# Submission to ACCC inquiry on digital platforms

Benjamin C. Dean
*15 February 2019*

***Key points:***

1. The concept of privacy embodied in preliminary recommendations 8(f) and 10 are outdated and not in line with the practices of digital platforms. Policy measures premised on this concept of privacy will not be effective at addressing the competition, fair trading and consumer protection issues created by these companies' practices.
2. Information asymmetry, due to collection and monopolization of data, allows digital platforms to perform potentially anti-competitive practices, unfair trading and harm consumer welfare. These acts could be in breach of the Competition and Consumer Act 2010. Examples include forcing competitors out of the market; theft of data and associated value from users; and appropriation of consumer surplus through price discrimination. The economic cost of these practices on the various stakeholders involved can be estimated with additional study.
3. To serve as an effective deterrent, fines levied under preliminary recommendation 8(e) would have to be calibrated in a way that is indexed to the skewed distribution of individuals affected by individual data/privacy breaches. Additional study is required to understand how best to perform this calibration.

***Introduction***

This submission pertains to the Australian Competition and Consumer Commission (ACCC) report 'Digital Platforms Inquiry: Preliminary Report', which was released in December 2018. In the course of this report, the ACCC has correctly identified that digital platforms are clear manifestations of a changed economic structure, which has implications for competition and consumer protection. Some of the preliminary recommendations are not correctly premised through, particularly those related to privacy, which may lead to ineffective policy interventions. This submission attempts to provide some additional information, which it is hoped will provide the ACCC with guidance that will lead to more appropriate and effective policy measures.

This submission is based on research and work undertaken over many years including: research on the economics of personal data while Fellow for Cybersecurity and Internet Governance, School of International and Public Affairs, Columbia University; consulting work on digital security with the Directorate for Science, Technology and Innovation, Organisation for Economic Co-operation and Development (OECD); research on use of torts in digital security incidents for the Center for Democracy and Technology; modelling of cyber risks for insurers for Iconoclast Tech LLC.

## 1. *Privacy in a digital age, pervasive data collection and competition*

Amongst the preliminary recommendations provided in the report, two in particular are related to breaches and invasions of privacy:

*Preliminary recommendation 8 - Use and collection of personal data*
*(f) Introduce direct rights of action for individuals: Give individual consumers a direct right to bring actions for breach of their privacy under the Privacy Act.*

and

*Preliminary Recommendation 10—serious invasions of privacy*

**Submission to ACCC inquiry on digital platforms**
Benjamin C. Dean, *15 February 2019*

*"The ACCC proposes to recommend that the Government adopt the Australian Law Reform Commission's (ALRC) recommendation to introduce a statutory cause of action for serious invasions of privacy to increase the accountability of businesses for their data practices and give consumers greater control over their personal information."*

The issue with these recommendations is that they embody legal notions of privacy that are no longer appropriate given the nature and scale of the activities conducted by digital platforms, such as Google and Facebook. The business models of these digital platform companies require the wholescale collection, storage and analysis of all kinds of user data – including but not limited to personal data – for the purposes of selling targeted advertising among other services. This business model has been referred to as a driving force behind 'surveillance capitalism'[1], which involves transformation of the global economic structure through increasingly pervasive data collection, storage and analysis.

Pursuit of digital platforms along the lines of privacy violations, and the recommendations from the 2014 Australian Law Reform Commission[2], which are premised on what Warren and Brandeis once called the right "to be let alone", "misses the scale of this transformation"[3]. Policy measures premised on this notion of privacy (i.e. the right to be left alone) would not be effective in a world where data is collected, stored and analyzed for every action that one performs using digital platforms. Put simply, "there can be no "alone" when so much of our daily activities generate unintentionally—and uncontrollably—sensitive data."[4] Moreover, when "location equals identity"[5], and digital platforms track the location of their users either via IP address or GPS, sometimes without the knowledge of users, as Google has done[6], privacy becomes an antiquated notion. To require these companies to protect user privacy is, "like asking Henry Ford to make each Model T by hand or asking a giraffe to shorten its neck."[7] It is simply incompatible with the business models of digital platforms. Attempts to regulate the practices of these companies via this means indicates a misunderstanding of the nature of the policy issues at hand.

Acknowledgement of the insufficiency of the notion of 'privacy' in a digital world can be seen in the alternate focus of 'data protection', which is embodied in the European Union's General Data Protection Regulation (GDPR). This approach is not perfect either though, as evidenced by the ability of digital platforms to move user data from one jurisdiction to another so as to avoid having to conform with the GDPR's requirement - and be subject to its penalties. Facebook did exactly this when it moved 1.5 billion user accounts out of the E.U. to California in April 2018 (i.e. one month before the GDPR came into force)[8]. A different policy approach would likely yield more effective outcomes for competitiveness and economic welfare.

---

[1] Zuboff Z. (2019), "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power", PublicAffairs.
[2] Australian Law Reform Commission (2014), "Serious Invasions of Privacy in the Digital Era"
[3] Morozov E. (2019), "Capitalism's new clothes: A review of The Age of Surveillance Capitalism by Shoshana Zuboff", The Baffler, available from:
[4] Burt A. and Geer D. (2019), "Flat light", Aegis Paper Series, Hoover Institution, Stanford University, available from: https://www.hoover.org/research/flat-light
[5] Greenberg A. (2012), "This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information", Dutton.
[6] Gibbs S. (2018), "Google has been tracking Android users even with location services turned off", The Guardian, https://www.theguardian.com/technology/2017/nov/22/google-track-android-users-location-services-turned-off-sim
[7] Zuboff Z. (2019), "The Age of Surveillance Capitalism".
[8] Hern A. (2018), "Facebook moves 1.5bn users out of reach of new European privacy law", The Guardian, https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law

**2. *The consequences of asymmetric data manipulation and aggregation for competition***

The ACCC has successfully identified the information asymmetries that exist between digital platforms and consumers. This is a policy issue given the potential for market failure in the presence of information asymmetries between transacting parties[9]. Some of the consequences of these asymmetries are identified in the December 2018 report e.g. consumers prevented from making informed choices; considerable consumer harm and decrease the likelihood of effective competition[10]. However, a less well-appreciated consequence of these asymmetries is the digital platforms ability to perform anti-competitive practices; the misappropriation of user data and the value they hold; and appropriation of the consumer surplus through price discrimination.

The objective of the Competition and Consumer Act 2010, which the ACCC is tasked with administering, is, "to enhance the welfare of Australians through the promotion of competition and fair trading and provision for consumer protection".

The pervasive collection and control of data performed by digital platform companies results monopolization of knowledge. Once established, if not monitored and understood by the appropriate authorities, this monopoly potentially enables anti-competitive practices, unfair and deceptive practices, price discrimination and consequent appropriation of consumer surplus. Rather than pursuing this objective using outdated notions of privacy, a more effective approach to addressing the issues created by digital platform companies, particularly from the position of the ACCC, would involve pursuing these companies the lines of the Competition and Consumer Protection Act 2010. This is in line with the approach adopted by the ACCC's German counterpart, the Federal Cartel Office, which has publicly stated that, "the combination of data sources substantially contributed to the fact that Facebook was able to build a unique database for each individual user and thus to gain market power[11]", then forbid Facebook from combining users' Facebook information with data about their activities on other sites.

Information asymmetry occurs when one party can cause market failure in a number of ways. The ACCC has correctly identified that digital platforms create monopolies over knowledge[12], which results in loss of user bargaining power. However, these monopolies over knowledge also permit price discrimination, which has consequences for competition and consumer welfare.

Digital platforms collect data from users, sometimes without those consumers' knowledge, and certainly not in a way that allows users to receive a price for the data exchange that is commensurate with the value of that data. Access to these user data, or insights/analysis based on these data, are then on-sold to other third parties such as advertisers, insurers or banks. For the online advertising market, real-time auctions are held to determine prices. The issue is that users, consumers and regulatory authorities do not have much knowledge of how this process of price determination/discrimination actually works in practice. This is because the algorithms used to facilitate the bidding process are not publicly available.

What is known are the economic consequences of these practices. The ability to collect data at almost no cost (i.e. price paid to users), then sell access to these data, or insights/analysis based on these data, in a non-transparent way permits prices to be set in a way that is as close as possible to the maximum willingness to pay of the consumer. This results in appropriation of the consumer

---

[9] Stiglitz, J.E. & Weiss, A. (1992) Asymmetric information in credit markets and its implications for macroeconomics, Oxford Economic Papers, 44, pp. 694-724.
[10] p222
[11] Henry J. (2019), "Germany Restricts Facebook's Data Gathering", New York Times, https://www.nytimes.com/2019/02/07/technology/germany-facebook-data.html
[12] Ledyard J. O. (2008). "market failure," *The New Palgrave Dictionary of Economics*, 2nd Ed.

surplus, which is large considering the data are collected at almost no cost to the digital platform company.

Were the ACCC to wish to pursue digital platforms in accordance with the Competition and Consumer Protection Act 2010, and thereby gain greater insight into the data collection and price determination practices of these companies, two avenues could be pursued. The first relates to the potential for anti-competitive practices through monopolization of knowledge and subsequent information asymmetry. The second would involve considering whether these digital platforms have been practices fair trading, and whether their practices have had detrimental effects on consumers, due to data misappropriation/theft as well as appropriation of the consumer surplus through manipulated pricing.

***Anti-competitive practices***

The 'winner take all' dynamic of digital platform markets carry with them implications for competition. It is imperative for digital platforms to reach a critical mass of users so as to collect as much data, and exclude others from the use of these data, as possible. Doing so, coupled with network effects - which effectively shut-out competitors - allows these platforms to maintain long-term competitive advantage and profitability. This situation has now evolved to the point where the online advertising market is controlled by a duopoly of Google and Facebook (at least 65% global market share in 2017)[13]. Moreover, extensive data collection from across the world wide web allows digital platforms to track competitive threats and neutralize these threats before they are able to gain scale. Evidence of these practices was provided in the British Parliamentary inquiry into Facebook[14]. The ACCC could potentially discover similar documents if it were to bring court against these digital platform companies for potentially anti-competitive practices.

This drive for continuous mass data collection has also led digital platform companies to conduct other underhanded and deceptive practices. The legalese-laden and non-negotiable Terms of Use that consumers are forced to agree to in order to use these platforms is another example. These Terms of Use are also not followed by the platform companies themselves, as demonstrated by the misuse of collected data in the Cambridge Analytica affair[15]. Were data to be treated as a tangible asset, and an exchange to occur on the terms of the Terms of Use contracts, such an exchange could be considered as theft[16]. Considering the detrimental effect of these practices on consumer welfare, and that they may constitute unfair trading, the ACCC might wish to consider pursuit of these companies under the Competition and Consumer Act 2010.

The data-related practices of digital platforms are detrimental to consumers and users in two ways

a) Theft of user data and associated value; and
b) Appropriation of the consumer surplus.

---

[13] Ingram M. (2017), "How Google and Facebook Have Taken Over the Digital Ad Industry", Fortune, http://fortune.com/2017/01/04/google-facebook-ad-industry/

[14] Note by Damian Collins MP, Chair of the DCMS Committee Summary of key issues from the Six4Three files, https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf

[15] For more information see the statements to the U.S. House Judiciary Committee by Senators Grassley and Feinsten, which are available here: https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data

[16] Considering the Oxford Dictionary definition of theft as "the act of stealing", and the definition of stealing being, "Tak[ing] (another person's property) without permission or legal right and without intending to return it.
Theft: https://en.oxforddictionaries.com/definition/theft
Stealing: https://en.oxforddictionaries.com/definition/steal

***Theft of user data and associated value:***
How much has been misappropriated from users of these platforms from potentially deceptive and unfair practices (e.g. non-negotiable Terms of Use, misuse of user data, etc.)? There are a variety of ways that one could estimate the value of these misappropriated data. Stolen information is often for sale on online marketplaces. The sum total of the average person's data (which it must be noted is not the 'typical' person owing to some people's information being worth orders of magnitude more than others, thereby skewing the distribution) is approximately **USD 50 (~AUD 70 as of Feb. 2019)**[17]. This number could be multiplied by the number of platform users to reach a rough total estimate. Another method might divide the total revenue of the platform by the number of users, which would give a per user revenue amount that is a proxy for the value of that person's data and attention. In 2017 this would have been roughly USD 89 billion / 2 billion monthly active users[18] = **~ USD 48 (~ AUD 68 as of Feb. 2019) per Google user** or USD 40 billion / 2 billion monthly active users[19] = **~ USD 20 (~ AUD 28 as of Feb. 2019) per Facebook user**.

***Appropriation of the consumer surplus:***
The metrics that digital platforms release on the effectiveness of their advertising products have been consistently concealed, manipulated and distorted for many years. For an example of the difficulty in finding reliable figures on the performance of digital platforms' advertising, and their poor performance once located, see this article in the footnote[20]. For instances of metric goalpost shifting and mis-stated metrics see these two examples in the footnotes below[21]. This potentially unfair trading, enabled by monopolization of knowledge and the information asymmetry it introduces, leads advertisers (i.e. the customers of digital platforms) to pay as close to their maximum willingness to pay for the advertising space that they purchase on digital platforms, which results in almost total appropriation of the consumer surplus by the producer.

In theoretical terms, the consumer surplus is the difference between the amount of money consumers are willing and able to pay for a good or service (i.e. willingness to pay) and the amount they actually end up paying (i.e. the market price). Attempting to estimate the exact size of the consumer surplus appropriated is difficult but some methods yield estimates that give an idea of the scale of the transfer within an order of magnitude.

For the online advertising market we can ascertain the total amount of money that consumers (e.g. advertisers) pay. These figures can then be compared to the amount that those consumers would be willing to pay (WTP) so as to determine the consumer surplus. A study could be conducted to estimate this WTP, and thereby estimate digital platforms' appropriation of consumer surplus in Australia, as has been done for Uber in the US in 2016. Other markets for user data, or insights/analysis based on these data, could also be usefully explored. Such markets could include the insurance or banking markets for data collected via digital platforms.

---

[17] Jacoby D. (2018), "Hey there! How much are you worth?", Kaspersky Labs, https://securelist.com/hey-there-how-much-are-you-worth/88691/
[18] Popper B. (2017), "Google announces over 2 billion monthly active devices on Android", The Verge, https://www.theverge.com/2017/5/17/15654454/android-reaches-2-billion-monthly-active-users
[19] Costine J. (2016), "Facebook now has 2 billion monthly users… and responsibility", TechCrunch, https://techcrunch.com/2017/06/27/facebook-2-billion-users/
[20] Dean B. (2014), "Hard evidence: how will social networks boost earnings when users ignore their product?", The Conversation, https://theconversation.com/hard-evidence-how-will-social-networks-boost-earnings-when-users-ignore-their-product-34110
[21] Wall Street Journal: "Facebook Overestimated Key Video Metric for Two Years", https://www.wsj.com/articles/facebook-overestimated-key-video-metric-for-two-years-1474586951
Wall Street Journal: "Google Issuing Refunds to Advertisers Over Fake Traffic, Plans New Safeguard", https://www.wsj.com/articles/google-issuing-refunds-to-advertisers-over-fake-traffic-plans-new-safeguard-1503675395

**Annual revenues of Google and Facebook, 2014-2018 in USD billion**

| | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|
| Google | 59.73 | 65.83 | 73.59 | 89.73 | 111.02 |
| Facebook | 12.47 | 17.93 | 27.64 | 40.65 | 55.84 |

### 3. Calibrating fines to reflect the damage caused by data/privacy breaches

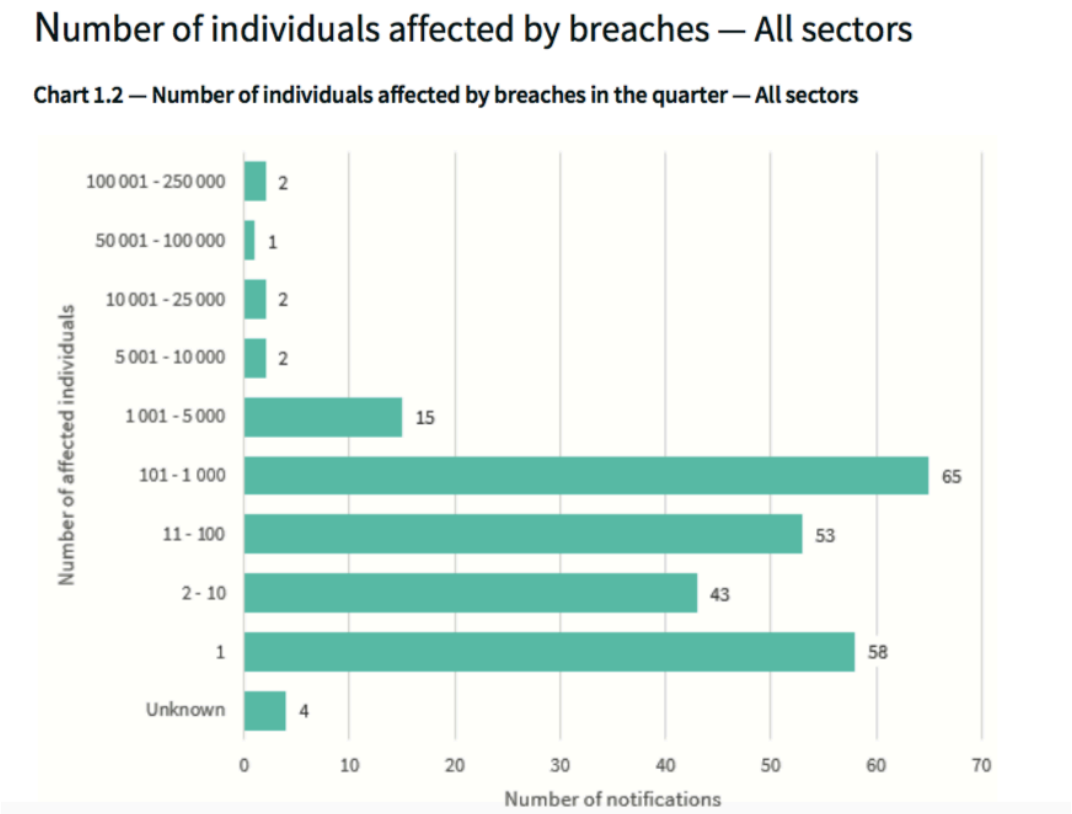
*Under Preliminary recommendation 8 (e)* it is proposed to increase the penalties for breaches of the Privacy Act to at least mirror the increased penalties for breaches of the Australian Consumer Law (ACL). This recommendation is suitable for two reasons.

First, it places a strong economic incentive on these companies to protect and not misuse user data. The lack of such an incentive has introduced moral hazard and is a major reason why data breaches continue to occur[22]. These are companies that generate tens of billions of dollars in revenues annually. Fines against Facebook such as those handed down by the European Commission (EUR 110 million)[23], the French CNIL (EUR 150,000)[24] or the UK Information Commissioner's Office (GBP 500,000)[25] are small enough to be considered as a cost of doing business.

Second, this preliminary recommendation responds to the need to be able to levy financial penalties in a way that takes into account the highly skewed distribution of the severity of data breaches affecting digital platforms. The majority of individual data breach incidents in a given period (i.e. one year) affect a relatively small number of people. A small minority of breaches affect a large number of people[26]. This dynamic has consistently emerged during more than ten years of reported data breaches in the United States[27] and can already be seen after one year of mandatory data breach reporting in Australia [see below]. For instance, during July to September 2018 most data breaches involved the personal information of 100 individuals or fewer (63 per cent of data breaches).

---

[22] Dean B. (2015), "Why companies have little incentive to invest in cybersecurity", The Conversation, https://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570
[23] European Commission (2017), "Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover", http://europa.eu/rapid/press-release_IP-17-1369_en.htm
[24] Commission Nationale de l'Informatique et des Libertés (2017), « Délibération n°SAN-2017-006 du 27 avril 2017, Délibération de la formation restreinte SAN-2017-006 du 27 Avril 2017 prononçant une sanction pécuniaire à l'encontre des sociétés FACEBOOK INC. et FACEBOOK IRELAND », https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000034728338&fastReqId=390211096&fastPos=2
[25] UK ICO (2018), "ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information", https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/
[26] Makridis C. & Dean B. (2018), "Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities", *Journal of Economic and Social Measurement*, Vol. 43(1-2), 10.3233/JEM-180450
[27] Dean B. (2017), "Data breaches: Their cost, who bears it and the future", https://bennydean.com/post/168196399578/data-breaches-their-cost-who-bears-it-and-the




*Source*: Australian Information Commissioner, Notifiable Data Breaches Quarterly Statistics Report, October 2018

As the ACCC is aware, the *Treasury Laws Amendment (2018 Measures No. 3) Bill 2018* (**Bill**) to substantially increased the maximum financial penalties for contraventions of the Australian Consumer Law (ACL). Under the new law, the maximum penalties for corporations increased from AUD1.1 million to the greater of one of the following:

- AUD10 million
- 3 x the value of the benefit
  or
- if the value of the benefit cannot be determined – 10% of the annual turnover.

For serious data breaches, such as those affecting more than 1 million individuals, penalties can now be levied in a way that can be ratcheted up or down given the sensitivity of the data breached and the number of individuals affected. For digital platforms, which have annual revenues at the scale of USD 111 billion (Google) or USD 55.84 billion (Facebook), the prospect of a fine levied as a proportion of annual revenue is a strong incentive. Considering the number of people affected by past large-scale breaches of user data/privacy involving these companies (e.g. 50 million people in one recent Facebook incident[28]; 500,000 people in one recent Google incident[29]), fines could be levied at various different levels.

[28] Kharpal A. (2018), "Facebook could face up to $1.6 billion in fines over data breach as regulators eye formal probe", CNBC, https://www.cnbc.com/2018/10/02/facebook-data-breach-social-network-could-face-eu-fine.html

[29] MacMillan D. & McMillan R. (2018), "Google exposed user data, feared repercussions of disclosing to public", https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194

How these fines should be levied in the future, in the presence of highly skewed incident and severity distributions, so as to achieve the ACCC's objective of, "reducing information asymmetries between consumers and digital platforms and enabling consumers to make informed choices regarding how their data is collected, used and disclosed"[30], could be explored through additional investigation.

[30] p227