recommendations:

- Include security in feature considerations when evaluating a product
- Place Internet of Things devices on a separate network if possible using a firewall

[NOTE: Given the fact that each deployment and every environment is different, it is important to weigh the pros and cons of implementing the advice above before taking each step.]...”

*Graphic D3.1 OWASP Consumer IOT Security Guidance* <sup>2126</sup>

Source: OWASP<sup>2127</sup>

<sup>2126</sup> OWASP, above n 1899.

<sup>2127</sup> All materials in Annex.D3 are licensed by OWASP under Creative Commons 3.0 License:  
[<https://creativecommons.org/licenses/by-sa/3.0/>](https://creativecommons.org/licenses/by-sa/3.0/)

## Annexure E Glossary

<b>app</b>	<b>A software application which operates on a device to fulfil a purpose or function - for example, to provide data analysis of smart self data collected by a smart band.</b>
<b>AI or artificial intelligence*</b>	technology that appears to emulate human performance typically by learning, drawing conclusions, appearing to understand complex content, engaging in natural dialogs with people, enhancing human cognitive performance (also known as cognitive computing) or replacing people on execution of non-routine tasks e.g. voice recognition technologies.
<b>Australian Standard</b>	Specifications, procedures and guidelines, designed to ensure products, services and systems are safe, reliable and consistent. International standards are developed by ISO, IEC, and ITU, and are adopted by Standards Australia if possible. <sup>2128</sup> For example, IT and cybersecurity are covered by ISO 27000 series.
<b>big data</b>	'the practice of combining huge volumes of diversely sourced information and analysing them, often using self-learning algorithms to inform decisions'. <sup>2129</sup>
<b>Bluetooth*</b>	a low-power wireless networking technology
<b>cloud computing*</b>	a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies.
<b>consumer telematics*</b>	end-user-targeted vehicle information and communication technologies and services. Used in smart cars to provide in-vehicle services, such as emergency assistance, Global Positioning System (GPS) navigation, traffic information, local search (e.g. restaurant locations) and manufacturer concierge services.
<b>cyber-attack ('hacking')</b>	any offensive activity designed to obtain unauthorised access to and/ or degrade, damage, disrupt or destroy, or expose vulnerabilities within, IT
<b>cyber security</b>	technical and compliance-based safeguards or actions to protect against cyber-attack and to manage cyber risk.
<b>data breach</b>	the loss of or unauthorised access to data or the modification, disclosure or other misuse or interference of data, (which may contain personal information) and often because of a cyber attack
<b>data broker*</b>	a business that aggregates information from many sources; processes it to enrich, cleanse or analyse it; and (usually) licenses it to other organizations.
<b>data fusion</b>	Collective term to cover all data amalgamation, including data matching, data linking and any other technologies or approaches which merge data and may thereby, generate more personally-identifying information.
<b>data linking</b>	linking identified and anonymous databases to de-anonymise or re-identify anonymous data by identifying data fingerprints, which may often then be linked to other data sets.
<b>data matching</b>	comparing multiple systems of records to aggregate data about an already identified subject.
<b>data portability<sup>^</sup></b>	the ability to move data stored on one IOT/cloud service to another or to download data
<b>device (CIOT)<sup>2130</sup></b>	"... equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing". Examples include a smart watch, TV or car. Note that while smartphones are not generally IOT devices, they become a part of the IOT when they are the 'remote' control for a CIOT system.
<b>hub</b>	a central device that coordinates CIOT devices such as lights, locks etc. to work together, or to be automated as required.
<b>internet of things</b>	See Ch. 1. See also consumer internet of things (CIOT or consumer IOT) in Ch 1.
<b>interoperability<sup>^</sup></b>	the capacity of devices from one manufacturer to work and interact with those of another
<b>IP or Internet Protocol*</b>	Transmission Control Protocol/Internet Protocol (TCP/IP) tracks the address of nodes, routes outgoing messages, and recognizes incoming messages. In smart homes, IP refers to a device sending information using the internet or a computer network.
<b>IPv6*</b>	Internet Protocol version 6 replaces IPv4, and greatly increases IP address space, as required by the IOT.
<b>IT</b>	Information technology, including software, hardware, communications and related services.

<sup>2128</sup> [http://www.standards.org.au/standardsdevelopment/what\\_is\\_a\\_standard/pages/default.aspx](http://www.standards.org.au/standardsdevelopment/what_is_a_standard/pages/default.aspx)

<sup>2129</sup> EDPS, 'Opinion 4/2015 Towards a new digital ethics' (11 Sept 2015 accessed 8 Feb 2016) <  
[https://edps.europa.eu/sites/edp/files/publication/15-09-11\\_data\\_ethics\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf)>

<sup>2130</sup> ITU-T, above n 101.

<b>M2M*</b>	automated data transmission and measurement between mechanical or electronic devices; e.g. CIOT devices which 'sense' (e.g. an empty fridge) and automatically order goods or services. Most consumer versions are mediated via smartphone approvals pre-order or payment.
<b>metadata</b>	"metadata" describes and gives information about other data
<b>Moore's Law</b>	the number of transistors that can be put on a microchip doubles about every 18 months: Gordon E. Moore (19 Apr 1965)
<b>mosaic effect or data fusion</b>	the integration of big data whereby personally identifiable information can be derived or inferred from supposedly de-identified datasets, using processes such as data matching or linkage.
<b>open standards</b>	"open standards" are written requirements for technical systems that are free and available for all to read and use. They enable interoperability and data exchange.
<b>privacy by design or PBD</b>	A compliance-based system which creates privacy as a default mode of corporate operation, rather than requiring mere legislative and regulatory framework adherence. PBD is proactive: it anticipates to prevent privacy invasive events; so is a preventative form of risk management.
<b>profiling or predictive analytics</b>	any form of automated processing of personal data, (e.g. data mining, data visualization, algorithm clustering, and neural networking) to evaluate personal attributes and to analyse or predict aspects as to a person's performance at "work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements..." [GDPR, Art 4 (4) (adapted)].
<b>RFID*</b>	Radio frequency identification; this is automated data collection technology using radio frequency waves to transfer data between a reader and a tag to identify, track and locate the tagged item.
<b>sensor</b>	A device which generates an electronic signal in response to a physical event or condition. <sup>2131</sup>
<b>smart car</b>	Motor vehicle with advanced software and electronics, including driver-assist technology, GPS navigation, reverse sensing systems, night vision, assisted parking, internet and e-mail access, voice control, smart card activation (in lieu of keys) and decreasing driver-control requirements – leading to a fully autonomous vehicle.
<b>smart home</b>	A networked home consisting of multiple interlinked and integrated devices, sensors, tools and platforms, to provide multiple services and analysed-data usually via apps, including security, climate-control, and home automation both in-home and remotely.
<b>smart self</b>	devices attached to or implanted inside the human body – in this thesis, they include devices which monitor human health. fitness and wellness. Note it excludes 'smart health' devices which improve monitor and improve disease management and identification and are therapeutic in nature.
<b>sustainability</b>	this incorporates the life-cycle issues related to long- term supportability of the device and service, transfers of ownership of devices and the control and usage of the data collected.
<b>telematics*</b>	the use of pre-installed or after-market wireless devices and "black box" technologies to transmit data in real time back to the car manufacturer; including vehicle use, maintenance requirements, servicing, air bag deployments or car crash information. It may use GPS to locate stolen vehicles and is used for usage-based, pay-per-use, pay as you drive, and pay how you drive insurance.
<b>trust mark</b>	A third-party mark, logo, picture, or symbol provided to reflect firm-specific compliance standards and promote trust.
<b>vendor or device "lock-in"</b>	where consumer switching costs inhibit changing devices (e.g.) the cost of changing providers, adverse contractual terms or technical difficulties such as device or data non-portability or non-interoperability
<b>'Wi-Fi'</b>	Wireless fidelity; this is the most common smart home device protocol via routers which become Wi-Fi-enabled device hubs.

Table E Glossary

Sources: author & various

<sup>2131</sup> Jonathan Holdowsky, Monika Mahto, Michael E. Raynor and Mark Cotteleer, 'Inside the IOT: a primer on the technologies building the IoT' *Deloitte* (21 Aug 2015 accessed 5 Feb 2016) <<https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-primer-iot-technologies-applications.html>>