Will emerging information technologies outpace consumer protection law? — The case of digital consumer manipulation

Kayleen Manwaring*

A ‘third wave’ of computing is emerging, based on the widespread embedding of processors with data handling and communications capabilities into everyday objects and environments, such as fridges, fitness trackers and hairbrushes. This sociotechnical change brings with it the possibility of a disconnection between current consumer protection law and new marketing activities. The widespread digitisation of commerce has given firms an enhanced ability, not only to compile detailed customer profiles, but also to exploit consumers’ cognitive biases and individual vulnerabilities: a form of ‘digital consumer manipulation’. Opportunities for digital consumer manipulation will be increased by the widespread use of third wave technologies, enabling the availability of a greater amount of intimate and personalised data and creating additional personalised targeting opportunities. Why does this matter? Digital consumer manipulation can erode consumer autonomy, limit choice and competition, violate privacy, compromise personal dignity and subvert reasonable decision-making by consumers. This article examines the key provisions of the Australian Consumer Law to establish its likely effectiveness in the face of digital consumer manipulation facilitated by the third wave.

Introduction

A ‘third wave’ of emerging information technologies, variously described as ‘ubiquitous’ and ‘pervasive’ computing, ‘ambient intelligence’, the ‘Internet of Things’, and ‘eObjects’¹ is currently driving significant sociotechnical change. Computer processors capable of data collection, processing and communications are being embedded in everyday objects, such as hairbrushes, fitness trackers, household appliances and cars. The technologies comprising the third wave are referred to as eObjects (enhanced objects), and are more fully described in Part 2.1. Sociotechnical change reflected in new digital data collection, profiling and targeting methods using eObjects may provide commercial entities with an enhanced ability, not only to target consumer preferences, but also to exploit consumers’ cognitive biases and individual vulnerabilities.

---

* Lecturer, School of Taxation and Business Law, UNSW Sydney; Researcher, Allens Hub for Innovation, Technology and Law. The author wishes to acknowledge the helpful comments of Lyria Bennett Moses, Roger Clarke, Leon Trakman, Gail Pearson, the anonymous referee and all participants in the Law, Innovation and Technology Junior Scholars Forum held at UNSW, Sydney on 24 November 2017 and the British and Irish Law Education and Technology Association (‘BILETA’) Conference held at the University of Aberdeen on 10–11 April 2018, particularly Graham Greenleaf, Catherine Easton, Nicole Vincent, Katherina Drinkuth and Jake Goldenfein. All opinions, errors and omissions are the author’s own.

vulnerabilities. This may lead to disconnection\(^2\) between current consumer protection law and consumers’ legitimate expectation to be protected against predatory conduct.

Before the rise of eObjects, conventional computing and the growth of ecommerce presented new opportunities for marketers to gather data on consumers and exploit behavioural research to improve the persuasiveness of their marketing.\(^3\) I refer to this as ‘digital consumer manipulation’ (‘DCM’). Earlier work analysing the sociotechnical change brought about by eObjects argued the adaptability, geolocatability and prevalence of eObjects would increase opportunities for DCM.\(^4\) Consumers have long been on the receiving end of persuasive tactics from advertisers.\(^5\) However, the greater volume, intimacy and personalisation of data collected by eObjects, combined with the capability to use eObjects as additional marketing channels, will offer significant advantages to marketers in accuracy, scope, scale and effectiveness,\(^6\) and may give rise to more significant harms for consumers. This article is intended to examine potential harms in the context of existing Australian consumer protection law and to assess what legal problems arise out of disconnection between the harms and the existing law.

Part 1 of this article summarises the types of legal problems arising in the face of sociotechnical change. Part 2.1 outlines the scope of the technologies at issue and Part 3.2 describes their current and potential use by marketers to engage in enhanced forms of DCM. Part 2.3 outlines the reasons why DCM has been considered to be problematic, and consequently how it may conflict with the goals of Australia’s consumer protection law. Part 2.4 sets out a hypothetical vignette on how DCM could be undertaken using eObjects (the ‘vignette’). Part 3 analyses the key provisions of the Australian Consumer Law (‘ACL’)\(^7\) and related case law potentially regulating DCM, and outlines the legal problems arising when the laws are applied to the vignette and DCM in general. Part 4 concludes with an examination of the shortcomings of the current law and suggestions for further development.

\(^7\) Competition and Consumer Act 2010 (Cth) sch 2.
1 Examining legal problems arising out of emerging technologies

Sociotechnical change occurs when new products, activities and relationships are made possible by the development and use of new technologies. When sociotechnical change occurs, this can cause a ‘disconnection’ between law designed for an earlier sociotechnical environment and new conditions. It is important to recognise that disconnection does not always occur in the face of sociotechnical change. Some legislation are general enough in application, and common law and equitable principles are sufficiently adaptable, to apply to a variety of new products, activities and relationships. When disconnection does occur, it is important to establish where the law has become disconnected and ‘reconnect’ the law with the present conditions and possibilities of human behaviour.

Legal problems arising from regulatory disconnection in the face of sociotechnical change can manifest in a number of categories:

• legal rules uncertain in their application to new products, activities and relationships;

• rules that are too wide or too narrow, that is, under- or over-inclusive in the face of sociotechnical change;

• rules that are obsolete; and

• when new harms or benefits are created, the need for ‘special rules’.

A timely examination of possible disconnection is essential to mitigate the effects of what has been labelled the ‘Collingridge dilemma’. Although regulators prefer a ‘wait and see’ approach to uncover the risks and benefits of sociotechnical change before regulation, too much delay can derail attempts at meaningful regulation as powerful vested interests can make regulatory change impossible or compromised. One version of this can be seen in weak or tentative initial responses, such as unenforced guidance from regulatory agencies, leading to long-term regulatory inaction. An illustration of this can be seen in Cortez’s extensive case study on the US Food and Drug Administration’s (‘FDA’) treatment of the regulation of computerised medical devices. Cortez found that the use of mere guidance by the FDA, without any substantive attempts at follow-up regulation and enforcement over 25 years,
led to a calcification into a ‘weak default position’, and to continued ‘[w]idespread problems’ with device software that have resulted in significant injuries to patients.

This article discusses not only DCM arising from existing technology and known marketing practices, but also marketing practices that may become possible with emerging technologies (that is, those claimed to be subject to imminent commercial release or to be at an advanced stage of development).

Additionally, publicly available scholarly knowledge of ‘behind-the-scenes’ marketing practices, data sharing models and proprietary technology are likely to be deficient due to intentional corporate secrecy policies. The opacity problem brought about by corporate secrecy is exacerbated by the difficulty non-specialist humans have in understanding complex code and algorithms and by emergent properties of machine learning technologies. These result in outcomes that cannot be explained, even by specialists. A certain amount of speculation, particularly around the nature of business models and subsequent information sharing between commercial parties, is unavoidable.

2 Emerging technologies and their effects on consumers

2.1 The rise of eObjects

The third wave technologies discussed in this article have been the subject of many different terms, including ‘ubiquitous’ and ‘pervasive’ computing, ‘ambient intelligence’, and the ‘Internet of Things’. However, inconsistencies and confusion around their definitions and use plague the literature. To deal with these problems, in an earlier article I identified core and common attributes and proposed a new term, ‘eObject’, for the central element of these new technologies.

An eObject (‘enhanced object’) is an ‘object that is not inherently computerised, but into which has been embedded one or more computer processors with data-collection, data-handling and data communication capabilities’.

The technologies and their effects are complex, so this definition does not give a complete view of the technologies. My earlier article provided a list of common attributes, none of which appear in all eObjects, but are common enough to drive significant sociotechnical change. These common attributes are active capacity (can act on the physical world), adaptability (context awareness), addressability (unique address), associability with living beings,

14 Ibid 227.
15 Ibid 194.
19 Manwaring and Clarke, above n 1, 611.
autonomy, dependency (on remote services or infrastructure), geo-locatability, identifiability (unique device identifier/s), mobility or portability, operational, economic and social impact, network locatability, prevalence, use pattern, visibility, volatility and vulnerability.20

These attributes not only apply to eObjects, but also to the systems in which they participate.

2.2 Digital consumer manipulation

Inferences from data may be used to benefit consumers; for example, by delivering more relevant advertising. However, concerns by scholars,21 practitioners,22 think tanks,23 journalists and industry commentators24 have been growing that the increase in electronic marketing and transactions may grant marketers a greater capacity to discover consumer preferences and use data and behavioural research to exploit the biases, emotions and vulnerabilities of consumers. For example:

advertisers may filter the available information; they may target consumers at the time when their willpower is lowest; or they may craft their advertisements to act upon known purchasing triggers of particular individuals, for example, feelings of guilt or obligation, or concerns about missing out, or a desire to emulate friends or celebrities.25

I use the term ‘digital consumer manipulation’, or DCM, to refer to this conduct, although other terminology has been used.26 This article’s main focus

---


24 Eg, see Yael Grauer, Dark Patterns are designed to trick you (and they’re all over the Web) (28 July 2016) Ars Technica <https://arstechnica.com/information-technology/2016/07/dark-patterns-are-designed-to-trick-you-and-theyre-all-over-the-web/>.


26 Calo originally dubbed this practice ‘digital market manipulation’: see Calo, above n 3, 995. This term is rooted in an earlier concept, ‘market manipulation’, coined by Hanson and Kysar in the late 1990s: see Jon D Hanson and Douglas A Kysar, ‘Taking Behavioralism Seriously: Some Evidence of Market Manipulation’ (1999) 112 Harvard Law Review 1420; Jon D Hanson and Douglas A Kysar, ‘Taking Behavioralism Seriously: The Problem of Market Manipulation’ (1999) 74 New York University Law Review 630. These two articles have been widely cited in the US literature (over 200 times each): see Calo, above n 3, fn 29. These articles explain how commercial entities use techniques to exploit consumers’ cognitive limitations and biases to sell them products and services. However, Calo, Hanson and Kysar’s terminology may create confusion, as it will produce different associations for Australian readers by its use of the word ‘market’. Corporations Act 2001 (Cth) s 1041A
is on the ‘enhanced’ forms of these practices in which eObjects are involved in data collection and/or delivery of marketing content. However, the doctrinal analysis in Part 3 of this article may also be relevant to DCM in ‘conventional’ e-commerce.

An examination of the core and common attributes of eObjects and related systems outlined in Part 2.1 reveals several are helpful to marketers. The capacity of all eObjects to collect and communicate data assists marketers in building customer profiles and in targeting their marketing campaigns. Marketers can leverage other attributes of eObjects such as mobility, prevalence, geo-locatability, associability and adaptability. The use pattern of many eObjects is limited to one or a few individuals and the eObject may also be addressable and/or identifiable. An ability to personalise data records improves the usefulness of the data gathered. Data utility is increased by another attribute of eObjects; adaptability (also known as context awareness), that allows eObjects to adapt their responses to the user: who, where, how, their habits and preferences.

In 1996, Kang and Cuff postulated the development of a ‘networked mall’: a mixed real/virtual shopping centre created using eObjects and related systems. Suppliers in a networked mall might attempt DCM in different ways. Music in a part of the store might change in response to the person entering, thermometer readings detecting a temperature might trigger a mobile telephone advertisement for paracetamol or the local medical centre or a ‘sudden up-tick [of heart rate] near lingerie might suggest a rated R feature at the gigaplex’.

Although Kang and Cuff’s idea of a networked mall was speculative, over a decade of technological development has seen the realisation of some of their ideas. By 2014, the data from mobile telephone sensors could be used to infer mood, personality, stress levels, gender, marital and job status, age, level of disease, mental health issues, sleep and physical movement. For example, in 2013 researchers were able to extract audio, GPS, accelerometer, call numbers, call duration, ratio between incoming and outgoing calls, changes in phone contacts, phone numbers and email addresses, and battery usage data.

---

28 Ibid 126.
from smartphones and analyse it to predict stress levels in the smartphone user.⁳⁰

eObjects have been developed for use as enterprise marketing devices. ‘Beacon’ implementation systems, such as Apple’s iBeacon, use indoor positioning devices with small, low-power sensors,³¹ capable of tracking when a smartphone enters a physical space. A shopper who has signed up to the service³² may be located by a beacon as they enter a clothing store. A general discount voucher may then be sent to their telephone, but systems with more sophisticated algorithms and programming might access their marketing profile, see they are a keen shoe shopper and generate a personalised discount voucher to the shopper for certain designer shoes in the aisle close to them. Beacon implementations are not yet widespread but currently they are being used in retail, museums, airlines, fast food providers, real estate agents and pharmacies in Australia³³ and overseas.³⁴ Interest in similar corporate tracking technologies appears to be growing: for example, in October 2018, a member of Chemist Warehouse’s IT architecture team announced that the pharmacy business was ‘considering’ installing thousands of sensors to track foot traffic within its stores and also where consumers ‘dwell in particular areas [and] ... pick up products and look at them’.³⁵

The accuracy of consumer profiles and opportunities for behavioural targeting may be assisted by the use of additional technologies, such as cross-device tracking (known as ‘XDT’) technologies. XDT technologies allow the tracking of a consumer across multiple devices, such as tracking television viewing by means of software installed on a smartphone. Companies such as Google, Domino’s and Nestlé have been using these services, such as SilverPush, Signal360 and Audible Magic, although not without controversy.³⁶ In 2016, the US Federal Trade Commission issued warning letters to Android application (‘app’) developers who used XDT technologies from SilverPush that could track television viewing habits, even when the app was not in use.³⁷

These types of marketing systems rely on access to personalised customer

---

31 iBeacon uses the Bluetooth Low Energy communications standard, but other beacon technologies use both Bluetooth and wi-fi (eg, Motorola Solutions and Datzing).
33 Woolworths (major supermarket chain); Homemart (real estate services). See Localz <https://localz.com/customer-stories/>.
34 Eg, Macy’s; McDonald’s; Major League Baseball; Walgreens; Virgin Atlantic; Japan Airlines; American Airlines. Trips Reddy, 15 Companies From Airports to Retail Already Using Beacon Technology (10 November 2014) Umbel <https://www.umbel.com/blog/mobile/15-companies-using-beacon-technology/>; John Lewis (department store) <https://localz.com/customer-stories/>.
37 Federal Trade Commission, ‘FTC Issues Warning letters to App Developers Using
profile data, with the potential to be programmed in response to behavioural research on how consumers make decisions. Despite the lack of ‘human touch’ in selling, this can provide marketing advantages. A human shop assistant is unlikely to have the same knowledge of a new shopper’s personal preferences and is also unlikely to have access to aggregated knowledge about purchasing patterns or cognitive biases. The persuasive powers of a human may not be an advantage; psychological research has indicated people can react in the same way to social persuasion (such as flattery or kindness) by a computer as they do to real people.38 Digital personal assistants or ‘helpers’ in the home, such as Amazon’s Alexa and Alphabet’s Google Assistant, are examples of the potential of these types of devices for data collection and marketing delivery.39

Although the effectiveness of DCM techniques is not yet proven,40 evidence is emerging to support predictions that:

- in the future the extent and type of information will mean that their inferences may be more accurate, more revealing, and their ability to manipulate consumer behaviour more successful.41

Recent empirical research has indicated that psychological characteristics:
- can be more accurately assessed by online behaviour (more than with human-based assessment);42 and
- when used in personalised advertising, targeted consumers will engage significantly more with advertisers and buy more than when compared with non-personalised advertising.43

I argue the ability of eObjects and related systems to collect more data and provide more personalised marketing messages and channels will provide a greater boost to scale and effectiveness when compared with, and combined with, current techniques employed in ‘conventional’ ecommerce. This is discussed further in Part 3.1.


39 Eg, Amazon’s Alexa and associated cloud services record and store voice requests for music, audio books, podcasts, web searches about ‘various subjects’ including health conditions and politics, and real-time information such as news, weather and traffic conditions. They also allow users to order products, including books and creative materials, and common consumer products such as beer. See Memorandum of Law in Support of Amazon’s Motion to Quash Search Warrant in Arkansas v Bates (Circuit Court of Benton County, Arkansas, Case No Cr-2016-370-2, 17 February 2017) 10; Matt Tate, Amazon’s new Alexa update means it can bring you beer in two hours (21 March 2017) ShortList <https://www.shortlist.com/tech/gadgets/you-can-now-tell-amazons-alexa-to-bring-you-a-b eer-amazon-echo/18775>.
40 Mik, above n 3, 15.
41 Kim, above n 6, 312. See also Mik, above n 3.
42 Wu Youyou, Michal Kosinski and David Stillwell, ‘Computer-based personality judgments are more accurate than those made by humans’ (2015) 112 Proceedings of the National Academy of Sciences of the United States of America 1036.
2.3 Consumer protection goals and the case of DCM

So why is this conduct problematic? Persuasive tactics by advertisers are not new and regulation or limitation of such tactics has always required something more egregious than persuasiveness. In relation to DCM, marketers could respond to calls for regulation by saying ‘there is nothing forcing a customer to make a purchase — they have a choice to go elsewhere or not shop at all’. However, this argument ignores the important and complex question of whether the consumer actually does have a proper ‘choice’ in all circumstances of DCM. A number of scholars have argued that choice and autonomy have significant and increasing potential to be impaired in a number of ways by DCM techniques. For example, Sax, Helberger and Bol conducted an analysis of selling techniques within mobile health applications (such as those used with fitness trackers and smartphones), and consumer responses to them. They concluded that these could lead to the undermining of autonomy in the following ways:

- alternative product and service options being obscured;
- unauthentic goals and desires being invoked in a consumer due to continued use of an application designed to be addictive, and/or the rewarding of behaviours desired by the supplier rather than those initially desired by the consumer;
- independent decision-making being circumvented due to the framing of economic choices as health or welfare choices.

Information asymmetry between supplier and consumer, which has long been seen as compromising consumer choice, is arguably also increased by DCM.

Other significant disbenefits of this type of conduct which have attracted condemnation include its potential to:

- be unfair to consumers;
- violate privacy;
- compromise the dignity of consumers; and
- hinder or distort competition.

It appears now that at least one regulatory agency is recognising the harms caused by this conduct. In March 2018, the European Data Protection

44 Mik, above n 3; Helberger, above n 4; Maurice E Stucke and Ariel Ezrachi, ‘How Digital Assistants Can Harm Our Economy, Privacy, and Democracy’ (2017) 32 Berkeley Technology Law Journal 1239.
45 Mik, above n 3; Calo, above n 3; Helberger, above n 4.
50 Mik, above n 3; Helberger, above n 4.
51 Helberger, above n 4; Calo, above n 3, 237.
52 Calo, above n 3.
53 Helberger, above n 4.
54 Calo, above n 3; Stucke and Ezrachi, above n 44.
Supervisor (‘EDPS’) issued an opinion concluding that ‘[o]nline manipulation poses a threat to society’. Although much of the EDPS’s concern relates to the use of data collected by corporate and government actors to influence the outcome of elections, it also recognises the general undesirability of hidden manipulation of consumers and the possibility of harms arising out of breaches of privacy, hindrances to competition, and the encouragement of addictive behaviours (particularly in children).

Increasing consumer unease with DCM practices, at least in relation to conventional ecommerce, is also a factor in considering the acceptability of DCM. The Consumer Policy Research Centre (‘CPRC’) Survey in 2018 revealed that slightly over 50 per cent of Australians surveyed found (conventional) targeted online advertising unacceptable, 27 per cent found it acceptable, and around 20 per cent were neutral. This supports an earlier study of Australian users and developers of eObjects, which included comments that users of eObjects ‘were concerned about their personal data and others’ ability to control and understand their patterns of behaviour stemming from their personal information’. More generally, there was an expectation expressed by most consumers in the CPRC Survey that it was the responsibility of government to become involved in regulating how companies use consumer data.

A 2016 review of US empirical work on consumer attitudes to personalised targeting also found considerable disquiet amongst consumers faced with targeted advertising, although, like the Australian consumers surveyed, there was a range of different attitudes. There were some indications from the US data that consumers’ actual marketplace activities were at odds with their expressed distaste for personalised advertising, as such advertising tended to be successful in increasing purchases. However, this could be advanced as an argument against allowing these practices, as it implies that the techniques can be successful even when the consumer is aware of them and of the negative effects on their behaviour and interests. Forms of disclosure are frequently proposed to mitigate harmful effects on consumers, but these types of results provide some limited indication that disclosure is not effective.

---

56 Ibid 9, 10, 12.
57 Nguyen and Solomon, above n 23, 61. The research question was: ‘How acceptable or unacceptable do you find it for companies to use your data in the following ways? Monitoring your online behaviour to show you relevant advertising and offers’ — 29.2 per cent of respondents found this ‘very unacceptable’, 22.8 per cent ‘somewhat unacceptable’, 19.8 per cent ‘neutral’, 24.6 per cent ‘somewhat acceptable’ and 2.4 per cent ‘very acceptable’.
58 Twenty-four participants, 12 of whom were designers and users of eObjects, the other 12 just users.
60 Nguyen and Solomon, above n 23, 62; 37.73 per cent of respondents indicated that ‘[t]he Government should ensure companies give consumers options to opt out of what data they provide, how it can be used, and if it can be shared with others’.
62 Ibid.
The case of digital consumer manipulation 151

The issues outlined above suggest some forms of DCM may conflict with consumer protection goals enshrined in Australia’s consumer protection laws. The objective of the legislation enacting the ACL is:

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.63

The ACL is intended to:

• ensure consumers are well-informed to benefit from and stimulate effective competition;
• ensure goods and services are safe and fit for purpose;
• prevent unfair practices;
• meet the needs of vulnerable and disadvantaged consumers;
• provide accessible and timely redress for consumer detriment; and
• promote proportionate, risk-based enforcement.64

When DCM is successful in persuading consumers to conduct transactions they would otherwise not have made, it has the potential to conflict with some of the ACL’s stated goals: in particular, those relating to unfair practices, protecting vulnerable or disadvantaged consumers and providing accessible and timely redress. Such conduct also has the potential to fetter a consumer’s freedom of choice, a value postulated65 as essential to be enforced by consumer protection law. Freedom of choice is not listed as an explicit goal of the ACL, although it is implied in the concepts of ‘consumer empowerment’ and the ‘foster[ing of] effective competition’ contained in the legislation’s objective.66

The factors discussed above suggest DCM practices should be restricted in some way, while recognising the line is sometimes difficult to draw between practices that are an acceptable part of competitive business practice and those that unacceptably compromise consumer welfare.67

Part 2.4 presents a vignette outlining possible uses of eObjects and related systems to undertake DCM. The vignette is used in Part 4 to assist in examining current provisions of the ACL to assess whether legal problems arise.

2.4 A DCM vignette

Fahim jogs home every day from work and tracks his exercise via his smart wristband.68 He uses an internet-connected insulin pump and continuous glucose monitor for his type 1 diabetes. He tracks the data using his smartphone,69 which he received at a discounted price in a shopping centre.

63 Council of Australian Governments, Inter-governmental Agreement for the Australian Consumer Law, 2 July 2009, 3 Recital C.
64 Explanatory Memorandum, Trade Practices Amendment (Australian Consumer Law) Bill (No 2) 2010 (Cth) 454 [23.7]–[23.8]; ibid 3–4 Recital D.
65 Helberger, above n 4.
66 Council of Australian Governments, above n 63, 3 Recital C.
67 Helberger, above n 4.
69 Jonah Comstock, ‘Medtronic launches smartphone connectivity for CGMs, insulin pumps’,
promotion. To get the discount, all he needed was to download an app, which he has found useful for identifying further good deals.

Fahim visits the local shopping centre every Saturday to check out the best bargains. This Saturday, he is feeling pretty tired and is almost ready to go home, when he receives a message on his telephone as he walks past Donuts & More! His favourite donuts are on special and he cannot resist. He feels a bit guilty because he succumbed to a similar ad last week at the same time.70

On Monday morning, Jessica looks in her bathroom mirror and sighs, ‘look at all those wrinkles, I’m getting old’. She brushes her hair with the hairbrush proffered by her hairdresser at her last visit, whose sensors indicate a too-hard brushing, risking split ends.71 Max, her smart home hub and digital personal assistant,72 hears her comment but does not respond. Business has been a bit slow lately, so later that evening, Jessica asks Max to find and play a few clips on her loungeroom screen containing tips on marketing to potential clients. She notices the lead-in advertisement for a beauty product.

The next day, Jessica’s 9-year-old daughter, Mylin, begs to go shopping for her birthday present. Max suggests the local shopping centre. As they enter, an interactive billboard displays an advertisement telling the story of a vaguely familiar beauty product transforming a down-at-heel looking middle-aged woman who just lost her job into a glamorous and successful CEO of her own consulting business. Jessica and Mylin go to the toy store and Mylin knows what she wants, including the brand, much to Jessica’s relief as she is pressed for time. What Jessica does not know is Mylin’s birthday present was suggested by Ella, Mylin’s internet-connected doll.73

As Jessica and Mylin begin to leave, Jessica’s smartphone pings — she has been offered a 10 per cent discount on Couteux’s new wrinkle cream and a 50 per cent discount on Prix Eleve’s dry hair conditioner. She makes a quick stop at the centre’s pharmacy.

At 9.30 pm, while Jessica is packing for an overseas work trip, Max reminds her of her sister’s birthday tomorrow. She asks Max to order her sister’s favourite flowers. She is a bit concerned at the price — she ordered the same flowers 2 weeks ago and was sure she only paid half. She confirms the order because she is out of time to think of anything else, and her sister has been calling a lot recently looking for support for her marital problems. Max reminds her that her smartphone contract is due to expire and quotes the price for a new 2-year contract, with a 10 per cent increase in price. She asks hopefully ‘Max, is there anything cheaper?’ Max replies ‘there are cheaper

---

70 Donut example taken from Calo, above n 3, 996.
71 Eg, Kérastase Hair Coach powered by Withings: Brian Heater, Here’s a Smart Hairbrush with a Built-In Microphone from Withings and L’Oreal (3 January 2017) TechCrunch <https://techcrunch.com/2017/01/03/withings-brush/>.
72 Eg, Amazon’s Alexa-powered Echo, Alphabet Inc’s Google Assistant. See also Amazon’s US patent: Kiran K Edara, Key word determinations from voice data, US8798995B1, 23 September 2011 <https://patents.google.com/patent/US8798995B1>.
packages, but this is the one that best suits your needs and preferences’. She tells Max to approve the renewal.

3 Legal problems in Australia arising from DCM using eObjects

3.1 The situation of the consumer

In this article, I argue many DCM practices will not be prohibited, nor even constrained, by the current consumer protection regime. Marketers have been exploiting the cognitive biases of consumers for many years through a number of means. What makes DCM different? In the context of DCM, I argue that the combination of ‘intense systematization’ and ‘personalization’74 innate in DCM, particularly when enhanced by eObjects, provides unprecedented opportunities for marketers when targeting such digital consumers. In other words, consumers have never before been in a position where:

- suppliers know so much about individual consumers;
- marketing analysts know so much about what combination of factors lead to particular purchase decisions;
- marketing channels are so plentiful and diverse, and can target consumers in so many different places and at so many different times; and
- consumers know very little about the rich variety of data collected, the inferences that may be drawn from it, and how those inferences might be exploited.75

To explain in practical terms how the changed position of the consumer affects marketing techniques, let us first look at an example of ‘conventional’ sales techniques. Jessica, 10 years ago, may have gone into her local shopping centre, as she does in the vignette. She would have moved through the centre and passed by a number of static ads. A decision to enter the pharmacy would mean that she would have passed through a fit-out and display designed to direct her steps past its most profitable products. An experienced salesperson would have been able to quickly and correctly peg her as a middle-aged working mother, time-poor but nevertheless looking for a bargain. The salesperson would have approached Jessica with suggestions based on her experience of previous similar customers’ buying patterns, and with the types of compliments that are most likely to achieve a sale.

Compare this with the vignette, in which Jessica’s and Fahim’s environments are ‘enhanced’ by eObjects. Max may have data on Jessica’s digital purchases over the last 2 years, age, personality type, career, weight, household salary, physical activity, where she is at different times of the day...

74 Calo, above n 3, 1021.
75 Note however that consumer awareness may now be somewhat greater due to the publicity surrounding the Facebook data harvesting undertaken by Cambridge Analytica and related companies for the purposes of influencing the US presidential election and the Brexit referendum: see, eg, Carole Cadwalladr and Emma Graham-Harrison, ‘Revealed: 50 Million Facebook profiles harvested for Cambridge Analytica in major data breach’, The Guardian (online), 17 March 2018 <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.
and how often she visits particular places, what she eats, her relationships with families, friends and service providers, health, mood, and day and time in the week she is most likely to make a purchase. Fahim’s and Jessica’s phones collect data from other eObjects and conventional computers, and pass it onto third parties, such as the shopping centre. Jessica’s television may well do something similar. Marketing approaches are based on algorithms researched and developed by marketing experts with large budgets for behavioural research, heavily personalised to Jessica’s and Fahim’s profiles, and deliverable anytime and anywhere. The eObjects with which Jessica and Fahim interact adapt to the success or failure of particular marketing approaches, and add this to both Jessica’s and Fahim’s profiles and the profiles of other people like them.

Publicly available empirical research concerning the effectiveness of DCM using eObjects is scant. However, I argue that DCM in this context provides suppliers with more relevant information and new avenues whereby they can detect and capitalise on opportunities, and even create them, such that some consumers are highly likely to buy their product. Less obviously, the framing of offers and the immediacy of particular channels, such as an always-available digital personal assistant, or the convenience of a supplier-specific ordering button, are also relevant. These may reduce both the availability of information to the consumer and the scope for them to give it proper consideration.

3.2 How the ACL might deal with DCM

DCM has been characterised by some scholars as a form of ‘unfair persuasion’. However, ‘unfairness’ is not recognised as a general principle of regulated conduct under the law in Australia. This contrasts with general prohibitions against unfair commercial conduct that can be found in other jurisdictions, such as in the United States and Europe. For example, s 45(a) of the US Federal Trade Commission Act of 1914 prohibits ‘unfair or deceptive acts or practices in or affecting commerce’. Chapter 2 of the European Union (‘EU’) Unfair Commercial Practices Directive prohibits ‘unfair commercial practices’ in general, and also provides a list in annex I of specific practices that ‘in all circumstances [would] be regarded as unfair’. Claims arising out of DCM in the United States and the EU are likely to invoke these.


77 However, one useful example of early stage empirical research can be seen in Sax, Helberger and Bol, above n 46.

78 Calo, above n 3, 1032; Helberger, above n 4.


80 This has been implemented in almost identical terms in The Consumer Protection from Unfair Trading Regulations 2008 (UK) reg 3.
prohibitions. However, a detailed comparison between these prohibitions and the Australian law is beyond the scope of this article.

However, a general prohibition on unfair conduct in commerce is not currently found in Australian law. Some specific sales techniques are designated as ‘unfair practices’ in the ACL and regulated accordingly, such as offering rebates, gifts and prizes, bait advertising, wrongfully accepting payment, providing unsolicited credit and debit cards or other goods and services and pyramid selling. However, none of these provisions (aside from s 29) apply generally to DCM techniques (although such techniques could be used to carry out regulated conduct, such as a service provider using Max in the vignette for bait advertising).

Some general principles exist that judges can call upon to restrict the ways service providers might manipulate consumers into forming contracts. Suppliers will usually be in a position to know much more about their products or services than consumers, and the provision of false or misleading information can affect individual choice and competition. The ACL attempts to enable ‘informed commercial activity’ by means of prohibitions on suppliers providing false, misleading and/or deceptive information to consumers about their products and services. Part 3.3 discusses the potential application to DCM of the general legislative provisions prohibiting misleading and deceptive conduct (s 18 ACL) and specific false and misleading representations (s 29 ACL). (This article does not deal with common law misrepresentation as it has a narrower application than the ACL provisions in the business-to-consumer context.) However, I conclude that some DCM may fall outside the prohibitions, even if otherwise objectionable or unfair.

Misleading or deceptive conduct may lead to significant information asymmetry, to the disbenefit of consumers and their decision-making processes. However, it has long been recognised in both case and statute laws that consumers’ decision-making processes can be manipulated in other ways, such as where one party suffers from a disadvantage and the other exploits that advantage to the first party’s detriment. Part 3.4 discusses the application of statutory (and, where relevant, equitable) principles relating to unconscionable conduct (ss 21–2 ACL) to DCM. Unfortunately, this Part demonstrates some significant barriers to the use of unconscionable conduct principles to regulate unwanted forms of DCM.

Part 3.5 will also briefly discuss the potential relevance of other areas of law.

### 3.3 Misleading and deceptive conduct

#### 3.3.1 Elements of misleading and deceptive conduct; false or misleading representations

Marketing practices must comply with the ACL provisions prohibiting ‘misleading or deceptive conduct’ (s 18 ACL) and ‘false or misleading
representations’ (s 29 ACL). While s 18 applies generally, s 29 prohibits a set of specific false and misleading representations from a ‘closed list’ regarding supply and promotion of goods and services, including misrepresentations relating to price (s 29(1)(i)), quality (ss 29(1)(a)–(b)), performance characteristics or uses (s 29(1)(g)), place of origin (s 29(1)(k)), necessity (s 29(1)(l)) and sponsorship (ss 29(1)(g)–(h)). Mirror provisions for ss 18 and 29 relating to financial services are found in ss 12DA–12DB of the Australian Securities and Investments Commission Act 2001 (Cth) (‘ASIC Act’). The ASIC Act provisions are relevant in two ways. First, the cases on the mirror provisions are relevant as precedent for ACL cases (and vice versa). Second, eObjects can be used to provide financial services and therefore the ASIC Act can be directly applicable.

The integers underlying both sections are as follows:

<table>
<thead>
<tr>
<th>Section 18 prohibits:</th>
<th>Section 29 prohibits:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. a person</td>
<td>same</td>
</tr>
<tr>
<td>2. in trade or commerce</td>
<td>same</td>
</tr>
<tr>
<td>3. engaging in conduct</td>
<td>representation (closed list)</td>
</tr>
<tr>
<td>4. which is misleading or deceptive</td>
<td>false or misleading</td>
</tr>
<tr>
<td>5. or is likely to mislead or deceive</td>
<td>no</td>
</tr>
<tr>
<td>6.</td>
<td>in connection with the supply/possible supply/promotion of goods/services</td>
</tr>
</tbody>
</table>

Integers 1 and 2 of s 18 are repeated in s 29, but what are prohibited are ‘false or misleading representations’. For integer 4, nothing turns on the difference in terminology. Australian judges have treated the terms ‘false or misleading’ in s 29 synonymously with the terms ‘misleading or deceptive’ in s 18.85 However, there are five significant differences between ss 18 and 29:

• integer 3 — s 29 requires ‘representations’ which are narrower than the ‘conduct’ prohibited in s 18;
• integer 3 — s 29 has a closed list of representations prohibited by the section, as opposed to the open definition of conduct regulated in s 18;
• integer 5 — the inclusion of ‘likely to’ in s 18;
• integer 6 — the required connection with the supply/promotion of goods/services in s 29; and
• the type of remedies applicable, as s 18 remedies are substantially confined to the civil remedies available under the ACL (such as damages/compensation orders, injunctions, orders for contract

variation or rescission, and adverse publicity orders)\textsuperscript{86} while a breach of s 29 can additionally attract civil pecuniary penalties\textsuperscript{87} and criminal remedies.\textsuperscript{88}

Integers 1 and 2 of ss 18 and 29 are the same, and easily satisfied in relation to DCM.

In relation to integer 3, s 29 requires a representation, that is, a ‘statement, made orally or in writing or by implication from words or conduct, relating to a matter of fact’.\textsuperscript{89} If the representation is false or misleading in relation to one of the elements of the closed list, then it is an actionable misrepresentation under the section. However, modern cases have made it clear that the s 18 term ‘conduct’ is wider. Not only does it cover conduct outside the closed list, it also prohibits both misrepresentations and other forms of conduct. In \textit{Butcher v Lachlan Elder Realty Pty Ltd},\textsuperscript{90} the High Court rejected earlier contentions that s 18 (then s 52 of the \textit{Trade Practices Act 1974 (Cth)} (‘\textit{TPA}’)) required a misrepresentation.\textsuperscript{91} In this case all the judges held the term ‘conduct’ in the section extended beyond representations. In 2010, the High Court confirmed that ‘[f]or conduct to be misleading or deceptive it is not necessary that it convey[s] express or implied representations … It suffices that it leads or is likely to lead into error.’\textsuperscript{92}

The difference in integer 6 is unlikely to make any difference in the context of DCM. However, the same cannot be said for integer 5. The High Court has made it clear that if conduct is only required to be ‘likely to’ mislead or deceive, then there is no need to prove anyone was actually deceived or misled.\textsuperscript{93} The conduct must just be capable of misleading or deceiving someone, to the extent there is a ‘real or not remote chance or possibility’.\textsuperscript{94}

The meaning of misleading and deceptive conduct in practice has been the subject of a rich variety of case law. However, the case law has made it clear that what constitutes misleading and deceptive conduct will depend on all of the circumstances of the case. Gordon J in \textit{Australian Competition and Consumer Commission v Google Inc} (2013) 249 CLR 435, 443 [6]. See also Parkdale Custom Built Furniture Pty Ltd v Puxa Pty Ltd (1982) 149 CLR 191, 198 (‘\textit{Puxa}’); McWilliam’s Wines Pty Ltd v McDonald’s System (Aust) Pty Ltd (1980) 33 ALR 394, 411.

\textsuperscript{86} ACL s 236 (damages); s 237 (compensation); ss 232–5 (injunctions); s 247 (adverse publicity orders); s 243 (variation or rescission of contract). This list is not exhaustive. Other orders are available under ACL ch 5.

\textsuperscript{87} Ibid ss 224–31.

\textsuperscript{88} Ibid s 151.

\textsuperscript{89} Russell V Miller, \textit{Miller’s Australian Competition and Consumer Law Annotated} (Thomson Reuters, 2016) 1670. See also \textit{Given v Pryor} (1979) 24 ALR 442; \textit{Aqua-Marine Marketing Pty Ltd v Pacific Reef Fisheries (Australia) Pty Ltd [No 5]} [2012] FCA 908 (24 August 2012).

\textsuperscript{90} (2004) 218 CLR 592, 603, 623 (‘\textit{Butcher}’). See also \textit{Campbell v Backoffice Investments Pty Ltd} (2009) 238 CLR 304.

\textsuperscript{91} For a discussion of the case law on this point, see Alex Bruce, \textit{Consumer Protection Law in Australia} (LexisNexis, 2nd ed, 2014) 85–6 [3.31].


Consumer Commission v Dukemaster Pty Ltd helpfully summarised a series of principles developed by courts relating to conduct regulated under s 18 (then s 52 of the TPA). The principles relevant to DCM techniques are:

1. The ‘conduct’, in the circumstances, must lead, or be capable of leading, a person into error ... and the error or misconception must result from ‘conduct’ of the corporation and not from other circumstances for which the corporation is not responsible ... 
2. [The section] is concerned with the effect or likely effect of ‘conduct’ upon the minds of that person or those persons in relation to whom the question of whether the ‘conduct’ is or is likely to be misleading or deceptive falls to be tested. The test is objective and the Court must determine the question for itself 
3. [The section] ... is not designed for the benefit of persons who fail, in the circumstances of the case, to take reasonable care of their own interests ...

To analyse the law in relation to DCM, we must look at the nature of ‘conduct’, ‘leading into error’ and the extent to which consumers must take ‘reasonable care of their own interests’.

3.3.2 Conduct and misrepresentations

The differences between ‘representations’ required by s 29 and ‘conduct’ in s 18 may matter in some cases of DCM. This is because some techniques otherwise falling within s 29’s closed list will arguably not amount to misrepresentations. For example, the sales technique of personalised pricing — where the price of an offer is calculated based on collected data about an individual’s willingness to pay — is not dependent upon a misrepresentation. Nevertheless, it could be considered unfair and manipulative.

In the vignette, Jessica is manipulated into paying an inflated price to buy her sister flowers. The service provider supporting Max’s search and ordering services has had the opportunity to build a detailed personalised profile of Jessica, including the timing of her sibling’s birthday, the nature of her recent interactions, and previous information on her willingness to pay in particular situations. If the ‘exigency mark-up’ imposed in this instance is shared between the company that provides Jessica with Max and the florist, both have incentives to raise the price to the maximum possible.

Variable, personalised or dynamic pricing is not generally prohibited. In Australia, personalised pricing is available at weekend markets and car dealerships. Supermarkets offer the same goods at different prices based on the location of the store. Prices based on willingness to pay are readily available on auction websites. In 2016, the Australian Competition and Consumer Commission (‘ACCC’) issued guidance to businesses for complying with the ACL regarding algorithmically-generated dynamic pricing based on market demand. This is commonly offered by businesses operating online ‘sharing economy’ platforms (such as surge pricing by car hire service Uber).
The case of digital consumer manipulation

regulator took no issue with the legality of the practice itself. The ACCC merely warned platform operators against saying their prices were lower than their competitors if the algorithmic pricing made this false in some instances. It also warned platform providers that if they had told their clients their pricing was demand-based, price increases for reasons other than demand would be misleading. However, it is worth noting that there is evidence that many consumers find the practice unfair. The CPRC Survey found that 88 per cent of consumers found it unacceptable to ‘[c]harg[e] people different prices for the same products in the same hour, based on their past purchasing, online browsing history, or payment behaviour’.99

Misrepresentations relating to price are prohibited by s 29(1)(i) of the ACL. However, no misrepresentation is identifiable in the vignette example described above. The service provider has programmed Max to ‘take advantage’ of consumers in exigent situations by increasing the price. However, absent a misrepresentation that, for example, pricing is ‘commission-free’, this would not constitute a breach of s 29(1)(i). The relevant question would then be whether in the absence of such a misrepresentation the conduct of imposing an ‘exigency mark-up’ without the knowledge of the customer would constitute a breach of s 18. This situation is discussed further below.

3.3.3 ‘Leading into error’: Factual errors versus evaluative errors

As discussed above, s 18 of the ACL covers a broader range of conduct than s 29. This is due to its open-ended definition and the absence of a misrepresentation requirement. However, even absent a misrepresentation, someone must be led (or must likely to be led) into error.100 Problems may arise depending on how judges interpret this requirement when faced with DCM techniques.

Applying the section to DCM is problematic due to the nature of the type of ‘error’ required. Craswell101 helpfully summarised several approaches generally used by advertisers to influence customers. First, advertising may act to change a consumer’s factual belief about a product, such as comparative price or quality. Second, advertising may change a consumer’s decision-making processes about whether to buy a product. Third, advertising can influence customers by producing a ‘fundamental liking or disliking for a brand that cannot be explained ... as resulting from specific beliefs about particular attributes’, such as might happen when a product is continually associated with a favourable image.102 Craswell considered ‘[t]he key distinction is that false factual beliefs represent errors of fact, while other forms of influence represent errors, if they can be called that, of evaluation or of normative judgment’.103

There are many decisions made by consumers because of DCM which may

---

99 Nguyen and Solomon, above n 23, 61: 76.9 per cent of consumers found it ‘very unacceptable’ and 11.2 per cent of consumers found it ‘somewhat unacceptable’.
100 Miller (2010) 241 CLR 357, 368 [15].
103 Ibid 665 (emphasis added).
fall into the latter category, a category I call 'evaluative errors'. For example, in the vignette, if Jessica is convinced by the techniques employed that she should hide her wrinkles and split ends to be successful in her business, then this is likely to constitute an evaluative error.

However, the Australian judgments are focused on the existence or possibility of a factual error, rather than the evaluative errors brought about by an advertiser’s influence on decision-making processes or fundamental attitudes towards brands.

Despite the High Court’s pronouncements in _Butcher, Campbell v Backoffice Investments Pty Ltd_ and _Miller and Associates Insurance Broking Pty Ltd v BMW Australia Finance Ltd_ (see Part 3.3.1) that s 18 requires ‘conduct’ rather than a ‘misrepresentation’, nevertheless most successful Australian claims under the section are based on some form of false or misleading statement of fact. These clearly fall into Craswell’s ‘factual error’ category. Of course, some cases have been successful which do not involve such a misrepresentation. But ‘almost invariably the claim will focus on specific acts or omissions’, rather than a claim as to everything the defendant has done have been misleading or deceptive. Common acts or omissions that do not involve a traditional misrepresentation have included claims relating to silence, opinions, statements as to future matters, statements of law and unauthorised use of character images. This cannot be a closed list considering the High Court statements and the statutory language relating generally to ‘conduct’. However, the decided ‘non-misrepresentation’ cases can be characterised as consumers being led into a factual error in the Craswell sense, and not an evaluative error.

For example, in the silence cases, victims are led into the factual error that all material facts have been disclosed. In cases of opinion and statements as to future matters, the consumer’s factual error is that the opinion is based on reasonable grounds. Regarding unauthorised use of character images, judicial reasoning has focused on the factual error that the owner of the intellectual property rights in the image has consented to their use for that particular purpose. Although it is common to make a distinction between statements of fact and statements of law, a misleading statement of the law still contains a factual error in the Craswell sense: the factual error subsists in the mistaken belief that a particular principle can be enforced by legal means when in fact it cannot (or vice versa).

Max’s comment in the vignette that its recommended smartphone contract is the one that ‘best suits [Jessica’s] likely needs’ brings up interesting questions of proof. Section 4 of the _ACL_ states that any representation as to a future matter must be based on ‘reasonable grounds’. Otherwise it is misleading. Case law states that statements of opinion must be ‘genuinely

---

107 Eg, _Pacific Dunlop Ltd v Hogan_ (1989) 23 FCR 553.
The case of digital consumer manipulation

held’ or otherwise they can be misleading. Some eObjects can make decisions with high levels of autonomy, based on technologies with emergent properties, that is, ones that cannot be fully understood by humans. In such cases, proof that an opinion is genuinely held, or that statement as to the future is based on reasonable grounds, may be difficult to produce, particularly with highly personalised recommendations and those based on autonomous technological agents. This may cause problems for the provider/s responsible for Max’s services. If Jessica or the ACCC can lead evidence that the smartphone contract was not very advantageous to Jessica, the burden of proof will most likely shift to Max’s service provider.

3.3.4 ‘Effect or likely effect on conduct’

As stated by the Full Federal Court in Global Sportsman Pty Ltd v Mirror Newspapers Ltd, the Court must be:

concerned with the effect or likely effect of conduct upon the minds of those by reference to whom the question of whether the conduct is or is likely to be misleading or deceptive falls to be tested.

The test as to whether such conduct was misleading or deceptive is an objective rather than a subjective one.

In the context of DCM, there are two questions of concern when assessing the effect or likely effect of the conduct at issue, that is, whether it misled or deceived, or was likely to. First, who is the target audience? Second, what ‘standard of skill and care’ is required of that audience?

The ‘target audience’ for most forms of advertising is considered to be the public as a whole or a particular segment of the public. For example, in Australian Competition and Consumer Commission v TPG Internet Pty Ltd, where the allegations of misleading and deceptive conduct pertained to a multimedia advertising campaign offering an ADSL2+ service, the relevant audience were held to be those in the market for broadband services. For personalised advertising, as is the case with most DCM activities, the ‘audience’ would arguably be characterised as the individual target of the advertising, although this has not been tested. However, this may not always be the case. Some forms of personalised advertising are carried out without the advertiser knowing the ‘individual’ they are targeting. For example,


109 Burrell, above n 17, 10.


112 Ibid.


114 Lockhart, above n 105, 103–4 [3.25].

115 ADSL is an asymmetric digital subscriber line service. At the time, ADSL2+ was considered to be a high-speed version.

116 (2013) 250 CLR 640 (‘TPG’).
de-identified data are used by marketers and data brokers\textsuperscript{117} to create anonymised groups, which can then be served targeted advertising based on individual preferences or circumstances. This advertising can be achieved without the relevant advertiser ever having access to information about an ‘identified’ individual.\textsuperscript{118} Rather it can serve up specific ads to someone who, for example, is a female in the 40- to 55-year-old age group with primary school age children, a history of shoe purchases over a certain frequency, and is currently within 5 metres of a dynamic advertising screen in Westfield Burwood.\textsuperscript{119}

The standard of care expected of the target audience varies with the objective characteristics of the audience, including its size.\textsuperscript{120} For the public at large, or a segment of the public, there has also been a significant variance in approaches. Some UK statements based on the law of passing off have been quite broad, for example including all persons in the target audience other than ‘moron[s] in a hurry’.\textsuperscript{121} Early Australian formulations included:

the effect on a person, not particularly intelligent or well informed, but perhaps of somewhat less than average intelligence ... although the test is not the effect on a person who is, for example, quite unusually stupid.\textsuperscript{122}

This test is sometimes still quoted, at least by trial judges.\textsuperscript{123} However, the test, particularly as used in the High Court, has also been the subject of narrower formulations. Gibbs CJ in Parkdale Custom Built Furniture Pty Ltd v Puxu Pty Ltd considered that the relevant question was:

the effect of the conduct on reasonable members of the class. The heavy burdens which the section creates cannot have been intended to be imposed for the benefit of persons who fail to take reasonable care of their own interests.\textsuperscript{124}

The ‘reasonable care’ standard has been supported in a number of subsequent cases.\textsuperscript{125} The High Court in Campomar Sociedad Limitada v Nike International Ltd held the relevant question to ask is whether ‘the “ordinary” or “reasonable” members of the class of prospective purchasers of a

\textsuperscript{117} Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability (2014).


\textsuperscript{119} A large suburban shopping centre in Sydney, Australia.


\textsuperscript{121} Morning Star Co-operative Society Ltd v Express Newspapers Ltd (1978) 1A IPR 661, 664.

\textsuperscript{122} Annand and Thompson Pty Ltd v Trade Practices Commission (1979) 25 ALR 91, 102.


\textsuperscript{124} (1982) 149 CLR 191, 199.

mass-marketed product for general use' \textsuperscript{126} would be misled, and the Court could exclude the effect of those ‘whose reactions are extreme or fanciful’. \textsuperscript{127} However, the difference between an ‘ordinary’ consumer and a ‘reasonable’ one is still unclear. More recently, the High Court in \textit{TPG} \textsuperscript{128} also adopted the \textit{Puxu} formulation of ‘reasonable care’. However, it was subject to the qualification of a causal link connecting the defendant’s conduct and the error of the alleged victim. \textsuperscript{129} 

However, in \textit{Taco Co of Australia Inc v Taco Bell Pty Ltd} \textsuperscript{130} and \textit{Butcher} \textsuperscript{131} the Federal Court and the High Court respectively indicated that a different approach should be used when the target audience were ‘identified individuals’, as opposed to the public or a member of the public. Further to this, the High Court in \textit{Butcher} stated that when individual consumers seek specific redress such as damages, two criteria must be met. First, ‘[t]he plaintiff must establish a causal link between the impugned conduct and the loss that is claimed.’ \textsuperscript{132} Second, the Court must consider the subjective knowledge of both parties, including:

the character of the particular conduct of the particular agent in relation to the particular purchasers, bearing in mind what matters of fact each knew about the other as a result of the nature of their dealings and the conversations between them, or which each may be taken to have known. \textsuperscript{133}

This would appear to imply that judges can and should consider the enhanced knowledge marketers can gain about individuals using the data collection techniques made possible by eObjects. The Court however went on to hold that the assessment must continue by reference to what ‘a reasonable person in the position of the [alleged victim], taking into account what they knew, would make of the [alleged perpetrator’s] behaviour’. \textsuperscript{134}

However, Lockhart casts some doubt on the authority that a ‘reasonable person’ requirement applies in all cases. \textsuperscript{135} Instead, he proposes instead that \textit{Butcher} and subsequent cases were only intended to apply to relatively sophisticated purchasers and high value property, where a greater standard of care should be expected. His assessment of the interpretation of the ‘reasonable care’ standard in the High Court and lower courts is that ‘extreme, fanciful or unusually foolish interpretations of widely disseminated conduct’ will mean that the relevant sections are not breached, but ‘uncertainty remains’ as to what extent a ‘reasonable care’ standard can be applied. \textsuperscript{136}

Where does this leave DCM? If a criterion of ‘reasonable care’ is applied, this is problematic for at least some DCM cases. If the relevant conduct is
intended to exploit cognitive biases, it is intended to undermine the consumer’s very capacity to take such reasonable care. This renders the test insufficient. The focus of DCM techniques is to convert an ordinary, ‘reasonable’ consumer into a vulnerable one, in the sense that they are less likely to exercise reasonable care in making a decision to buy a supplier’s product or service. Marketers undertake this conversion in several stages. First, they undertake personalised data collection programs to discover what particular weaknesses and cognitive biases operate most strongly upon particular individuals. For example, in 2017, access to databases containing contact details of ‘wheelchair and insulin users, of people addicted to alcohol, drugs, and gambling, as well as ... suffering from breast cancer, HIV, clinical depression, impotence, and vaginal infections’ were offered on a commercial basis. Then, they find opportunities to exploit those weaknesses and biases in individuals, based on behavioural research. For example, in 2013, a US marketing firm released a study claiming to identify the day and times of week where women ‘feel their least attractive’, and then recommended a strategy to beauty product marketers ‘to heavy-up and wrap marketing ... activity around the days that the beauty consumer feels the best and worst about her image’.

It is not new that commercial entities hold and use large amounts of consumer data. What is new that is occurring at an unprecedented scale is the intensity and extensiveness of the collection, the sophistication of the processing, the degree of automation, and the social distance of marketer from customer. An example of this can be found in the vignette where Jessica and Fahim are the subjects of manipulative techniques designed to persuade them to buy consumer products. Each of Jessica’s and Fahim’s data profiles has been used to target them at a time and place designed to minimise resistance to entering into a transaction.

These techniques are not scattergun approaches designed to pull in as many consumers as possible, such as physical posters in a food court, or television ads, but are personalised to each of Jessica and Fahim, or at least to people with characteristics very much like theirs. Fahim has been targeted based upon time, location, and earlier purchasing patterns. Jessica’s manipulation by beauty product marketers is somewhat more sophisticated, consisting as it does of:

- identification of a possible vulnerability by surveillance of her comments to Max and the hairbrush’s use as data collector and signaller;
- embedding of vulnerability by the targeted storytelling ad on the electronic billboard in the shopping centre; and
- further pressure to purchase due to the location- and time-targeted discount.

137 Helberger, above n 4.
Some or all of these levels of manipulation might be considered *unfair*, in that they involve a business taking advantage of a vulnerable consumer.\(^\text{140}\) However, I argue that it is not on its face *misleading* or *deceptive*. It therefore falls outside the scope of prohibition contained in ss 18 and 29. For this reason, the imposition of the exigency mark-up on flowers for Jessica’s sister discussed above is also unlikely to breach s 18. Merely unfair or distasteful conduct does not constitute a breach of s 18 (or indeed s 29).

### 3.3.5 Conclusion

The ability of consumers to protect themselves may well improve over time, once consumers become more aware (and therefore warier) of these practices. Digital literacy programs in schools discussing digital marketing practices may assist increasing this awareness. However, a growth in understanding is likely to be hindered by the lack of incentive, or real disincentive, for service providers to reveal details of these practices. Corporate secrecy is likely to be maintained for as long as possible.\(^\text{141}\)

Where DCM involves a misrepresentation, ss 18 and 29 will apply to such conduct. Where the conduct does not amount to a representation, s 18 will only apply where the consumer is led (or likely to be led) into a factual error. If the error is a normative one, such as where the consumer’s biases are exploited to an extent that their actions are considered not ‘reasonable’, then the sections will not apply. In these circumstances, service providers are not providing the consumer with incorrect or incomplete information as to any innate attribute of the goods or services. Rather, consumers are being put in a situation where they are more likely to agree to buy them due to their own vulnerabilities, such as Jessica’s, Mylin’s and Fahim’s situations outlined in the vignette.

The analysis above shows that DCM techniques are not wholly unregulated by the existing law. Where DCM techniques lead consumers into a factual error, such techniques will infringe the *ACL* provisions on misleading and deceptive conduct and specific misrepresentations. However, sanctions arising under these provisions are commonly triggered when the relevant conduct produces or is likely to produce a detrimental effect on the ‘reasonable consumer’. In cases where there is no factual ‘error’, but the techniques nevertheless create a vulnerability to the extent consumers are persuaded to act unlike ‘reasonable’ or ‘ordinary’ consumers, these provisions will not provide protection to consumers from DCM.

Consumers may nevertheless find a remedy under other provisions of the *ACL*, such as those governing unconscionable conduct.

### 3.4 Unconscionable conduct

#### 3.4.1 Elements of unconscionable conduct

Conduct that is ‘unconscionable’ is prohibited under s 21 of the *ACL*. The question is to what extent the practices involved in DCM are liable to be


\(^{141}\) Pasquale, above n 16; Mik, above n 3.
considered as unconscionable. No definition of unconscionability is provided in the section, and Australian appellate courts have shown a marked reluctance to attempt a precise definition.

Section 21 prohibits unconscionable conduct in connection with the actual or possible supply of goods or services. Section 22 sets out a non-exclusive list of matters to which a court may have regard when assessing if conduct is unconscionable under s 21. Relevantly to DCM, these include:

- relative bargaining power (s 22(1)(a));
- undue influence or pressure, or unfair tactics (s 22(1)(d));
- comparative price (s 22(1)(e));
- consistency of a supplier’s conduct towards others (s 22(1)(f));
- unreasonable failure to disclose conduct affecting consumer interests or unforeseeable risks to the customer (ss 22(1)(i)(i)–(ii)); and
- the extent to which both parties acted in good faith (s 22(1)(l)).

Additionally, s 21(4) states as ‘interpretative principles’ that the doctrine:

- is not limited by the ‘unwritten law’ of unconscionable conduct;
- applies to ‘a system of conduct or pattern of behaviour, whether or not a particular individual is identified as having been disadvantaged by the conduct or behaviour’; and
- includes terms and performance, not just formation.

Mirror provisions exist in ss 12CB–12CC of the ASIC Act regarding the supply of financial services, and are relevant for similar reasons to the misleading and deceptive conduct mirror provisions (see Part 3.3.1).

Section 20 of the ACL, and its mirror provision s 12CA of the ASIC Act, also prohibit unconscionable conduct ‘within the meaning of the unwritten law’. However, I argue that these provisions will not directly apply to DCM, due to the operation of s 20(2) of the ACL and s 12CA(2) of the ASIC Act, which exclude conduct prohibited by s 21.

Remedies for breach of the unconscionable conduct provisions are significant. They are similar to those discussed in Part 3.3.1 for a breach of s 29 of the ACL, including pecuniary penalties. However, breach of the unconscionable conduct provisions does not attract a criminal remedy.

3.4.2 Meaning of unconscionable conduct

It is difficult to extract from the statute and the cases a precise meaning of ‘unconscionable conduct’ under s 21. One definition adopted in several decisions is ‘[s]howing no regard for conscience; irreconcilable with what is right or reasonable’. However, there remains no judicially accepted ‘standard of wrongdoing’. The courts have, deliberately it seems, embraced unconscionable conduct in relation to financial services’ (2005) 23 Company and Securities Law Journal 105, 107–9.


the ambiguity of ss 21–2 in a sacrifice to flexibility and broadness of applicability, as illustrated in the Full Federal Court decision in *Paciocco v Australia and New Zealand Banking Group Ltd* where Allsop CJ said:

In any given case, the conclusion as to what is, or is not, against conscience may be contestable. That is inevitable given that the standard is based on a broad expression of values and norms ... An agonised search for definition, for distilled epitomes or for shorthands of broad social norms and general principles will lead to disappointment, to a sense of futility, and to the likelihood of error. The evaluation is not a process of deductive reasoning predicated upon the presence or absence of fixed elements or fixed rules. It is an evaluation of business behaviour ... as to whether it warrants the characterisation of unconscionable, in the light of the values and norms recognised by the statute.145

Unfortunately, the cases have failed to articulate a clear statement of the ‘values and norms recognised by the statute’. A continuing controversy over whether unconscionability requires a ‘high level of moral obloquy’,146 ‘moral taint’,147 or some other standard149 has been unhelpful in clarifying the meaning of the section. In particular, the term ‘moral obloquy’ has been judicially condemned as notoriously imprecise.150 Even attempted substitutes, such as ‘accepted and acceptable community values’,151 have provided little assistance to those attempting to assess their own conduct or the conduct of suppliers.

In contrast, the definition of s 20 or ‘unwritten law’ unconscionability is somewhat clearer due to the seminal High Court decision in *Commercial Bank of Australia Ltd v Amadio*. Here, the Court required an ‘unfair or unconscientious advantage’ to have been taken of a party who was at a ‘special disadvantage’.152 The existence of an Amadio ‘special disadvantage’ may be relevant to the assessment of unconscionable conduct under ss 21–2, but it is not required.153 It also sets a higher standard than is required for ss 21–2 unconscionability. It is generally accepted that Parliament’s intention in ss 21–2 was to prohibit a wider range of unconscionable conduct than encompassed by the Amadio definition, and that this objective has been achieved.154

---

147 Eg, *Paciocco v Australia and New Zealand Banking Group Ltd* (2016) 258 CLR 525, 587 [188].
149 Brody and Temple, above n 140, 171; Paterson and Brody, above n 144.
150 Ispat Australia Pty Ltd v APS Satellite Pty Ltd (2018) 356 ALR 440, 496 [278].
151 *Australian Competition and Consumer Commission v Lux Distributors Pty Ltd* [2013] FCAFC 90 (15 August 2013) [23] (‘Lux’).
152 Amadio (1983) 151 CLR 447, 462 (Mason J); Supplementary Explanatory Memorandum and Corrections to the Explanatory Memorandum, Trade Practices Amendment (Australian Consumer Law) Bill (No 2) 2010 (Cth).
153 Explanatory Memorandum, Competition and Consumer Legislation Amendment Bill 2010 (Cth).
154 Paul Vout, ‘Unconscionability and Good Faith in Business Transactions’ (Paper presented at the National Commercial Law Seminar Series, Federal Court of Australia, Melbourne,
Other than the fact that s 21 unconscionability is broader than s 20, little more can be said with certainty about the applicable general principles. In 2016, Allsop CJ was optimistic that certainty would develop:

Over time ... the courts will develop principles and legally relevant considerations that will give comfortable form to fact situations ... the courts will work through the notion of a business conscience. This is not something foreign to the judicial process ...

However, despite the fact that the section is on its face technologically neutral, the discussion in the following sections indicates that as yet, there is no apparent ‘comfortable form’ to apply to a fact situation involving DCM.

3.4.3 Choice of flexibility over clarity

The choice of retaining flexibility over ‘fixed elements or fixed rules’ has been supported by successive Parliaments. The flexibility of the section does, on its face, leave room for it to accommodate emerging technologies and data-driven challenges to consumer protection. However, its meaning and effectiveness remain contentious, to the point of being considered ‘amorphous and ambiguous’, ‘a category of meaningless reference’, and ‘generically unhelpful’. Repeated criticism by consumers, small businesses and downstream suppliers has focused on the uncertainty of the section, particularly relating to the lack of specificity in the definition, the failure of the provisions to provide any real guidance to assess whether particular forms of conduct would be considered unconscionable, and difficulties of proof. Attempts by businesses and consumers to apply the section in any meaningful way to emerging technologies will face significant challenges.

Additionally, several other problems with statutory unconscionable conduct have been identified, relevantly:

- the lack of familiarity with, and understanding of, the term ‘unconscionability’ outside of the courts, particularly by business and consumers;

---

156 Paciocco (2015) 236 FCR 199, 276 [304].
157 Attorney-General (NSW) v World Best Holdings Ltd (2005) 63 NSWLR 557, 583 [118].
161 Sarida McLeod, ‘Statutory unconscionable conduct under the ACL: The case against a
• a high threshold level of misconduct,\textsuperscript{162} in that conduct which is merely unfair,\textsuperscript{163} or where one party has more bargaining power than the other,\textsuperscript{164} is unlikely to be considered as unconscionable without more;

• uncertainty as to the applicability of the factors in s 22 (discussed further below in this Part); and

• practical enforcement difficulties due to vulnerable victims either being unable to bring actions themselves or providing poor testimony for regulator actions.\textsuperscript{165}

The contention surrounding the doctrine has led to multiple government and parliamentary inquiries since the introduction of statutory unconscionability in 1986.\textsuperscript{166} There have been repeated requests to legislate for a specific definition, or to include a list of examples of unconscionable conduct in the ACL (similar to the unfair contract terms provisions).\textsuperscript{167} The government and parliamentary inquiries have led to some restructuring of the sections and amendments to supporting wording, such as the introduction of s 21(4). But on the whole, successive governments have refused requests for more specificity. Instead it has been recommended that the ACCC run test cases\textsuperscript{168} and issue guidance.\textsuperscript{169} However, the ACCC’s current guidance document for requirement for “moral obloquy”\textsuperscript{170} (2015) 23 Competition and Consumer Law Journal 123, 129; Paterson and Brody, above n 144, 352; Brody and Temple, above n 140.

\textsuperscript{162} Brody and Temple, above n 140, 170. See in particular the formulation in \textit{Australian Competition and Consumer Commission v Allphones Retail Pty Ltd [No 2]} (2009) 253 ALR 324, 347 [113] (‘Allphones’) which requires that ‘the actions of the alleged contravener show no regard for conscience, and be irreconcilable with what is right or reasonable’ (although note this was an interlocutory application).

\textsuperscript{163} AMI [2015] FCA 368 (22 April 2015) [39].

\textsuperscript{164} CG Berbatis Holdings Pty Ltd v \textit{Australian Competition and Consumer Commission} (2001) 185 ALR 555 (‘Berbatis’); \textit{Australian Securities and Investments Commission (‘ASIC’), Senate inquiry into the performance of the Australian Securities and Investments Commission – Submission by ASIC on reforms to the credit industry and ‘low doc’ loans} (2013) 6.

\textsuperscript{165} Brody and Temple, above n 140, 171.


\textsuperscript{167} ACL s 25.

\textsuperscript{168} Commonwealth, above n 166.

\textsuperscript{169} Horrigan, Lieberman and Steinwall, above n 166.
business does not inspire confidence: it begins its explanation of the term with the words ‘[u]nconscionable conduct can be a difficult concept to understand’.170

Section 22, which contains a non-exclusive list of matters that can be considered in an assessment of unconscionability, could have provided more fertile ground to ensure that the doctrine was given real content. However, the section itself gives no guidance on the extent to which these factors or others should be considered, and judicial guidance has been inconsistent. Some decisions discuss the factors explicitly.171 Others do not mention them at all,172 although arguably they are nevertheless identifiable in some cases without specific reference.173 No formula has been adopted as to how many, or to what extent, the factors must be present.174 It is worth noting, however, that the cases indicate that it is not necessary to show that one factor is determinative. A number of factors can be aggregated together, and a decision made based on ‘all the circumstances’.175 As to the importance of individual factors, it appears inequality of bargaining power, without more, is insufficient,176 and similarly, inadequate disclosure.177 However, little more than that of general principle can be drawn from the cases.

Many cases of DCM could be considered as cases of ‘undue influence or pressure’, or ‘unfair tactics’, which are factors under s 22(1)(d) to which the court may have regard in making a decision about unconscionable conduct. There are several cases where inappropriate pressure or unfair tactics have been considered unconscionable.178 However, these generally involve face-to-face or telephone contact between the seller representatives and the consumers.179 Commonly (although not exclusively),180 some aspects of the


174 Bruce, above n 91, 154 [6.10].


conduct either breached or was likely to breach other sections of the ACL, such as the door-to-door selling provisions, unsolicited consumer agreement provisions, and/or the prohibitions on misleading and deceptive conduct, and false and misleading representations. In *Australian Competition and Consumer Commission v ACN 117 372 915 Pty Ltd (in liq)* (discussed further in Part 3.4.4), considerable emphasis was placed on the nature of the misconduct emanating from a medical practice, ‘which characteristically make[s] patient welfare a primary concern’. On its face, s 21 unconscionability does not require a breach of other laws, an Amadio-style ‘special disadvantage’, or a duty above and beyond that of a normal business to its customers, but it remains uncertain as to where the line can be drawn. It also remains to be seen whether judges will be convinced that marketing messages delivered by SMS, a digital personal assistant such as Max, a doll such as Ella, or other non-human means have the same persuasive force as ‘real person’ (face-to-face or over the phone) high-pressure selling. Further public empirical research on the effectiveness of such would assist, as currently most such experimentation is proprietary to marketing companies profiting from it.

### 3.4.4 DCM as predatory business conduct

Despite the problems discussed above, some assistance can be found in two places. First, in 2015, Paterson and Brody conducted a detailed analysis of the judicial treatment of ‘predatory business conduct’. They examined cases involving ‘business models whose very operating premise relies upon taking advantage of the reduced ability of the consumers ... to protect their own interests’. They concluded that Australian courts have generally been successful in applying the unconscionable conduct provisions in the ACL and the ASIC Act to respond appropriately to a broad selection of predatory business conduct, such as funeral insurance, payday lending, and sale of inappropriate educational services to those dependent on social security payments.

Second, the distaste of judges for predatory business conduct, especially...

---

171 The case of digital consumer manipulation

---


183 *Lux* [2013] FCAFC 90 (15 August 2013).

184 *AMI* [2015] FCA 368 (22 April 2015) [905]. Some form of expected commitment to patient welfare was mentioned by the trial judge seven times throughout the judgment.

185 See, eg, Nadler and McGuigan, above n 21.

186 Paterson and Brody, above n 144, 332.

187 Ibid 346.

188 Ibid 332.
that targeting vulnerability, is also reflected in two important recent Full Federal Court decisions, *National Exchange Pty Ltd v Australian Securities and Investments Commission*189 and *AMI*.190 In the former case, the Full Federal Court held National Exchange had breached the relevant unconscionable conduct provisions of the *ASIC Act*.191 The subject of the case was National Exchange’s offer to shareholders of Aevum to purchase their shares, at a price well under market value. An accurate estimate of the shares’ market value was included on the reverse side of the offer document. The company’s controller admitted targeting members of demutualised companies that he believed were more likely to accept less than fair value.

The Full Federal Court held that the offer document was *not* misleading or deceptive.192 However, the targeting of inexperienced members and the framing of the document were held to be unconscionable because:

National Exchange set out to systematically implement a strategy to take advantage of ... a group of inexperienced persons who would act irrationally from a purely commercial viewpoint and would accept the offer. They were perceived to be vulnerable targets and ripe for exploitation, as they would be likely to act inadvertently and sell their shares without obtaining proper advice, and they were a predictable class of members from whom [National Exchange] could procure a substantial financial advantage by reason of their commercially irrational conduct ...

This is not a case of obtaining a low price by shrewd negotiation. It is predatory conduct designed to take advantage of inexperienced offerees.193

*AMI*194 concerned a claim of unconscionable conduct under the *ACL* relating to the marketing activities of a medical clinic. The trial judge, North J, (with whom the Full Federal Court agreed)195 discussed in detail the impact of *AMI*’s high-pressure selling techniques in ‘targeting vulnerability’, specifically the vulnerability of those seeking treatment for perceived sexual dysfunction. The judge, in finding *AMI*’s conduct in breach of s 21, declared that *AMI*’s ‘technique of selling was prone to rob men of independent judgement’.196 He also adjudged it ‘immoral to seek to harness the fears and anxieties of men suffering from [erectile dysfunction] or [premature ejaculation] for the purpose of selling medical treatments’.197

One view is that some forms of DCM are more severe, or against conscience, than the predatory business models discussed above. DCM in some cases is not marked by mere opportunism, but by a deliberate *intent* to track down, or even create, circumstances in which a vulnerability is likely to operate more strongly, and then to take advantage of it. Therefore, it appears

191 In this case, the relevant section breached was s 12CC, a mirror provision to s 51AC of the then *Trade Practices Act 1974* (Cth). The corresponding new provisions are *ACL* ss 21–2, and *ASIC Act* ss 12CB and 12CC.
193 Ibid 142 [43].
195 Appeal heard as *NRM* [2016] FCAFC 98 (7 July 2016).
196 *AMI* [2015] FCA 368 (22 April 2015) [896].
197 Ibid [892].
The case of digital consumer manipulation

possible that at least some DCM techniques would fall foul of the unconscionable conduct prohibitions. In the vignette, marketing disguised as a conversation between the 9-year-old Mylin and Ella, a doll to which she is emotionally attached, may indeed be considered unconscionable. If a marketer has access to and implements in its algorithms behavioural research that shows fatigue, blood sugar levels and time of day significantly affecting willpower, then unhealthy ‘nudges’ to Fahim, recorded in marketers’ databases as a diabetic, may also be seen as sufficiently predatory to contravene the provisions.

This result is supported by the words of the statute, particularly s 21(4)(b), which indicates that s 21 ‘is capable of applying to a system of conduct or pattern of behaviour, whether or not a particular individual is identified as having been disadvantaged by the conduct or behaviour’. The wording of this section suggests there is no need for proof of actual consumer disadvantage from the scrutinised conduct. Another possible consequence of s 21(4)(b) is that an attempt to exploit consumers (even if unsuccessful) is sufficient to breach the section. This is particularly noteworthy as the actual effectiveness of some behavioural marketing techniques is still controversial. The lack of a requirement to prove the behaviour’s effectiveness would stifle a potential defence by suppliers, making it easier for regulators to bring an action.

One possible counterpoint to this view is contained in two cases involving problem gamblers, both brought against the owners of the Crown Casino, Crown Melbourne Ltd (‘Crown’). These cases show a judicial predisposition to assuming consumers are perfectly rational and must look after themselves, even when their psychological traits, such as a gambling addiction or disorder, make doing so difficult. In the High Court decision of Kakavas v Crown Melbourne Ltd, Mr Kakavas suffered from a gambling addiction, which was known to Crown (at least constructively). However, this was dismissed as a basis for a holding of unconscionable conduct under s 20 and the ‘unwritten law’ on unconscionable conduct. The Court held that Mr Kakavas, who was a wealthy ‘high-roller’ gambler, did not suffer an Amadio-style ‘special disadvantage’, as the Court considered his gambling problem did not make him incapable of making rational decisions (including self-exclusion). The Court did concede that the result may have been different where a gambler was obviously drunk, young, old or ‘incompetent’.

A few years after the Kakavas decision, a group of individuals who had suffered large losses on poker machines brought a case against Crown and the supplier of the poker machines (Aristocrat Technologies Australia Pty Ltd). They alleged that the design of the Dolphin Treasure electronic gaming machine constituted unconscionable conduct in relation to players who were ‘vulnerable to becoming habituated and/or addicted to playing’ this particular kind of poker machine. In finding against the plaintiffs in Guy v Crown Melbourne Ltd [No 2], Mortimer J emphasised that it was a ‘significant

---

198 Mik, above n 3, 15.
199 (2013) 250 CLR 392 (‘Kakavas’).
200 Ibid.
201 Ibid 405 [30].
203 Ibid 530 [465].
challenge’ to prove that those with a gambling problem or disorder had ‘no capacity to make judgements for themselves’. On a strict construction of the Court’s language, both Kakavas and Guy would set a very high bar for proof in their ‘all or nothing’ attitude. A gambler must be rendered totally incapable of making rational decisions in order for unconscionability to be found. It would appear that impaired capacity, even significantly impaired capacity, is insufficient. As with gambling, a proof of total incapacity in relation to DCM is surely an unattainable goal.

However the application of these two cases to conduct in a wider context is uncertain, for a number of reasons. In Kakavas, the High Court emphasised the uniqueness of the activity involved: ‘Gambling transactions are a rare, if not unique, species of economic activity in a civilised community, in that each party sets out openly to inflict harm on the counterparty.’ Additionally, Kakavas was decided solely on the basis of a predecessor provision to s 20. However, Mortimer J’s decision in Guy suggests that there may be some applicability to the broader notion embodied in ss 21–2. Mortimer J’s ‘no capacity’ comments in Guy related specifically to the s 20 case and the assessment of a special disadvantage. However, in dismissing an additional claim based on ss 21–2 unconscionable conduct, Mortimer J stated that her reasoning in relation to s 20 had ‘some application’ to her decision on the ss 21–2 case. Mortimer J also acknowledged that:

There are real debates to be had, on the law and on the facts ... in relation to the state of research and knowledge about gambling addictions, and pathways to addiction.

3.4.5 Conclusion

Consumers, regulators and advocacy organisations may be able in some cases to find more useful protections for the more egregious forms of DCM under the statutory doctrine of unconscionable conduct, as opposed to a misleading or deceptive conduct claim. While the scope of the statutory doctrine is still undefined, the breadth of the potential definition of unconscionable conduct makes it likely that many forms of DCM will fall foul of the prohibition.

However, the operation of the unconscionability provisions in the face of DCM is uncertain. The lack of a useful definition of unconscionability, in addition to the lack of analogous cases, make it difficult to assess when and where DCM techniques would constitute unconscionable conduct. The uncertainty about what is considered ‘unconscionable’ is exacerbated by the current lack of clear societal norms about the acceptability of DCM, and the inability of the courts and Parliament to articulate real and useful content for the concept.

Judicial and parliamentary attitudes have certainly made the section flexible, but at what cost? The concept of unconscionable conduct is ‘technologically neutral’, so there is nothing on its face preventing it from applying appropriately to DCM and other forms of sociotechnical change. However, the failure of courts to articulate details of a test or principles to give

204 Ibid 537 [495] (emphasis added).
207 Ibid 530 [460].
content to the term ‘unconscionable’ makes it difficult for business and consumers to assess whether particular forms of new conduct, such as DCM, are indeed unconscionable. This uncertainty also provides a deterrent to bringing cases, particularly by consumers, but also by regulators. Governments may encourage the running of test cases, but they do not generally provide unlimited (or even particularly adequate) budgets to do so.

3.5 Other areas of relevant law

Other areas of relevant law worthy of further research are outside the scope of this article, including unfair contract terms, unsolicited consumer agreements, spam, and financial advice regulation. However, most are unlikely to apply to DCM generally, but rather to specific instances. While more general, the unfair contract terms regime excludes terms relating to subject matter and price, which are usually the most prominent in deciding whether to enter into a consumer contract. Other legal and equitable doctrines targeted against questionable practices in commercial dealings may also be worthy of further research, such as undue influence, undue harassment, duress and mistake. However, these are unlikely to provide substantial additional protection for a consumer who has been subject to DCM, as they tend to apply in far narrower circumstances than statutory unconscionable conduct. A consideration of the Contracts Review Act 1980 (NSW), which provides relief against unjust, harsh or oppressive contracts or contractual terms, is also excluded as it is limited to contracts where the law of New South Wales is the proper law of the contract.

The omission of a detailed analysis of data protection legislation from this article requires more substantial justification. While the regulation of marketing practices has traditionally been the domain of the ACL and its predecessors, misuse of consumer data is usually seen as falling under the remit of the Privacy Act. However, this section outlines some serious barriers to relying upon the Privacy Act to protect consumers from data-related harms.

First, there are many gaps in the Privacy Act’s protections. Threshold requirements exclude many businesses from its operation. There are also important exemptions from all or some of its provisions, such as employee records or disclosures to related bodies corporate.

Second, many types of consumer data may not be subject to the Privacy Act, as demonstrated in the recent decision in Privacy Commissioner v Telstra Corporation Ltd. This case set out a narrow definition of the meaning of

---

208 ACL pt 2-3.
209 Ibid pt 3-2 div 2.
210 Spam Act 2003 (Cth).
212 ACL s 26.
213 Ibid s 50.
214 In particular, Privacy Act 1988 (Cth) (‘Privacy Act’) s 6D excludes businesses with $3 million or less in annual turnover, unless they hold health information, are a credit reporting body, a Commonwealth contractor, or deal in personal information.
215 Ibid s 7B.
216 Ibid s 13B.
personal information ‘about an individual’. The definition of ‘personal information’ in the Privacy Act has since been slightly reworded to include ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable’, but I do not think this rewording improves the protection much for consumers. Much information of value to consumers and third parties will fall outside this definition, particularly if similar reasoning to the Telstra case is adopted. As discussed in Part 2.2, advertising can be personalised without the advertiser having access to information about an ‘identified’ individual.

This type of data processing can be used to engage in activities such as DCM, as well as other conduct of concern such as data-based discrimination. Concerns have already been expressed in Europe that this type of data processing does not fall within the EU’s definition of personal information in the new General Data Protection Regulation (‘GDPR’), and therefore will not attract its protection. The definition of personal information in the GDPR is much broader than that contained in Australia’s Privacy Act.

Third, enforcement mechanisms are weak, particularly for consumers. No direct right of action is available to consumers, although under s 36 of the Privacy Act they may make a ‘complaint’ to the regulator, the Office of the Australian Information Commissioner (‘OAIC’). OAIC decisions relating to complaints are only subject to review where the OAIC makes a ‘determination’ under s 52 of the Privacy Act. Few such determinations have been made under this provision, and this has resulted in a paucity of appellate jurisprudential development. Also, competitors have no right of action under the Privacy Act. Under s 18 of the ACL and its predecessors, competitor actions have provided significant impetus to enforcement of the misleading and deceptive conduct provisions.

Additionally, the sanctions that have been applied have been insubstantial. Compensation amounts awarded have been too small to have any meaningful deterrent effect. No civil penalties (available up to $1.8 million) have been awarded since their introduction in 2014, standing in stark contrast to some other jurisdictions such as the United Kingdom. Insufficient funding and resourcing of the OAIC, restricting its capacity to bring actions, has also attracted public criticism.

217 Privacy Commissioner v Telstra Corporation Ltd (2017) 249 FCR 24 (‘Telstra’).
218 See, eg, Bogle, above n 118.
224 Eg, Allie Coyne, ‘Starved of funding, resources, OAIC is left to shrivel’, iTnews (online),
Further, and most importantly, ‘consent’ overrides most safeguards for consumers in relation to the use of consumer data, and transfer to third parties. The consent required is weak, and its adequacy to protect data subjects vigorously contested.225 Commercial entities are permitted to deal with consumer data even though in most cases the nominal consumer consent obtained is not informed, is non-negotiable, and is subject to unilateral interpretation and extension at the will of the commercial party. In some cases, such as in direct marketing, where it is ‘impracticable to obtain consent’,226 even the requirement of weak consent is disregarded. This problem is exacerbated by forms of consent and privacy policies that are lengthy, difficult to understand, ambiguous, hard to find, vague and/or overly broad.227 Empirical evidence suggests this encourages consumers not to read most policies or helplessly accept unfavourable terms because ‘[i]t [is] the only way to access the product or service’.228 For all of these reasons, the Privacy Act is limited in its protections against DCM.

Consumer law provides a more fertile area to examine the existence of effective mechanisms. In particular, the drafters of the ACL and its predecessors recognised that ‘consent’ is insufficient to absolve sellers of responsibility in their marketing activities, and that consumers need to be protected against seller misconduct even when they have said ‘yes’ to a transaction.

4 Concluding remarks: Uncertainty, regulatory timing and corporate secrecy

The ACL provisions most likely to be called into action by consumers and regulators to offset harms brought about by DCM enabled by eObjects are technologically neutral. This may lead people to the conclusion that the provisions are broad enough and flexible enough to accommodate emerging technologies. This is a common argument provided by those advocating broadly drafted ‘neutral’ provisions. However, the analysis above has shown that while some forms of DCM may be caught, the provisions are insufficient to protect consumers from many harms caused by DCM due to uncertainty. I argue that the ACL’s unconscionable conduct provisions on their face should have provided a useful tool to protect consumers from unfair tactics and exploitation of consumer vulnerabilities. However, the uncertainty engendered by overly broad drafting and unhelpful case law has provided little

---

226 Eg, under the Australian Privacy Principle 7, which regulates direct marketing.
228 Nguyen and Solomon, above n 23, 59.
guidance to business, consumers and regulators. This provides a strong disincentive to both proactive good practice and the likelihood of enforcement actions.

The uncertainty of the unconscionable conduct provisions is not confined to DCM. However, the negative effects of uncertainty may be greater in the context of sociotechnical change compared to other forms of social change, because of its relative speed. Various parliamentary inquiries have suggested that the specificity craved by consumers and small business groups could be dealt with by the regulator running test cases, rather than facing the administrative burden of providing examples within the legislation that must be continually updated. They have also suggested the use of guidance material by the ACCC. However, a number of problems arise from these suggestions in the context of sociotechnical change, particularly around effective regulatory timing.

First, the judicial process invoked in running test cases has many problems, although I will mention only two here. Despite all of the attention given in recent years to efficient case management, litigation remains very slow and expensive. As discussed above, it has not previously produced useful general principles easily applied by businesses engaging in different conduct. If useful cases are produced too slowly, or not at all, then society ends up on the side of the Collingridge dilemma where it may be too late to mitigate harms because of entrenched interests. A judge’s decision disrupting profitable business models will not be popular with corporate political donors, and will likely lead to attempts to limit its effects. In any event, judges have previously accepted arguments that conduct that is ‘normal’ or ‘ordinary’ business practice should not be considered unconscionable. Therefore, conduct left unchecked for too long may create its own legitimacy, to the detriment of consumers and others.

The use of guidance material as a substitute for stronger regulation has also been subject to criticism. Cortez’s case study about the failure of guidance material to substitute for appropriate regulation and enforcement discussed in Part 1 is subject to a US regulatory context and therefore the results cannot be applied without caution in the Australian regulatory landscape. However, it does raise questions that should be addressed. In particular, to what extent can the preservation of ‘flexibility’ as the dominant factor in making decisions about regulation — and vaunted as a virtue in the cases on unconscionable conduct — lead to ‘legal procrastination’ and a ‘regulatory inertia’ hard to break without a significant and public failure?

Negative effects of uncertainty are likely to be exacerbated by corporate secrecy and other forms of opaqueness. It is generally known that commercial entities and their third party contractors conduct a large amount of

---


230 Eg, Australian Competition and Consumer Commission v Woolworths Ltd [2016] FCA 1472 (8 December 2016).


experimentation on consumer responses to the digital environment, but these are kept confidential.\textsuperscript{233} This makes the specific details of the experiments and their results difficult to come by.\textsuperscript{234} There is no incentive — rather the opposite — for service providers and marketers to disclose to consumers or regulators the full extent of data collected and used, or the nature of the cognitive biases or vulnerabilities they choose to attempt to exploit. Suppliers unsurprisingly favour vague, broad and generic privacy policies. There are some circumstances where suppliers have actually ostensibly attempted to provide more information such as in advertisements on some social media sites saying ‘Why am I seeing this ad’.\textsuperscript{235} However, empirical research has found this information to be ‘incomplete’, ‘misleading’, and ‘vague’.\textsuperscript{236} It is counterproductive for service providers to disclose to consumers when and how they use DCM techniques, due to the possibility of decreased effectiveness,\textsuperscript{237} (although this does not always occur)\textsuperscript{238} and/or reputational damage due to consumer backlash. The employment and job description of behavioural psychologists, and algorithm writers, is not something most suppliers will willingly reveal to consumers. The very design of such techniques is intended to preclude self-discovery by consumers.

Without a working understanding of the data collected, the inferences drawn from that data, and what companies know about the effects of behavioural advertising, there is every chance that consumers will not actually realise what has actually happened to them, other than a case of buyer’s remorse. They will ask themselves the question ‘why did I do something so irrational or so harmful?’, without having any idea someone is to blame other than themselves.

The lack of transparency of DCM techniques is just one example of the recent issues arising around market and algorithmic transparency. For example, Pasquale has sketched out other possible detrimental consequences of the growing collection of data by corporate actors, where use and abuse are screened from data subjects’ view due to permitted corporate secrecy practices.\textsuperscript{239} Other scholars have delineated problems in state use of data and algorithms, for example in policing contexts.\textsuperscript{240} In Europe, legislators have recognised the need to address the problems that a lack of transparency can bring, such as inappropriate discrimination in decision-making by algorithms. As a result, the EU’s GDPR attempts to restrict some forms of automated individual decision-making, including a ‘right to explanation’ of algorithmic

\begin{footnotesize}
\begin{itemize}
  \item\textsuperscript{233} Nadler and McGuigan, above n 21, 156.
  \item\textsuperscript{234} Ibid 156.
  \item\textsuperscript{235} Eg, Facebook, Twitter.
  \item\textsuperscript{237} Mik, above n 3, 8.
  \item\textsuperscript{238} Nadler and McGuigan, above n 21.
  \item\textsuperscript{239} Pasquale, above n 16.
\end{itemize}
\end{footnotesize}
decisions. However, the efficacy of this attempt has already been doubted.

As the use of data analytics increases, and transparency decreases, the likelihood of disbenefits for consumers and other data subjects is likely to increase. I argue this type of lack of transparency falls under Bennett Moses’ category of a ‘new harm’ type of legal problem. The new activities now made possible by the eObjects’ attributes, particularly hyper-personalised profiling, and algorithmic microtargeting of marketing campaigns, may lead to an opaqueness unprecedented in the consumer space: in other words, a mass inability to know our own minds.

It is beyond the scope of this article to develop solutions to these problems, but I offer some preliminary observations that could form the basis for further research. The adoption of an ‘unfair conduct’ prohibition, such as in the United States (15 USC § 45) and the EU (Art 5 Unfair Commercial Practices Directive), will be effective only if defined underlying principles provide content to this doctrine, in order to avoid the existing problems with the unconscionable conduct regime. The introduction of ‘privacy by design’, such as contained in the GDPR (Art 25), is attractive because of the relative newness of the eObjects consumer industry. However, massive amounts of consumer data already exist ‘in the wild’ due to conventional ecommerce practices, and data collection by existing eObjects continues apace. Realistically, much of this data cannot be returned to consumers: it has escaped for good. The effectiveness of disclosure and consent regimes for consumers is questionable.

Schemes for disclosure to regulators (possibly commercial-in-confidence to prevent unnecessary trade secret disclosure) may be more fruitful in preventing harms when there is a commitment and mechanism for a swift legislative response. Specific regulation targeting inappropriate conduct, such as particular forms of behavioural advertising or inappropriate recommendations, may be needed, preferably in a form amenable to quick review and assessment to keep it up-to-date. The use of technology assessment panels or specialist agencies may assist in this objective.

Entrenched corporate secrecy practices and a consequential lack of transparency are not new. However, these are now combined with new and powerful ways to collect, disseminate, analyse and use data for an overwhelmingly one-sided benefit. Certain attributes of eObjects add to that power, both because of the nature of the data that can be collected, and the ways in which it can be used to manipulate consumer behaviour. As DCM

241 GDPR Art 22.
243 Christl, above n 23.
244 Omri Ben-Shahar and Carl E Schneider, More Than You Wanted to Know: The Failure of Mandated Disclosure (Princeton University Press, 2014).
enhanced by eObjects relies on emerging rather than mature technologies, a ‘wait and see’ strategy by law and policymakers may seem attractive. However, the price of delay is significant. As businesses invest more in developing business models around the collection and use of this data, as well as in the development of new eObjects to further their marketing activities, their resistance to subsequent restriction of these activities will increase. Without substantive and properly informed attempts by regulators and legislators to understand the extent and disbenefits of this behaviour in the present, the opportunity for effective and efficient regulation may pass by.
Emerging information technologies: challenges for consumers

Kayleen Manwaring

To cite this article: Kayleen Manwaring (2017) Emerging information technologies: challenges for consumers, Oxford University Commonwealth Law Journal, 17:2, 265-289, DOI: 10.1080/14729342.2017.1357357

To link to this article: https://doi.org/10.1080/14729342.2017.1357357

Published online: 17 Aug 2017.

Article views: 71

View related articles

View Crossmark data
Emerging information technologies: challenges for consumers

Kayleen Manwaring

School of Taxation & Business Law, UNSW Business, University of New South Wales, Sydney, Australia

ABSTRACT
A ‘third wave’ of computing is emerging, encompassing technologies that have been called many names, including ubiquitous and pervasive computing, ambient intelligence, the Internet of Things and eObjects. This third wave will bring about significant socio-technical change, especially in the lives of consumers. With this change comes the possibility of a disconnection between consumer protection law and the new things, activities and relationships enabled by the third wave. This article analyses the attributes of these technologies, and identifies where consumers may face challenges relating to acquisition and interaction. These challenges are appraised in the light of common consumer protection principles, to identify whether likely detrimental outcomes for consumers may conflict with these principles. This article provides a basis for consumer protection lawyers in Commonwealth jurisdictions to examine whether or not their current consumer protection legislation can adequately provide appropriate consumer protection in the face of the third wave.

ARTICLE HISTORY
Received 1 February 2017; Accepted 15 May 2017

KEYWORDS
Internet law; eObjects; consumer protection; Internet of Things; ubiquitous computing; ambient intelligence

1. Introduction
A ‘third wave’ of computing is emerging, encompassing devices and infrastructures that depart from conventional forms of distributed computing, embedding miniaturised and networked computers in everyday objects, such as cars, fridges, people and animals. This third wave has the potential to bring about significant socio-technical change, especially in the lives of consumers who acquire and/or interact with these technologies. With this change comes the possibility of disconnections between current consumer protection law and the new things, activities and relationships enabled by the third wave.1

CONTACT
Kayleen Manwaring kayleen.manwaring@unsw.edu.au


© 2017 Faculty of Law, Oxford University
In most jurisdictions, there is limited legislative or judicial analysis of the possibility of such disconnections, although recently some industry and consumer groups have begun preliminary policy evaluations. As these technologies become more prevalent, legislatures, policy-makers and judges will all need to consider whether existing law can adequately regulate the new things, activities and relationships now emerging. This paper is intended to provide a basis for lawyers in different jurisdictions to examine whether their current laws provide acceptable levels of consumer protection in the face of the third wave.

Third wave technologies have been called many names, such as ubiquitous and pervasive computing, ambient intelligence, and the Internet of Things. The inconsistency and intersecting nature of terminology usage over country, time and research institution make the use of all or any one of these terms problematic. To avoid these problems, in this paper I adopt Manwaring and Clarke’s approach developed in 2015, and use the term ‘eObjects’ (enhanced objects), which is more fully defined in Section 2.

Most of the discussion of eObjects to date has concentrated on the inadequacy of existing privacy and data protection laws. These are undeniably important to consumers, but do not tell the whole story. Until recently, only a small amount of literature raised misgivings about other effects on consumers and their contracts with suppliers. From late 2015, however, greater

---


4 Manwaring and Clarke (n 3).


concern began emerging in some government departments and consumer
groups about these types of challenges for consumers acquiring and interact-
ing with eObjects.7 These challenges can arise not only in relation to the attri-
butes of eObjects themselves, but also out of contractual arrangements used
to supply them to consumers.

Section 2 of this paper outlines the scope of the emerging technologies
discussed in this paper and provides a definition of ‘eObject’. Section 3
describes a set of consumer protection principles (CPPs) derived from the
Guidelines).8 Section 4 uses the eObjects framework summarised in Section
2 to identify the challenges consumers may face when entering into a con-
tract relating to eObjects. Section 4 proceeds to identify whether likely detri-
mental outcomes for consumers faced with these challenges may conflict
with the CPPs. This provides a basis for Commonwealth scholars and policy-
makers to assess whether their consumer protection laws are adequate to
address the supply to and use of eObjects by consumers. Section 5 concludes
the article by highlighting some of the most important legal areas that bear
further investigation in individual jurisdictions.

2. eObjects and the socio-technical landscape

In short, an eObject (as defined by Manwaring and Clarke) is an:

\[
\text{object that is not inherently computerised, but into which has been embedded one or more computer processors with data-collection, data-handling and data communication capabilities.}^{9}
\]

Such a shorthand definition, while helpful, cannot be complete, considering the
variety and complexity of the technologies involved. eObjects already appear in
many industries, including transport, utilities, healthcare, building, industrial
and home automation, agriculture, fitness and lifestyle, toys, entertainment,
consumer appliances, logistics, sport, security and art. Many examples of eOb-
jects are discussed in this paper, including Internet-connected kettles, cars,
fitness trackers, heart defibrillators, children’s and adults’ toys, guns, locks, e-
book readers, fridges and thermostats, but there are many more.10

To focus attention for further research and give a more complete view of the
technologies, Manwaring and Clarke developed a framework with three dimen-
sions: core attributes, interactions and common attributes. The core attributes
are italicised in the definition above. Four key types of interactions with eOb-
jects were also identified: living things, the physical world, other eObjects,

---

7eg Coll and Simpson (n 2); Vukanovski (n 2).
9Manwaring and Clarke (n 3) 599 (emphasis added).
and other computing devices or systems. Common attributes of eObjects do not appear in all eObjects, and even where they do appear, the nature and significance of their effect can vary. However, the italicised attributes below have been identified because they appear sufficiently frequently, and have such effects, that they are capable of driving significant socio-technical change either by themselves or (more likely) in combination with other attributes or interactions. These common attributes are: **active capacity** (capability to act on the physical world), **adaptability** (context-awareness), **addressability** (unique address), **associability with living beings**, **autonomy**, **dependency** (on remote services or infrastructure), **geo-locatability**, **identifiability** (unique device identifier/s), **mobility or portability**, **operational, economic and social impact**, **network locatability**, **prevalence**, **use pattern**, **visibility**, **volatility** and **vulnerability**.

This framework with its italicised attributes is used in Section 4 to identify the challenges consumers may face when acquiring eObjects.

### 3. Consumer protection principles

The 2015 Guidelines were adopted by the UN General Assembly in December 2015, comprising a revised version of Guidelines originally adopted in 1985 (Old Guidelines). The 2015 Guidelines contain a set of principles intended to describe ‘the main characteristics of effective consumer protection legislation, enforcement institutions and redress systems’. These CPPs can be summarised as follows.

<table>
<thead>
<tr>
<th>Section of 2015 Guidelines</th>
<th>Description</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>III.5(a), V.E</td>
<td>Consumers should have access to essential goods and services</td>
<td>Essentials</td>
</tr>
<tr>
<td>III.5(b), IV.11(a)</td>
<td>Consumers who are vulnerable or disadvantaged should be protected</td>
<td>Disadvantage</td>
</tr>
<tr>
<td>III.5(c), V.B, V.D</td>
<td>Consumers should be protected against threats to health and safety</td>
<td>Safety</td>
</tr>
<tr>
<td>III.5(d), IV.11(b), V.C</td>
<td>Consumers should be protected against unfair practices, such as misleading marketing practices and unfair contract terms</td>
<td>Fairness</td>
</tr>
<tr>
<td>III.5(d), V.C</td>
<td>Businesses should supply goods and services which are durable, reliable and fit for purpose</td>
<td>Quality</td>
</tr>
<tr>
<td>III.5(e), IV.11(c)</td>
<td>Consumers should be given access to sufficient information to make informed individual choices</td>
<td>Information</td>
</tr>
<tr>
<td>III.5(f), V.G</td>
<td>Consumers should be given access to education programmes</td>
<td>Education</td>
</tr>
<tr>
<td>III.5(g), V.F</td>
<td>Effective dispute resolution and redress should be provided to consumers</td>
<td>Redress</td>
</tr>
<tr>
<td>III.5(h)</td>
<td></td>
<td>Representation</td>
</tr>
</tbody>
</table>

(Continued)
Continued.

<table>
<thead>
<tr>
<th>Section of 2015 Guidelines</th>
<th>Description</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>III.5(i), V.H</td>
<td>Sustainable consumption by consumers should be promoted</td>
<td>Sustainability</td>
</tr>
<tr>
<td>III.5(j), V.I</td>
<td>Consumers using electronic commerce should be given no less protection than is provided in other forms of commerce</td>
<td>Parity</td>
</tr>
<tr>
<td>III.5(k)</td>
<td>Consumers’ privacy should be protected</td>
<td>Privacy</td>
</tr>
</tbody>
</table>

The most significant changes introduced by the 2015 Guidelines include:

- the inclusion of the CPP of Parity for electronic commerce;
- a consumer right to Privacy and
- protection against Disadvantage.

The consumer protection principles contained in the Old Guidelines have generally been adopted, in whole or in part, by UN member states, including Commonwealth countries. Of course, the consumer protection laws in each Commonwealth jurisdiction differ in their detail, and there has been little time for UN member states to revise their consumer protection legislation to ensure compliance with the 2015 Guidelines. However, the history of broad adoption of the UN Guidelines means the CPPs provide a useful preliminary basis on which to assess the adequacy of a Commonwealth country’s consumer protection law in the face of socio-technical change brought about by eObjects.

4. Challenges for consumers

So what aspects of eObjects might pose challenges for consumers that may conflict with these CPPs? This paper argues that consumers face significant challenges due to the following features of eObjects:

- eObjects are imperfect (see Section 4.1);
- eObjects can be controlled and modified remotely by suppliers and others in the provider network (see Section 4.2);
- eObjects can manipulate or impede consumer choice (see Section 4.3);

16I use this term ‘provider network’ in preference to the commonly used ‘supply chain’, as the latter term implies linear progressive connections. In an eObject context, the provider connections are much more likely to be distributed or weblike in nature rather than linear.
eObjects have a significant post-supply value to suppliers and other related goods and services providers (see Section 4.4) and eObjects are complex (see section 4.5).

4.1. Imperfection

Suppliers with low profit margins and limited experience in manufacturing computing products may have little incentive or capability\(^\text{17}\) to ensure that eObjects operate reliably. Possible harms to consumers faced with the challenges described in this section raise potential conflicts with the CPPs of Quality and Safety and with other CPPs, as set out below.

4.1.1. Risks of failure

Vulnerability is an important attribute of consumer eObjects. In the early days of eObjects, Satyanarayanan argued that eObjects are more prone to physical interference and remote attacks than conventional connected computers.\(^\text{18}\) A deluge of subsequent reports supports this view. Security vulnerabilities have been identified in: fitness trackers;\(^\text{19}\) medical eObjects such as insulin pumps, heart defibrillators and CT scanners;\(^\text{20}\) domestic appliances such as Internet-connected kettles,\(^\text{21}\) baby monitors,\(^\text{22}\) children’s toys\(^\text{23}\) and location trackers;\(^\text{24}\) as well as guns\(^\text{25}\) and cars,\(^\text{26}\) just to name a few.

\(^{17}\)Peppet (n 5) 135–36.
The increased risk of security exploits arises from security vulnerabilities in both the eObjects themselves and the systems to which they are connected; they include inadequate encryption, weak passwords, lack of account lock out, poor authentication, authorisation and updating practices, and lack of physical safeguards.27 The nature of many manufacturers as consumer goods specialists rather than ICT specialists, the small size of many devices, and design flaws prohibiting software patches have all been cited as reasons why security problems arise so commonly in eObjects.28

Security attacks enabled by these vulnerabilities include unauthorised remote operation of the eObject (‘hacking’) and/or the delivery of malware. When these attacks occur, sensitive data might be disclosed or modified, or the eObject could be used to attack other eObjects or conventional computers. In September 2016, the website of security journalist Brian Krebs experienced a distributed denial of service attack delivered primarily through eObjects.29 Of course, such attacks are also delivered using conventional computers; what is more particular to eObjects is the physical harm that might occur to the eObject, surrounding objects and/or living things.30

The potential for physical harm is likely to emerge when the attribute of vulnerability interacts with that of mobility and/or active capacity. Security researchers have found ways to control connected cars’ locks, brakes, steering and transmission remotely.31 Internet-connected kettles have been exposed as significant security threats.32 Hackers can potentially wrest control from drivers of heavy objects travelling at speed or find an entry point into a smart home where connected sprinklers could be turned off and hotplates turned on. Ransomware, already used to breach the security of medical eObjects,33 offers a financial incentive to threaten such harm.

---


31See n 26.

32Cimpanu (n 21).

Many, if not most, eObjects or their associated systems have the attribute of volatility: limited or intermittent access to resources needed to operate, particularly network connections, energy sources and processing power.\textsuperscript{34} This constraint is a particular challenge for users of mobile eObjects, where the size, weight and form of the eObject dominate design decisions,\textsuperscript{35} often at the expense of resource allocation. Mobile eObjects currently need to be designed to minimise power usage, which can negatively affect processing power and speed. For simple applications, this constraint may matter little; but for healthcare eObjects, the draining of a power source or the loss of connectivity leading to loss of control can cause serious harm, even death.

\textbf{4.1.2. Risky decision-making: inaccuracy and autonomy}

All eObjects can collect, handle and communicate data.\textsuperscript{36} Data may be or become inaccurate during the eObject’s performance of any of these processes. Sensors can be misled by physical phenomena; algorithms can be wrong; data records can be corrupted. Questions have been raised about the accuracy of accelerometers\textsuperscript{37} and sleep trackers.\textsuperscript{38}

Consumers, the provider network and others who rely on accurate data (eg users and receivers of insulin injections) are, of course, at risk of physical or other harm if such data is inaccurate.\textsuperscript{39} This is particularly the case where the eObject has autonomous decision-making capabilities: decisions may be made for the user without adequate notification and/or capacity for manual override. Even before eObjects were produced, risks were identified in autonomous objects with active capacity. In the mid-80s, two people died and others were injured when computerised radiotherapy machines in hospitals administered massive overdoses of radiation to patients, partially due to an incorrect zero value in a failsafe counter.\textsuperscript{40} Although the risks are not new, the increased prevalence of autonomous eObjects can potentially increase the likelihood of such incidents occurring, particularly when such objects are also vulnerable to security breaches.

Even when data are accurate, eObjects with some autonomous decision-making capability are risky. Decision-making algorithms could be
programmed to result in outcomes not desired by the user. Consumers rarely see the content of such algorithms, and most are not equipped to understand them even if they did. Additionally, there are some machine learning technologies in development where it is anticipated that decision-making will not be completely deterministic, meaning that even the original programmers may not be able to predict the results.41

An eObject’s decision-making capabilities could also cause economic harm, for example if it institutes a contract for purchase not desired by a consumer. Consider the automatic reordering function in products such as Amazon Dash Buttons:42 who is liable to pay if 1,000 cartons of washing detergent are ordered instead of one, due to a failure in the eObject?

In addition to issues around Safety and Quality, there is a risk that the provider network will not provide sufficient Information. The Redress CPP may also be compromised, as autonomous decision-making raises the fundamental question of liability for the actions of a machine: who is liable for an unfavourable and unwanted contract entered into by a machine, which was not predictable by the machine’s user (or indeed its programmer)?

4.1.3. Management of risk
All eObjects contain hardware, software and a physical object (which may be a living thing). Very many eObjects also constitute what Helberger calls a ‘product-service package’,43 where services are provided along with the object. These elements of an eObject may have been provided by different entities, such as the manufacturer of the object, the programmers of the embedded software, the providers of cloud data storage and processing services, and other actors, depending on the complexity of the eObject and the system in which it participates.44

Risk management is complicated by the nature of eObjects as product-service packages, and further so when there are multiple players in the provider network. There are three main challenges:

- Proactive management of risk: what are the provider network’s obligations in relation to monitoring and updating of software?45

---

44See eg Guido Noto La Diega and Ian Walden, ‘Contracting for the “Internet of Things”: Looking into the Nest’ (2016) 7 (2) European Journal of Law and Technology 1, for a detailed description of the large number of product and service providers that can be involved in provision and support of an eObject.
45Christiane Wendehorst, ‘Consumer Contracts and the Internet of Things’ in Schulze and Staudenmayer (n 43) 189, 194–95.
• When things go wrong: who is responsible for fixing problems with the eObject?46
• What limitations will entities in the provider network attempt to place on their obligations regarding risk management?

Considering the risks outlined above, these are important things for the consumer to know before entering into a contract. Say a consumer lives in a house with a smart lock system. She has just separated from her partner, who until the separation lived at the same address. Due to threats of violence, she has changed the password on the locks, and has taken out an apprehended violence order against her ex-partner. Hackers discover a vulnerability in the system and publish details on how to exploit it on the World Wide Web.

The consumer would be concerned with the following questions:

• Does the provider network undertake any security monitoring?
• Will she be notified if there is a vulnerability? And if so, when?
• Who is responsible for supplying security patches and when will they be available?
• If urgent repair is needed, and either the provisions for repair or the agreed timeframe is inadequate, what rights does she have to bring in a third party to secure the lock? (Any locksmith can fix or replace a conventional house lock, but will administrative passwords or proprietary knowledge of other security measures be required to fix or replace a lock in a smart home?)
• What limits does the contract place on supplier liability for damage caused due to the failure of the smart lock? Does it cover repair, damage to property and personal harm?
• If the ex-partner is the contracting party for the locking system, what redress does the consumer have?
• What happens if the security provider goes out of business?

Consumer judgement on the adequacy of answers to these questions may be essential when choosing between competing products. Information that is not readily available, or is unintelligible or imprecise, will lead to a conflict with the CPP of Information. In addition, if suppliers are allowed to drastically limit their liability without some form of core responsibility, this will come into conflict with the CPPs of Safety, Quality and Redress.

4.2. Remote control

The capacity of eObjects for data-handling and data communication, and in some cases their dependency on remote services and infrastructure, exposes
consumers to a number of challenges. eObjects and associated services may be designed to allow entities in the provider network to control or modify the eObject, the data held within it, and/or the services supplied along with the eObject, potentially without the consumer even realising what has been done and certainly without the means to prevent it. This can raise issues in ensuring the CPPs of Fairness and Safety are not compromised.

Most physical consumer goods are only subject to change imposed by time or by parties controlled by the customer. However, the potential for remote modification in eObjects means that members of the provider network may be able to:

- disable temporarily or permanently all or part of an eObject’s functionality;
- programme the eObject to work differently;
- remove or modify digital content stored on the eObject and/or
- prevent changes by the user to the eObject, for example the modification of personalisation features or the removal of data.47

A connected eObject can be remotely disabled from working, for example where a purchase instalment or a related service fee has not been paid. Starter interrupt devices (installed in approximately 2 million cars in the US by late 2014) allow lenders or their agents to remotely disable a vehicle using their mobile phone, which they are contractually entitled to do when owners are late on car repayments.48 This ability to remotely disable an eObject gives the provider network powerful new private enforcement capabilities, leading to some unique situations. For example, the remote triggering of a starter interrupt device in a car reportedly prevented a mother from taking her asthmatic child to the hospital, and another woman was forced off the road when her car powered down, allegedly due to the use of an interrupt device by her lender.49

Other forms of disablement are less direct, and much less likely to be subject to overt consumer agreement or understanding. Revolv’s smart home hub hardware and application was shut down less than two years after release, after Revolv was acquired by a company that refused to support the product.50 This ‘bricking’ of eObjects can be effected in other ways, such as in the case where a supplier issues an upgrade to firmware or other software that reduces the speed of the eObject’s data-handling

49Corkery and Silver-Greenberg (n 48).
capabilities to a level that makes the hardware unusable. Or a service provider may go into liquidation or simply decide to discontinue a service, such as cloud data storage and processing. This can make the eObject worthless to the consumer, for example where the eObject was designed to communicate only with a proprietary service. In the end, a consumer may have no choice but to buy a new device with upgraded hardware, or to pay a premium price for an upgraded service. Other than the impact on individual consumers, this contribution to the world’s e-waste problems could also breach the CPP of Sustainability.

Digital content that is resident in or accessed through eObjects may well be blocked to protect rights holders; such as when there is no record of a user holding a licence to that content, but also in cases where the consumer has not been involved in a breach of contract or any wrongdoing. For example, in 2009, Amazon remotely deleted copies of the novel 1984 from customers’ e-book readers when Amazon discovered it had been made available in its store by an unlicensed vendor.

Some types of remote disablement may produce the same result as a court order. However, the challenge for consumers subsists in the one-sided nature of the remedy, as well as the immediacy and the inflexibility of such supplier reactions. Safeguards brought about by the engagement in a formal dispute resolution process, overseen by a neutral party, the court, will no longer apply to protect the consumer except well after the detriment has had an impact.

The situations outlined above indicate a clear conflict with the CPP of Quality, and in some cases, Safety and Redress. It is worthwhile noting that in these situations, the eObject as originally supplied to the user may well have been fit for purpose. It may be only afterwards, by a deliberate or inadvertent act by the supplier or someone else in the provider network, that the case becomes otherwise. Suppliers’ ability to act in this way, often supported by non-negotiable contractual terms explicitly granting the right to such modifications, could also conflict with the CPP of Fairness.

4.3. Consumer choice

Some attributes of and interactions involving eObjects can remove or impede consumers’ freedom of choice, and detrimental effects on consumers arising from this limitation of choice are most likely to compromise the CPP of

---

52Wendehorst (n 45) 201–02.
54Coll and Simpson (n 2) 35–36.
Fairness. Some behaviours may also be incompatible with the CPPs of Disadvantage and Information.

4.3.1. Digital market manipulation

Evidence presented to a recent US enquiry asserted that existing smartphone sensors can currently be used to infer:

- a user’s mood; stress levels; personality type; bipolar disorder; demographics (e.g., gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson’s disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement.\(^55\)

This type of information can be very valuable to a marketer attempting to persuade consumers to buy their products. In fact, a number of attributes present in eObjects are helpful to such a marketer, particularly when viewed in conjunction with the development of sophisticated data-processing techniques.

Many eObjects are mobile, and even for those that are embedded rather than mobile, the mobility of people interacting with the embedded object can increase the amount and variety of data collected, especially considering the increasing prevalence of eObjects. The value of geo-locational and data-collection technologies in marketing has been enhanced by the use pattern of eObjects, as they are likely to be ‘personal’; that is, intimately associated with an individual. This personal use pattern greatly enhances both the value of the geo-locational functionality and the utility of the data gathered and communicated by the eObject.

Data utility is also increased by the adaptability attribute (also known as ‘context-awareness’). Adaptable eObjects identify in real time some part of user context, and vary their responses accordingly. As the use of eObjects becomes more widespread, this increases the likelihood that a greater quantity of data—and data that is more intimate and personalised in quality—can and will be collected and processed. Inferences potentially derived from all of this data can be used for purposes that the owner of the eObject might find beneficial: for example, better targeting of advertising. However, there are also less beneficial uses. Digitisation of commerce generally (mediated through both conventional desktop ecommerce and eObjects) may give firms with large marketing budgets an enhanced ability not only to target consumer preferences but to exploit consumers’ cognitive biases and individual vulnerabilities.\(^56\) For example, advertisers may filter the available information; they may target consumers at the time when their willpower is


\(^{56}\)Calo (n 6) 1 ff; Kim (n 6) 312; Helberger (n 43) Part II; Eliza Mik, ‘The erosion of autonomy in online consumer transactions’ (2016) 8 Law Innovation and Technology 1, 1 ff; James Halliday and Rebekah Lam, ‘Internet of Things: Just Hype or the Next Big Thing? Part II’ (2016) 34 Communications Law Bulletin 4, 7.
lowest; or they may craft their advertisements to act upon known purchasing triggers of particular individuals, for example, feelings of guilt or obligation, or concerns about missing out, or a desire to emulate friends or celebrities. Calo has dubbed this practice ‘digital market manipulation’.

Currently, most examples of digital market manipulation have been identified in conventional ecommerce. However, the use of eObjects in these practices is increasing. Beacon implementations, such as Apple’s iBeacon, combine precise geo-location and context data (such as proximity, preferences, buying history and time of day) to target marketing communications. These implementations use indoor positioning devices and low-power sensors to track subscribers’ mobile phone signals. For example, when a person’s phone is located close to the menswear section in a department store, this might trigger an SMS to that person offering a discount on ties. Although the use of beacon technology is not yet widespread, in 2016 it was being used or piloted by retail, fast food, sporting, airline, real estate services, pharmacies and other business enterprises.

So why does this matter? Consumers have always been on the receiving end of persuasive tactics from advertisers. Data collected by eObjects will arguably provide significant advantages to marketers in accuracy, scope, scale and effectiveness. The impact of scale in particular may be amplified by the implementation of software (eg Silverpush) that allows tracking across different consumer devices, particularly if done without the knowledge of the consumer. The key question is ‘at which point digital marketing practices, and in particular if they are based on intrinsic data analysis, opaque algorithms and sophisticated forms of persuasion, turn the normally “average” consumer into a vulnerable one’.

It is clear that some forms of digital market manipulation have the potential to conflict with the CPPs of Disadvantage and Fairness. However, what is unclear is where the line should be drawn. Generally, society accepts that a marketer’s job is to convince a consumer to do something: but it is unclear when this type of behaviour would cross over from ‘normal’ marketing.

---

57 Calo (n 6) 1.
58 Ibid.
59 iBeacon uses the Bluetooth Low Energy communications standard, but other beacon technologies use both Bluetooth and Wi-Fi (eg Motorola Solutions and Datzing).
61 Kim (n 6) 312.
62 Hartzog and Selinger (n 50) 591–92.
63 Helberger (n 43) 160.
practice into something that is considered to be ‘unfair’ persuasion. Should those with particular ‘vulnerability profiles’ be able to claim greater protection than the ‘average’ consumer? For example, society may look askance at a marketer who targets a habitual gambler with an offer of an extended limit on her credit card as she passes a betting shop. However, the attitude towards someone who is persuaded to buy a face cream just because his favourite celebrity’s voice is used to persuade him to take advantage of a discount as he passes the cosmetics aisle in his local department store may be less sympathetic.

4.3.2. Consumer ‘lock out’
The prevalence of eObjects may lead to a scarcity problem: non-eObject versions of consumer products may become unavailable. Consumers with legitimate concerns about the attributes and interactions of eObjects and their disadvantages, such as in the areas of privacy and security, may find it impossible to opt out.

Where dependency on remote resources is essential to the functionality of the eObject, this can also lock certain consumers out. Regional areas in many Commonwealth countries may not have the connectivity required for particular eObjects. If it is not profitable to make non-eObject versions, then rural and regional residents may have to function without the object at all.

This problem would appear to directly affect the CPP of Disadvantage and, possibly in the future, the CPP of Essentials.

4.4. Post-supply value
The use pattern of eObjects can allow significant post-supply value to be exploited; for example, in reuse or sale of the data collected by the eObject, or the long-term recoupment of contractual premiums for licences or other services provided. Many eObjects return value for suppliers additional and separate to the upfront price paid for the underlying object. For example, a fridge that is not an eObject delivers little or no post-sale value for its supplier. On the contrary, the supplier maintains a significant post-sale obligation, in the form of warranties. However, the potential for post-sale value in eObjects is significant. For example, a smart fridge may deliver post-sale value to a supplier in the following ways:

- data on consumption patterns may be on-sold to supermarkets;

---

64 Calo (n 6) 1032.
65 Coll and Simpson (n 2) 38.
ongoing service fees, such as for software maintenance and updates, or cloud data processing and handling;

- commissions for automatically ordered produce from a retail partner and

- effective brand loyalty, once consumers looking to buy a new fridge realise if they switch brands they will need to re-enter all of their ordering data (a form of consumer ‘lock in’).  

4.4.1. Data

Privacy and data protection issues dominate the scholarly and popular literature on eObjects. To deal with these issues in full in relation to eObjects is outside the scope of this paper. However, some data-gathering practices by suppliers in relation to eObjects have a direct impact on consumer contracts, so they will be discussed briefly in this paper.

Consideration for eObjects in a consumer transaction is often not confined to a money price. The most common form of additional consideration is a requirement of consent to the provision of personal data. Demand for data did not of course begin with eObjects, but the greater amount of data made available by eObjects, based on the prevalence and mobility of such objects, considerably increases the likelihood of suppliers requiring data as a mandatory part of the consideration for the supply contract.

The developmental tendency of the design of many eObjects towards reduced visibility can also affect this situation, to the detriment of the consumer. Unobtrusiveness of the data-gathering function in many eObjects can intensify existing problems around data collection, storage and redistribution. An effectively invisible eObject will not advertise the data being collected, and if that is the case, how can a person unknowingly interacting with it exercise any real choice in prohibiting or limiting the use of information gathered?

The eObject itself need not be invisible in order to cause problems, just its data-gathering function. In 2016, an Illinois consumer brought a class action against Standard Innovation (US) Corp, the manufacturer of the ‘We-Vibe’ vibrator. Consumers and their partners can pair the We-Vibe via Bluetooth with a smart phone to allow for remote control of the device. The plaintiff in the Illinois action alleged that the manufacturer programmed the smartphone app to:

- secretly collect intimate details about its customers’ use of the We-Vibe, including the date and time of each use, the vibration intensity level[,] … mode or pattern selected by the user … and … the email address of We-Vibe customers … allowing [Standard Innovation] to link the usage information to specific customer accounts.  

67 Coll and Simpson (n 2) 47.
68 Wendehorst (n 45) 193–94.
The complaint alleged this was done without consumers’ consent or knowledge, and made the obvious point that most customers would not have bought the We-Vibe if they had known about this data collection.\(^{69}\) This is a clear breach of the new CPP of Privacy, and the litigation was settled on 9 March 2017, for CAD5 million.\(^{71}\)

Two significant challenges for consumers arise in relation to the data demanded by suppliers as part of the supply of eObjects. These are ensuring that consumers:

- are aware of what data are being collected, to whom it will be provided, and for what purpose (‘data awareness’) and
- can take their data with them if they terminate their use of the original eObject, for example, to move to another brand (‘data portability’).

If these challenges are not met by the provider network, the concern arises that the CPP of Information may also be compromised. Also, mandatory data requirements, even when the consumer has been fully informed, could arguably breach the Fairness CPP in certain circumstances.\(^{72}\)

### 4.4.2. Post-supply restrictions

The fact that eObjects contain a programmable computer with data collection and handling capabilities means that some form of software will be provided in every eObject. Some types of eObjects, such as e-book readers and networked media players, will also contain a substantial amount of digital content aside from software.

Post-supply restrictions on the consumer may arise in many different ways. For example:

- consumers may be required to enter into an ongoing service contract, such as for cloud data processing and storage;
- the eObject may not be ‘sold’ to the consumer, in the sense of granting full transfer of property rights—the supply contract may be a lease or licence, imposing an obligation to return the eObject on breach or termination;\(^{73}\)
- the supply may be subject to restrictive licence terms for the software or other digital content, such as those restricting copying, modification or particular types of use (included in separate agreements such as End

---

\(^{69}\)Complaint, *NP v Standard Innovation (US) Corp* (Case No 1:16-cv-08655, US District Court for the Northern District of Illinois) [19].  
\(^{70}\)Complaint, *NP v Standard Innovation (US) Corp* (n 69) [23].  
\(^{71}\)Class Action Settlement Agreement, *NP v Standard Innovation (US) Corp* (n 69).  
\(^{72}\)Helberger (n 43) 147–51.  
\(^{73}\)Walker Smith (n 47) 1815–16; Fairfield (n 6) 83; Hon, Millard and Singh (n 39) 16.
User Licence Agreements (EULAs) or alternatively in the supply agreement itself). These terms may also effectively prevent resale of the eObject, even if property in the physical device is transferred outright and

- the original set-up of the eObject may impose mandatory and irreversible personalisation of the eObject (such as user names, inability to delete data) that may limit its resale attractiveness.\(^{74}\)

Challenges for consumers arising out of these post-supply obligations include:

- post-supply notification: consumers may not be aware at the time they ordered the eObject that the post-supply obligations would apply or be mandatory, such as when an agreement to a EULA is required as part of set-up;
- greater restrictions on use compared with a non-eObject version;
- greater restrictions on resale by consumers even when the physical eObject is owned and not leased or licensed, as the EULA on software essential to the functionality of the eObject may be non-transferable\(^{75}\) and
- more significant penalties for breach of use restrictions, such as those contained in anti-hacking\(^{76}\) and/or copyright legislation, as opposed to civil remedies for contractual breach.

For example, if consumers wish to make their own repairs to an eObject, such as a connected vehicle, they may need to access integrated software, and face both legal and technical barriers to do so. Software modification without provider consent will in many cases be a breach of the EULA and/or copyright legislation. Modification may also be technically impossible without circumventing technological protection mechanisms (TPMs), often an illegal act itself in jurisdictions signatory to and compliant with the WIPO Copyright Treaty.\(^{77}\) Providers might also use their remote disablement capacity (see Section 4.2) to lock down software for a perceived breach of copyright law or contractual conditions.\(^{78}\)

These challenges are not merely theoretical. For several years, US farmers have been disputing the attempts of Deere & Company (John Deere) and

\(^{74}\)Wendehorst (n 45) 201.


\(^{76}\)Walker Smith (n 47) 1815–16 and fn 313.

\(^{77}\)World Intellectual Property Organisation Copyright Treaty, opened for signature 20 December 1996, entered into force 6 March 2002. Art 11 requires signatories to provide adequate legal protection and remedies against TPMs.

\(^{78}\)This possibility was suggested by one of the OUCLJ anonymous reviewers.
other manufacturers to restrict their rights to repair their agricultural machinery, which contains embedded software and TPMs.79 In 2015, against the objections of John Deere and others,80 the US Copyright Office granted a three-year exemption for vehicle software modification to the anti-circumvention provisions of the Digital Millennium Copyright Act81 (DMCA).82 A year later, John Deere issued a licence agreement which prohibits almost all software modification and circumvention of TPMs,83 in what appears to be an attempt to replace its DMCA rights with contractual rights84 and ensure that all repairs are done by John Deere contractors.

These types of post-supply obligations can severely restrict a consumer’s choice, not necessarily of the first purchase of the eObject, but as to third-party service providers and the subsequent purchase of other products. These types of ‘walled gardens’ may unreasonably fetter effective competition.

Suppliers and others in the provider network will need to make consumers aware of any post-supply restrictions on use, in order to comply with the CPP of Information. Unreasonable restrictions on post-supply use will also compromise the CPP of Fairness.

4.5. Complexity

The core attributes of an eObject mean there is no such thing as a ‘simple’ eObject. Each eObject is a hybrid of software, hardware and physical object, usually inseparable,85 and many eObjects are dependent on additional services, such as data processing. Software and services are often supplied by more than one entity in the provider network. Systems with nested and/or multiple eObjects, or multiple eObjects interacting with conventional computing, such as smart homes, can be very complex, both technically and in terms of associated service contracts.

Two types of complexity produce challenges for consumers:

81§1201(a)(1), Title 17, USC.
84Koebler (n 79).
85Noto La Diega and Walden (n 44) 8; Coll and Simpson (n 2) 33.
• the complexity of the technology itself and
• the complexity of the contractual arrangements associated with supply.

The nature of eObject ecosystems promotes the likelihood of numerous actors in the provider network. A complex network means complexity in contractual arrangements and therefore liability allocation. Even a basic eObject such as a thermostat may require many separate contracts dealing with hardware, software development, software licences, installation, website and app usage, payment services, connectivity provision, sale, distribution and rental.86 These contracts may be with separate entities, some having no connection with (or knowledge of) others in the network.87

The complexity of contractual arrangements within a network can make it difficult to identify all applicable contracts, let alone interpret them for end-consumers (including enterprises) and network actors.88 For example, the Nest thermostat is sold subject to at least 13 documents stipulating the ‘rights, obligations and responsibilities’ of the various parties in the provider network.89 Therefore, the likelihood of conflicting terms and conditions90 is high, as is uncertainty regarding their effects.

Challenges for consumers therefore arise in meeting the CPPs of Information and Redress.

4.5.1. Making an informed choice
A consumer entering into a contract requires sufficient, accurate and intelligible information on the nature, features and dependencies of the product or service, in order to meet the CPP of Information. A supplier of a simple product needs only provide minimal information to fulfil this requirement. The complexity of eObjects, particularly product-service packages, dictates that more than minimal information is required to sufficiently inform a consumer. And mere provision of information by one supplier is insufficient—the consumer’s knowledge of alternatives on offer and their judgement of the price and quality differences are also required.91

Consumers face three main challenges to receiving adequate Information:

• the type of information required (content);92

86Noto La Diega and Walden (n 44) 4–6.
87Hon, Millard and Singh (n 39) 7.
88Noto La Diega and Walden (n 44) 3.
89Noto La Diega and Walden (n 44) 6.
90Hon, Millard and Singh (n 39) 16–17, citing generally an earlier version of Noto La Diega and Walden (n 44).
92See section 4.5.1.1.
whether the consumer can adequately understand the information provided (intelligibility)\textsuperscript{93} and
when and how the information is provided (delivery mechanism).\textsuperscript{94}

\textbf{4.5.1.1. Content.} Consumer knowledge of the eObject’s functionality is important, as is its suitability for the consumer’s particular purposes. Knowledge of ‘normal’ functionality is usually insufficient, particularly for eObjects with significant volatility and/or dependencies: such eObjects face significant limitations on functionality in particular situations.\textsuperscript{95}

Knowing exactly what the eObject does enables consumers to assess whether it meets their needs. This knowledge is also important because the post-supply value of eObjects (particularly data collection) can incentivise suppliers to include features that benefit the supplier or others in the provider network but are a disbenefit to consumers and therefore affect their purchasing decision. Such functionality may be \textit{invisible} or unobtrusive; overt disclosure of this ‘dark’\textsuperscript{96} functionality may need to be formally required, otherwise consumers may remain unaware of it, as in the We-Vibe example above.

Aside from functionality, the attribute of \textit{dependency} and the nature of eObject interactions mean specific information on interoperability is often critical. A smart kettle that cannot connect to a particular type of home network has limited utility. If a homeowner is not told the kettle is only usable if connected through the homeowner’s mobile network (with associated higher data costs), the bargain may be substantially different to what they expect. Alternatively, particular systems may only allow add-in of particular brands of eObjects,\textsuperscript{97} thereby restricting consumers’ freedom of choice.

Clear information on price is fundamental to any consumer contract. This includes not just the price of initial supply, but also follow-on costs, such as purchase of additional applications, subscription fees for service agreements and costs of consumables. Consumers should also be aware of non-money considerations, such as post-supply obligations, for example in relation to data and use restrictions.

Ascertaining payment terms and the consequences of failure to pay may also be problematic, particularly when billing is done by more than one

\textsuperscript{93}See section 4.5.1.2.
\textsuperscript{94}See section 4.5.1.3.
\textsuperscript{95}Wendehorst (n 45) 191–92.
\textsuperscript{96}This term is adopted from the ‘dark scenarios’ terminology used in the SWAMI research project. See David Wright and others (eds), \textit{Safeguards in a World of Ambient Intelligence} (The International Library of Ethics, Law and Technology, Springer 2008).
\textsuperscript{97}Coll and Simpson (n 2) 37.
provider network entity. Payment terms, such as due dates and price increases, may vary greatly between entities.

Gaps in providing this content may compromise the CPP of Information.

4.5.1.2. Intelligibility. An additional information challenge inherent in complexity is that ‘consumers cannot make well informed decisions when they are presented with information that is incomplete, misleading, overly complex or too voluminous’.98 Opaque wording and technical terms are the norm for software and hardware contracts, and initial research indicates this has not changed for eObjects.99 The content provided may be accurate, but if it is not intelligible to the average consumer, it is insufficient to enable an informed choice.

Consumers also find contractual terms and conditions difficult to understand.100 Careless drafting adds to the problem. Researchers have identified terms and conditions in contracts involving eObjects that contain wording obviously written for older technologies and not properly redrafted.101 A common practice in information technology contracts is to use wording drafted for one jurisdiction in contracts made for another. US standard drafting is commonly used in European102 and Australian103 contracts, even when not particularly suitable. This latter issue is not new for eObjects, but it adds to problems of complying with the CPPs of Information and Fairness.

4.5.1.3. Delivery mechanism.

Behavioural economics has demonstrated that, among other things, the manner in which information is presented and the way that choices are framed can significantly influence marketplace choices, sometimes in ways that are not in the best interests of a consumer.104

A clear theme of early visions105 of ubiquitous computing was the idea that technology should merge into the background. An eObject or associated system may be designed so that interactions are invisible or at least unobtrusive.106 This is often achieved by removing or miniaturising text-supporting

---

99 See the analysis of the Nest thermostat contractual arrangements in Noto La Diega and Walden (n 44) 6ff.
100 Ibid 3, 9.
101 Ibid 3.
102 Ibid.
103 This observation is from the author’s own experience as a solicitor in Australia specialising in commercial negotiation of information technology contracts.
104 OECD (n 98) 10.
106 See section 4.5.1.1 above.
interfaces such as screens. Such interfaces cannot practically be used to deliver most contractual terms and conditions.

In some cases, this does not matter. Suppliers can provide a hyperlink to the terms and conditions when an eObject is ordered online, or provide printed terms and conditions over the counter or in the box for a bricks-and-mortar purchase. However, in other cases, the contractual processes encourage ‘lack of proximity between consumers, contract terms and the contract formation process’, a phenomenon labelled ‘Contract Distancing’.107 Contract Distancing leads to consumers entering into contracts with significantly limited access to terms and conditions and, consequently, a reduced ability to understand the bargain. Contract Distancing practices are seen both at contract formation and where initial contracts allow for unilateral amendments by the provider network.

Clear delivery of full terms before purchase of eObjects is not ubiquitous. Consumers may be given the price upfront on purchasing the product, but not be presented with other terms and conditions (such as EULAs, service agreements and maintenance agreements) until well into the set-up process—that is, after the product has been ordered, delivered, unpacked and partially or even fully set up.

Therefore, consumers may face challenges in finding out the terms and conditions applicable to their eObject, particularly in relation to data usage. Peppet’s 2014 survey of 20 commercially available consumer eObjects found that suppliers had not included anything in the box or packaging relating to data, privacy or security.108 While the relevant terms and conditions were displayed on the website, many eObjects were bought in bricks-and-mortar stores. Therefore, consumers were at risk of buying these eObjects without any knowledge of those terms, as there was no clear indication the purchase was subject to further terms and conditions.

If consumers do not receive proper notification of contractual terms due to Contract Distancing, the Information CPP is breached. Contract Distancing also removes the notification some steps away from the actual transaction, raising a question about the CPP of Fairness. Fairness is further compromised if Contract Distancing is combined with a supplier’s right to unilateral amendment without a corresponding consumer right to terminate without penalty, as in some fixed-term contracts.

4.5.2. Complexity’s effect on redress

The complexity of eObject ecosystems can hamper the allocation of liability for faults. Even where liability is clear, the mobile nature of eObjects and

---


108Peppet (n 5) 141, 167–78.
the differing locations of provider network actors can make practical enforcement difficult. Commonwealth consumers are particularly affected, as most eObjects they purchase are imported, with contracts likely to contain foreign jurisdiction and foreign law clauses. These impediments, combined with the usually low value of a consumer claim relative to legal costs, often hinder consumers achieving Redress.

The complexity of the technology and the contractual arrangements produces a significant challenge for consumers. Defects in an eObject ecosystem causing detriment to consumers can arise in several places, including physical faults in the dominant object or embedded computer hardware, bugs in the software, corruption or deletion of data or failure of network connections. And the overall detriment may arise from a combination of defects, as where a network failure corrupts data, causing the eObject to fail to recognise critical inputs.

Where a single supplier provides the hardware, software and associated services, liability allocation is relatively simple, limited only by whether the type of harm is legitimately excluded under the contract. But where there are multiple providers, the issue becomes uncertain. And where entities from multiple jurisdictions are involved, with different rules for allocating liability (under tort, contract or statutory provisions), this uncertainty multiplies. Contract drafters for provider networks also inevitably attempt to avoid liability, using favourable jurisdiction and choice of law clauses, or arbitration and class action waivers—practices already common in conventional ecommerce.

All of these uncertainties are likely to obstruct proper Redress for consumers, particularly in relation to low-value contracts. However, consumers are not the only ones facing detrimental effects. Uncertainty about the legal liability of provider network actors may hinder investment and innovation in eObjects.109

5. Conclusion

This paper has identified a number of challenges for consumers in consumer transactions arising out of new things, activities and relationships made possible by eObjects that bear further investigation and analysis in Commonwealth and other jurisdictions as to whether they are likely to give rise to legal problems. Identification of legal problems is crucial at an early stage of technological development, to assist in avoiding two problems: the first is the stifling of beneficial innovation by overregulation, the second is the cementing of socially undesirable outcomes if vested interests are left unchecked for too long.110

110 Manwaring (n 1).
It is important to note that the fact that consumers may have challenges to face does not automatically imply that legal problems exist in particular jurisdictions. Depending on the jurisdiction, legislation or other rules may exist that have direct application to the new activities, things or relationships causing consumers concern. Even in circumstances where there are no decided cases that discuss that law’s application to eObjects, such a law could still exist.\textsuperscript{111} For example, both contract law principles and the consumer protection provisions applicable in Commonwealth countries such as Australia and the UK are generally quite broad and generic, and are, at least to some extent, not technologically specific.

However, the challenges identified are not just mere inconveniences to consumers. This paper is intended to lay the basis for further examination of particular laws in the Commonwealth and elsewhere, as to whether or not these challenges are currently addressed, in whole or in part, by the law in specific jurisdictions. Early literature on eObjects made it clear that laws concerning consumer privacy need to be a priority for further examination.\textsuperscript{112} However, this paper goes past a focus on privacy to examine other problematic areas. Laws concerning safety and quality also need urgent examination to deal with widespread security problems already evident in eObjects, and particularly the potential for physical harm. Incentives for suppliers to provide intelligible and timely information to consumers must also be evaluated to ensure that complexity of the technology does not effectively negate consumer choice and effective competition. Less evident in current technologies, but likely to be a concern as technologies develop and become more prevalent, is the potential for unfair marketing practices that target already vulnerable consumers or even create them. It is also important that consumer access to appropriate redress for breaching other CPPs be protected, as this forms the foundation of the efficacy of those other principles.

\textbf{Acknowledgements}

The author thanks Associate Professor Lyria Bennett Moses and Professor Leon Trakman of the University of New South Wales Law School, for their helpful comments on earlier versions of this paper. She also thanks the anonymous reviewers for their useful feedback and Marie-Louise Taylor and Lilla Wendoloski for their editing assistance. However, all errors and omissions are the author’s own.

\textbf{Notes on contributor}

\textit{Kayleen Manwaring} is a lecturer at the University of New South Wales, School of Taxation and Business Law.

\textsuperscript{111}Bennett Moses (n 1) 252–53.
\textsuperscript{112}See n 5.
Six things every consumer should know about the ‘Internet of Things’

June 8, 2017 6.11am AEST

At least 40% of Australian households now have at least one home “Internet of Things” device. These are fridges, window blinds, locks and other devices that are connected to the internet.

While the Internet of Things (IoT) may lead to more efficiency in our daily lives, my research shows that consumers are exposed to many risks by the use of IoT devices, ranging from disclosure of private information, to physical injury and problems with the devices themselves.

Australia has no specific laws aimed at addressing IoT issues, and current laws intended to protect consumers have gaps and uncertainties when dealing with IoT devices.

1) Your devices can spy on you (and your kids)

Many IoT device manufacturers and suppliers show little regard for customers’ privacy. Some even make money from customer data.

Consumer electronics company Vizio recently agreed to pay US regulators US$2.2 million, after allegedly failing to get appropriate consent from users to track their TV viewing habits.
Late last year, the Norwegian Consumer Council found that a children’s doll recorded anything said to it by children and sent the recordings to a US company. The company reserved the right to share and use the data for a broad range of purposes.

2) Many IoT devices are vulnerable to hacking

The same doll was also found to have a security flaw that allowed strangers to talk and listen through the doll. Security vulnerabilities such as these can be exploited to cause damage in both the physical and virtual worlds.

IoT devices were recently involved in some of the largest “distributed-denial-of-service” attacks - flooding websites with traffic until they crash. The recent huge attacks on internet company Dyn and on the security researcher Brian Krebs were in large part fuelled by hacked IoT devices.

But hacked IoT devices can also be dangerous by themselves. In 2015 Fiat Chrysler recalled 1.4 million vehicles when security researchers proved they could break into smart cars’ systems remotely and control brakes, steering and transmission.

3) Your devices are never really yours, even after you pay for them

Most IoT devices come with some form of embedded software, and the devices won’t work properly - or sometimes at all - without it. This software is usually licensed, not sold, and the conditions imposed through licence agreements can hinder users’ repairing, modifying or reselling their devices.

This can be anti-competitive, as individual users are effectively “locked in” to one brand and one supplier.

For several years now, US farmers have been in a dispute with agricultural machinery manufacturers such as John Deere, over their rights to repair tractors that contain embedded software.

The farmers were granted a three-year exemption to certain copyright laws in 2015. However, John Deere is fighting back.

In October 2016, the company issued a new licence agreement which prohibits almost all software modification on its tractors. This action appears to be an attempt to ensure all repairs are done by John Deere contractors.

4) Your devices know your weaknesses

IoT devices have the potential to collect more intimate data about individuals than was possible with previous devices. This data can then be used to create profiles that give incredible insight into consumers, and can even predict their behaviour.

For a number of years now we’ve known that the embedded technology in smartphones can be used to detect users’ mood, stress levels, personality type etc.
But some IoT devices can collect even more intimate and personalised data. This was evident after a recent out-of-court settlement by a wireless vibrator manufacturer allegedly collecting data without consent.

The consumer profiles that can be built with all this data can then be used to sell us products at times when our willpower is lowest. Retailers are currently using technology to track consumers through stores and send customised messages to mobile phones. This may be linked to our purchase history and what is known about our mood.

**5) It’s almost impossible to know what you’re getting yourself into, or how long it will last**

Many IoT products are complex hybrids of software, hardware and services, often provided by more than one supplier. What your rights are when things go wrong, and who best to fix it for you, can be hard to figure out.

A recent investigation of the Nest thermostat system revealed that if consumers wanted to understand all of the rights and obligations of those in the supply chain, they needed to read a minimum of 13 different contractual documents.

Even if you know and trust your supplier, they may not be around forever. And when they go, services essential to their products working may disappear as well.

Revolv, a maker of home automation devices, was shut down after the company was acquired by Nest, which was itself acquired by Google. Nest refused to support Revolv’s products, and they stopped working less than two years after being released.

**6) The law may not protect you**

Many IoT devices put consumer privacy at risk, but the Privacy Act has significant limitations, as the definition of “personal information” is very narrow. The Act doesn’t even apply to many Australian companies, as they do not meet thresholds such as having A$3 million in annual turnover.

Consumers and regulators may attempt to pursue device suppliers under the consumer guarantees in the Australian Consumer Law. But there are grey areas here too. We don’t know what “acceptable quality” is when it comes to some of these devices, for instance. Is an internet-connected kettle that boils water perfectly well, but can be easily hacked, of acceptable quality?

**Proceed with caution**

Consumers are exposed to significant risks from IoT devices, from predatory use of data, to security flaws and devices no longer being supported. Meanwhile Australia has no specific laws aimed at addressing these IoT issues.

The most recent review of the Australian Consumer Law recommended investigating “emerging technologies” be made a priority. It is vital that a close examination of consumer protection relating to
IoT devices be included front-and-centre in this project.

In the meantime, consumers should think long and hard about the risks they are taking on with IoT devices. Do you really need that internet-connected hairbrush?

Found this article useful? A tax-deductible gift of $30/month helps deliver knowledge-based, ethical journalism.

Make a donation