University of New South Wales Law Research Series

CONCEALED DATA PRACTICES AND COMPETITION LAW: WHY PRIVACY MATTERS

KATHARINE KEMP

[2019] *UNSWLRS* 53

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

CONCEALED DATA PRACTICES AND COMPETITION LAW: WHY PRIVACY MATTERS

Working Paper

Katharine Kemp*

1. Introduction

The relationship between market power, the accumulation of consumer data and individual privacy in digital markets increasingly commands the attention of regulators, and sparks debate about what type of regulation should apply. The United States Federal Trade Commission recently settled on a fine of USD 5 billion for Facebook's conduct in repeatedly misrepresenting the extent to which its users could control access to their personal data.[1] By contrast, the Bundeskartellamt controversially found that Facebook's practice of collecting and combining its users' information across third-party websites amounted to an abuse of its dominant position, even if consumers were aware of the practice.[2] Meanwhile, a series of reports have investigated how consumer protection, privacy regulation and competition policy should apply to Google, Facebook and other digital platforms,[3] and particularly whether competition

* Senior Lecturer, Faculty of Law, UNSW Sydney. I am grateful to Graham Greenleaf, David Howarth and Megan Richardson for helpful comments on an earlier draft, and to Roseanna Bricknell for research assistance; with the usual disclaimers.

[1] United States Federal Trade Commission, 'FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making' (24 July 2019) < https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history>.

[2] Bundeskartellamt, Germany, 'Bundeskartellamt prohibits Facebook from combining user data from different sources: Background information on the Bundeskartellamt's Facebook proceeding' (7 February 2019); *Facebook Inc i.a. – The Use of Abusive Business Terms pursuant to Section 19(1) GWB* (B6-22/16, Bundeskartellamt, Administrative Proceedings, 6 February 2016).

[3] See, eg, Australian Competition & Consumer Commission, 'Digital Platforms Inquiry: Final Report' (June 2019) ('ACCC Digital Platforms Report'); European Data Protection Supervisor, 'EDPS Opinion on Online Manipulation and Personal Data' (Opinion 3/2018, 19 March 2018); Government of Canada, 'Strengthening Privacy for the Digital

regulators should also take account of privacy concerns under competition law.[4] This paper argues that the degradation of consumer data privacy in the digital environment causes objective detriment to consumers and undermines the competitive process and should therefore be of critical concern under competition law.

There are larger issues at stake in the broader debate about increasing digital surveillance and corporate data practices.[5] These issues ultimately go to the very nature of the society we live in and our fundamental human rights in that society. This paper is not an attempt to address these larger issues, nor to diminish them. Rather, it argues for an acknowledgement of the importance of privacy harms and concerns under one type of regulation, which plays a key role in decisions about the private acquisition, preservation and exploitation of market power and the manner in which our markets function.

The collection and use of consumers' personal data has become a vital feature of digital markets and created significant efficiencies and benefits for consumers.[6] It is well accepted that, when competition authorities assess the health of competition in these markets, they should consider the benefits consumers receive from digital services – online search, social

---

Age' (Discussion Paper, May 2019); House of Lords Select Committee on Communications, 'Regulating in a Digital World' (2nd Report of Session 2017-19, March 2019). See also Mission to French Secretary of State for Digital Affairs, 'Creating a French Framework to Make Social Media Platforms More Accountable: Acting in France with a European Vision' (Mission Report, Version 1.1, May 2019).

[4] See, eg, Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the Digital Era' (European Commission, 2019); Digital Competition Expert Panel, United Kingdom, 'Unlocking Digital Competition' (Report, March 2019) ('Furman Report'). See further Eugene Kimmelman, Harold Feld and Agustìn Rossi, 'The Limits of Antitrust in Privacy Protection' (2018) 8 *International Data Privacy Law* 270.

[5] See, eg, Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile, 2019); Brett Frischmann and Evan Selinger, *Re-Engineering Humanity* (Cambridge University Press, 2018); Karen Yeung, '"Hypernudge": Big Data as a Mode of Regulation by Design' (2017) 20 *Information, Communication & Society* 118; Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy and Manipulation' (2019) 8 *Internet Policy Review* (forthcoming); Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press, 2016).

[6] See Phuong Nguyen and Lauren Solomon, 'Consumer Data and the Digital Economy: Emerging Issues in Data Collection, Use and Sharing' (Report, Consumer Policy Research Centre, 2018) 20-21 ('CPRC Emerging Issues Report'); George J Stigler Center for the Study of the Economy and the State and The University of Chicago Booth School of Business, 'Committee for the Study of Digital Platforms: Market Structure and Antitrust Subcommittee: Draft Report' (15 May 2019) 5-6 ('Stigler Center Digital Platforms Report').

networks, fast and convenient connections with relevant products, news and entertainment, and real-time information on healthier lifestyle choices.[7] However, there is uncertainty and disagreement about the extent to which competition authorities should take into account, and respond to, the degradation of consumer data privacy which results from data practices in these markets.

Some antitrust commentators argue that privacy terms are a matter of subjective preference which should be left to individual bargains between each consumer and the suppliers they deal with,[8] and that only an apparently "small group of privacy-sensitive consumers" who have not protected themselves with available privacy tools, are harmed by reductions in privacy quality.[9] On this version, consumers accept the privacy terms on which digital services are offered if they continue to use that service: this is a personal choice.[10] These commentators also tend to argue that privacy protection does not fall within the economic objectives of antitrust and particularly antitrust's narrowly defined concept of consumer welfare.[11] Privacy is seen as a non-economic objective which should be left to consumer protection and privacy regulation, to the extent that

[7] See, eg, 'Common Understanding of G7 Competition Authorities on "Competition and the Digital Economy"' (July 2019) 3; D Daniel Sokol and Roisin Comerford, 'Antitrust and Regulating Big Data' (2016) 23 *George Mason Law Review* 1130, 1133-1135; Geoffrey A Manne and Joshua D Wright, 'Google and the Limits of Antitrust: The Case Against the Case Against Google' (2011) 34 *Harvard Journal of Law & Public Policy* 171, 203-206. See also David S Evans, 'Attention Platforms, the Value of Content and Public Policy' (January 2019) 3, 21-24; Alessandro Acquisti, 'The Economics of Personal Data and Privacy: 30 Years After the OECD Privacy Guidelines' (Organisation for Economic Co-operation and Development (OECD), 2010) 8-11.

[8] Torsten Körber, 'Is Knowledge (Market) Power? On the Relationship between Data Protection, "Data Power" and Competition Law' (2016) <https://ssrn.com/abstract=3112232> 9-10, 18; Geoffrey A Manne and R Ben Sperry, 'The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework' (CPI Antitrust Chronicle, May 2015) 5-6. See further Sokol and Comerford, above n 7, 1144-1145; Maureen K Ohlhausen and Alexander P Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015) 80 *Antitrust Law Journal* 121.

[9] Manne and Sperry, above n 8, 5-6.

[10] Manne and Sperry, above n 8, 3-4. See further Maria Estrella Gutierrez David, 'Discussing Transparency of Privacy Policies in the Age of Big Data: Towards the 'Social Norm' as a New Rule of Law' (2017) *Etica de Datos, Sociedad Y Ciudadania* 165, 182. See also Körber, above n 8, 10, 16-17.

[11] Measured in terms of price and output levels of the relevant product. See Sokol and Comerford, above n 7, 1145, 1156-1158; Maureen K Ohlhausen and Alexander P Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015) 80 *Antitrust Law Journal* 121.

intervention is necessary.[12]

Other commentators also regard data privacy as a matter for individual bargains but acknowledge that consumers are likely "underpaid" in these transactions due to their lack of bargaining power and information about the value of their data.[13] Seeing data as "payment" by consumers for digital services, some have proposed measures that would allow consumers to have more control over which suppliers collect their data and/or to be compensated for the "true" value of their personal information to those suppliers.[14]

This paper proposes an alternative approach: the collection and use of personal data is not so much a price paid, but an objective cost imposed on consumers in the process of digital transactions. The extent of this cost is a reflection of the quality of the service in question.[15] We should be more concerned about the consequences of these revelations for consumers, than what the supplier gains from each incremental revelation of consumer data.[16] A critical problem

[12] See Manne and Sperry, above n 8; Sokol and Comerford, above n 7, 1156-1161; Maureen K Ohlhausen and Alexander P Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015) 80 *Antitrust Law Journal* 121; European Commission, 'Facebook / Whatsapp' (COMP/M 7217, 3 October 2014) para 164.

[13] See Gianclaudio Malgieri and Bart Custers, 'Pricing Privacy: The Right to Know the Value of Your Personal Data' (2018) 34 *Computer Law & Security Review* 289; Viktoria H S E Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in an Era of Big Data' (Working Paper, June 2019) 9-11. See also Jan Whittington and Chris Jay Hoofnagle, 'Unpacking Privacy's Price' (2012) 90 *North Carolina Law Review* 1327, 1346-1351; Carmen Langhanke and Martin Schmidt-Kessel, 'Consumer Data as Consideration' (2015) 6 *EuCML* 218, 219.

[14] See OECD, 'Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value' (White Paper, 2013) 6, 18-34 (on "data lockers"); Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54 *Journal of Economic Literature* 442, 447-448 (on attempts to value, and permit consumers to trade in, personal information). Cf Chris Jay Hoofnagle and Jan Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price' (2014) 61 *UCLA Law Review* 606, 637-640, 646-648 (on the value of personal information to *consumers*).

[15] Importantly, the degradation of privacy is also detrimental to broader social welfare: diminished privacy in society in general will benefit some while harming others: Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880, 1881. Privacy is also essential to the intellectual, political and cultural development of society as a whole: Julie E Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 *Stanford Law Review* 1373, 1428. Cf Acquisti, 'The Economics of Personal Data and Privacy', above n 7, 4 (explaining arguments as to why privacy is a source of economic inefficiencies).

[16] See Michal S Gal and Daniel L Rubinfield, 'The Hidden Costs of Free Goods: Implications for Antitrust Enforcement' (2014) 521 (arguing that regulators should not be content with "the simplistic conclusion that the free good creates positive welfare effects" but that "the analysis should be expanded to include long-term effects in the same market as well as in interdependent and affected markets").

for consumers and for the competitive process is that, currently, these costs are hidden and consumers have almost no power to address them. Aside from the direct harm to consumer welfare, these hidden data practices critically impede privacy-enhancing competition that might otherwise improve consumer welfare.[17]

In this paper, I define a set of "concealed data practices" which have been observed in numerous digital markets, and which create objective costs and detriments for consumers and undermine the competitive process.[18] I argue that competition authorities should take account of these costs and detriments in assessing the state of competition and determining whether there has been a substantial lessening of competition in the case of any alleged anticompetitive conduct.

It is important to note at this point that some commentators object to the very idea that it should be possible for individuals to "bargain away" their privacy rights.[19] On this view, given that privacy is a fundamental right which "belongs to the core of human dignity",[20] it is vital to the health of our society as a whole that individuals should not be able to waive or trade at least certain parts of this right.[21] In the same way that we do not permit individuals to sell their own organs, we should not, for example, permit individuals to negotiate a bigger discount in exchange for giving up their right to access their personal information.[22] This is a vital debate.

---

[17] As explained in Part 4.3 below. See OECD, 'The OECD Privacy Framework' (2013) 32 (on the importance of privacy-enhancing technologies (PETs) in complementing laws protecting privacy). See also Acquisti, 'The Economics of Personal Data and Privacy', above n 7, 19-20.

[18] See Part 3 below.

[19] See Anita Allen, *Unpopular Privacy: What Must We Hide?* (Oxford University Press, 2011) Chap 7. See further Roger Brownsword, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality' in S Gutwirth et al (eds), *Reinventing Data Protection?* (Springer, 2009) 102.

[20] Volker Boehme-Neßler, 'Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection' (2016) 6 *International Data Privacy Law* 222, 223.

[21] Anita Allen, *Unpopular Privacy: What Must We Hide?* (Oxford University Press, 2011) Chap 7 ("Privacy should be thought of as a partly inalienable foundational good."). See also Adam D Moore, 'Privacy, Interests & Inalienable Rights' (Research Paper, 22 January 2018) 1-3 <https://ssrn.com/abstract=3107324>.

[22] Personal correspondence with Graham Greenleaf. See Moore, above n 21, 1-2 (drawing comparisons with slavery).

However, these "bargains" presently take place in numerous jurisdictions, including those, like Australia, which only debatably recognise privacy as a human right.[23] We should recognise that the supposed efficiency of these practices fails to weigh up even under the free market lens.

This paper proceeds as follows. Part 2 provides an explanation of the "notice and choice" approach to data privacy regulation and the challenges to that approach in the digital era. Part 3 defines, and provides illustrations of, "concealed data practices" which have been used in digital markets in particular to secure and maintain consumers' "consent" to the handling of their personal information. It proceeds to describe the objective costs and detriments suffered by consumers as a result of concealed data practices and degraded data privacy.

Part 4 considers the two main responses by antitrust scholars to the question whether privacy is a competition law issue and proposes a third response, namely that the degradation of data privacy causes objective harm to consumers and undermines the competitive process and should therefore be of concern to competition regulators. It proceeds to explain the manner in which concealed data practices undermine the competitive process by chilling competition on privacy quality and increasing inequalities in bargaining power and information asymmetries between suppliers and consumers. Part 5 sets out four ways in which these factors should be taken into account by competition authorities.

2. Data privacy regulation and big data incentives

On the traditional view, "[p]rivacy, in its simplest sense, allows each human being to be left alone in a core which is inviolable."[24] While scholars have provided numerous definitions of privacy, and accounts of its benefits,[25] in essence, privacy establishes the boundaries between

[23] See Megan Richardson, *The Right to Privacy: Origins and Influence of a Nineteenth-Century Idea* (Cambridge University Press, 2017).

[24] *Justice K S Puttaswamy (Ret'd) v Union of India* (Supreme Court of India, 24 August 2017) 4 [2] (Plurality Opinion delivered by Chandrachud J).

[25] See Daniel J Solove, 'Conceptualising Privacy' (2002) 90 *California Law Review* 1087.

ourselves and others; boundaries which are vital to the development and dignity of the individual and the cultural, political and economic development of society as a whole.[26]

"Data privacy laws systematically regulate the use of information about people."[27] Data privacy regulation, or information privacy as it is sometimes termed, therefore concerns control over one's personal information. Information privacy may be distinguished from other aspects of privacy, including bodily privacy (freedom from interference with our physical bodies or decisions concerning our bodies) and territorial privacy (freedom to be let alone in our own homes and private places).

In the area of information privacy, one of the major models of regulation, which prevails in the United States and largely in Australia, is the "notice and choice" model.[28] Essentially, suppliers provide notice of their proposed privacy terms and consumers choose whether to accept those terms and thereby permit certain collection and use of their personal information. Regulation does not impose substantive restrictions on the kinds of personal information that may be collected or the uses to which that information can be put, but leaves these to be agreed between the entity collecting the information and the individual in question.[29]

---

[26] "Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be suffocating …": Daniel J Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745, 762. See, generally, Julie Cohen, 'What is Privacy For' (2013) 126 *Harvard Law Review* 1904 (on the manner in which privacy allows individuals to develop with independence and space for critical thinking and the vital role privacy plays in innovation).

[27] Graham Greenleaf, *Asian Data Privacy Law* (Oxford University Press, 2014) 5. In Europe, the term "data protection law" tends to be used, while in North America, Australia and New Zealand, the term "privacy law" is used, and there is growing use of "data privacy law": Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) xxv.

[28] Thomas B Norton, "The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model" (2016) 27 *Fordham Intellectual Property, Media and Entertainment Law Journal* 181, 195-198; Solove, 'Privacy Self-Management', above n 15, 1882-1883. See also Policy and Research Group, Office of the Privacy Commissioner of Canada, 'Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent under the *Personal Information Protection and Electronic Documents Act*' (Discussion Paper, 2016) 2 ('Privacy Commissioner of Canada Consent and Privacy Report').

[29] Solove, 'Privacy Self-Management', above n 15, 1882.

The "notice and choice" model therefore relies heavily on the adoption of privacy policies by suppliers and the idea that individuals can make effective bargains about the privacy of their information in response to those policies. In Australia, for example, entities regulated by the *Privacy Act 1988* (Cth) are required to publish a privacy policy which sets out, among other things, the kind of personal information the entity collects, how and for what purpose the information is used, how the information can be accessed, and whether the entity is likely to disclose the information to overseas recipients.[30] These obligations do not apply in respect of all information that concerns an individual, but only to "personal information", that is, information or an opinion about an identified individual, or an individual who is reasonably identifiable.[31]

This approach to privacy regulation has been significantly influenced by views on privacy which prevail in the United States, and particularly the neoliberal approach of treating privacy as a matter of individual economic choice.[32] It is regarded as an acknowledgement of the autonomy of the individual and the wide variety of privacy preferences between individuals.[33] The state should not impose its views regarding privacy on its citizens, but leave each individual to determine their own information privacy destiny. The approach has therefore been described as "privacy self-management".[34]

---

[30] *Privacy Act 1988* (Cth), s 15, sched 1 (Australian Privacy Principle 1). These obligations apply to certain government agencies and private organisations, but there are numerous exempt entities, including small businesses, which account for the majority of businesses in Australia.

[31] *Privacy Act 1988* (Cth), s 6, sched 1. See *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4; ACCC Digital Platforms Report, above n 3, 458-461, on the ACCC's recommendation to amend the definition of "personal information" under the *Privacy Act 1988* (Cth) to clarify its inclusion of certain "technical data" that may be used to identify an individual.

[32] See Gordon Hull, 'Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data' (2015) 17 *Ethics of Information Technology* 89, 90-91 ("individual risk management coupled with individual responsibility for poorly-managed risks"); Omri Ben-Shahar and Carl E Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press) 5.

[33] See Solove, 'Privacy Self-Management', above n 15, 1889, 1895-1896; Privacy Commissioner of Canada Consent and Privacy Report, above n 28, 2.

[34] Solove, 'Privacy Self-Management', above n 15, 1880.

For a long time, however, some scholars have expressed scepticism about the extent to which individuals are truly able to determine their own information privacy destiny.[35] That scepticism has justifiably increased in recent decades as giant leaps in information technology have reduced the individual's ability to control or understand the uses of their personal data.[36] The "notice and choice" model, it should be remembered, came to prominence in the 1970s, in an era of filing cabinets, paper records and fax machines.[37] In that context, it was conceivable that the individual consumer would be aware of what personal information was being collected, when and by whom, and the opportunities for disclosure and storage of personal information were physically and technologically limited.

Today's consumer instead faces pervasive and invisible collection of their personal information by corporations and governments alike,[38] and mounting proposals to increase disclosure and surveillance.[39] Individuals are constantly tracked as they use credit cards and devices to access the internet; by CCTV and biometric identification systems; by their mobile phones, wearable devices, in-home digital assistants and everyday appliances connected via the internet.[40]

Where the successful combination of human, capital and physical resources drove outcomes in

[35] See, eg, Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press, 2010); Julie Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press, 2012); Hull, above n 32, 91; Fred H Cate, 'The Failure of Fair Information Practice Principles' in Jane K Winn (ed), *Consumer Protection in the Age of 'Information Economy'* (2006) 341.

[36] See Privacy Commissioner of Canada Consent and Privacy Report, above n 28, 1, 8; The White House, 'Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy' (Report, February 2012).

[37] Solove, 'Privacy Self-Management', above n 15, 1882 (describing the Fair Information Practice Principles (FIPPs) which appeared in the 1973 US Department of Health, Education, and Welfare Report "to address concerns about the increasing digitization of data"). See also Privacy Commissioner of Canada Consent and Privacy Report, above n 28, 6.

[38] See Bruce Schneier, *Data and Goliath* (Norton, 2015) 92-103.

[39] See, eg, Productivity Commission, Australian Government, 'Data Availability and Use' (Inquiry Report No 82, 31 March 2017); Department of Prime Minister and Cabinet, Commonwealth of Australia, 'New Australian Government Data Sharing and Release Legislation: Issues Paper for Consultation' (Issues Paper, 4 July 2018).

[40] Maurice E Stucke and Ariel Ezrachi, 'Alexa et al, What Are You Doing with My Data?' (2018) 5 *Critical Analysis of Law* 148, 149-150.

traditional markets, technology and the use of data determine commercial success in digital markets. Suppliers have been enjoined to "measure everything" in the interests of customer profiling, targeted marketing, customisation, price discrimination, risk analysis and to support other potential applications of artificial intelligence in their businesses. For these purposes, on one view, more data is better.[41] Machine learning is data hungry.[42] Competitors are benefiting from millions of "insights" about consumers in the market and possibilities of extending into other markets. Prominent critiques explain the dynamics of a new "surveillance economy" or "surveillance capitalism", which pervasively and increasingly monitors and extracts human experience for profit.[43]

In this context, suppliers have an incentive to accumulate a wide range of increasingly detailed personal information about an enormous number of consumers,[44] and to persuade consumers to permit this to occur.[45] This incentive often leads suppliers to use hidden tracking technologies,[46] and conceal their data practices from the consumers they are investigating, lest consumers experience concern about these practices and object.[47] Suppliers realise that wearing a fitness tracker might not be nearly so appealing if the wearer knew their biometric

[41] See also Acquisti, 'The Economics of Personal Data and Privacy', above n 7, 8.

[42] See Joseph A Cannataci, 'Report of the Special Rapporteur on the Right to Privacy to the General Assembly of the United Nations' (Advanced Unedited Report, A/73/45712, 17 October 2018) [91]-[97].

[43] See Zuboff, above n 5. See also Susser, Roessler and Nissenbaum, above n 5.

[44] Stigler Center Digital Platforms Report, above n 4, 23-24, 27-28 (on increasing returns to scale of data collection). Cf Acquisti, 'The Economics of Personal Data and Privacy', above n 7, 12-14 (on the economic costs and detriments to firms from collecting large quantities of consumers' personal information).

[45] See Whittington and Hoofnagle, 'Unpacking Privacy's Price', above n 13, 1341-1342 (on the incentives for opportunistic behaviour on the part of "information-intensive companies"); Maurice E Stucke and Allen P Grunes, *Big Data and Competition Policy* (2016) 54-56.

[46] Eg, Google trackers, Facebook pixels, web beacons and identification over multiple devices: Brigid Richmond, 'A Day in the Life of Data: Removing the Opacity Surrounding the Data Collection, Sharing and Use Environment in Australia' (Report, Consumer Policy Research Centre, 2019) 6 ('CPRC Day in the Life of Data Report'); 'CPRC Emerging Issues Report', above n 6, 11-12; ACCC Digital Platforms Report, above n 3, 388-389. On the internet of things (IoT), see Privacy Commissioner of Canada Consent and Privacy Report, above n 28, 8.

[47] See Whittington and Hoofnagle, 'Unpacking Privacy's Price', above n 13, 1341-1342, 1368. See also Maria Lindh and Jan Nolin, 'Information We Collect: Surveillance and Privacy in the Implementation of Google Apps for Education' (2016) *European Education Research Journal* 1, 5-11.

information could be used to raise their future health insurance premiums, or exclude them from insurance. We might think twice about searching online for a psychologist if we realised potential mental illness could be added to a permanent profile attached to our identity.

3. Concealed data practices and consequent detriment to consumers

"Concealed data practices" occur when suppliers' terms provide weak privacy protections for consumers while the extent of those terms, the resultant data practices and the consequences of these data practices are concealed from consumers. These obscured terms frequently permit the collection, retention, use and/or disclosure of personal information, beyond that which is necessary for the provision of the service in question and beyond the reasonable expectations of the consumer.[48] Practices of this kind have been identified with concern in digital markets by a number of consumer protection and privacy regulators around the world,[49] and increasingly by competition regulators investigating the nature of competition in digital markets.[50]

Consumers face obstacles at the outset in attempting to comprehend privacy policy terms and manage their own privacy due to their lack of bargaining power and understanding of the data environment.[51] As in many consumer situations, consumers in this sphere suffer from a

[48] In the context of the many "free" online services provided to consumers, some argue that broad data handling practices may be a necessary element of this type of business model: see Sokol and Comerford, above n 7, 1133-34. See also Körber, above n 8, 17-18. That is, the supplier of these services needs to "leverage" consumer data to sell advertising services, which in turn fund the zero-price service for consumers. However, even in these cases, privacy terms do not seem to be set at a particular level necessary to secure this funding from advertising. Instead they frequently appear to provide suppliers with a broad and open-ended licence to extract and exploit consumer data at will: see Hoofnagle and Whittington, 'Free: Accounting for the Costs', above n 14, 625.

[49] See Privacy Commissioner of Canada Consent and Privacy Report, above n 28; Patricia Kosseim, Office of Privacy Commissioner of Canada, 'Consent as a Universal Principle of Global Data Protection' (Remarks at 7th European Data Protection Day, Berlin, Germany, 15 May 2017); Federal Trade Commission, United States, 'Data Brokers: A Call for Transparency and Accountability' (Report, May 2014). See also United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' (Report, 30 June 2014).

[50] See, eg, ACCC Digital Platforms Report, above n 3, chap 7; Crémer, De Montjoye and Schweitzer, above n 4; Autorité de la Concurrence and Bundeskartellamt, 'Competition Law and Data' (Report, 10 May 2016) 25-28.

[51] Hoofnagle and Whittington, 'Free: Accounting for the Costs', above n 14, 640-641 ("Despite lengthy and growing terms of service and privacy, consumers enter into trade with online firms with practically no information meaningful enough to provide the consumer with either ex ante or ex post bargaining power. In contrast, the firm is aware of its cost structure, technically savvy, often motivated by the high-powered incentives of stock values,

collective action problem. Left to make incremental bargains with suppliers, individual consumers have no power to bargain for better privacy terms: standard terms are put forward by suppliers on a "take it or leave it" basis.[52] In many cases, consumers have no real choice but to use the relevant service in the first place, or to continue to use the service after data practices are revealed, or unilaterally amended by the supplier.[53]

Suppliers frequently use privacy policies to give themselves the right to amend privacy terms in future without the consumer's consent,[54] and impose an obligation on consumers to check periodically for such changes on the supplier's website. Given the number of suppliers with privacy policies that apply to a consumer, it is clearly an impossibility for any individual consumer to inform themselves of the new terms in this way.[55] This unilateral right to change the privacy terms might also be exercised by a subsequent purchaser of the relevant business or database, with quite different business interests or privacy reputation to the original supplier.

Many consumers also suffer from very poor understanding of data practices.[56] Recent research by the Australian Competition and Consumer Commission (ACCC) shows 36 percent of

---

and adept at structuring the deal so that more financially valuable assets are procured from consumers than consumers would prefer.").

[52] See Margaret Jane Radin, 'Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law' (Princeton University Press, 2014) 13-16; Hull, above n 32, 95 (the collective action problem may in fact be exacerbated in the case of privacy as stigma attaches to being the only person not to share information, eg, in insurance situations where others consent to tracking of their driving or health data).

[53] See ACCC Digital Platforms Report, above n 3, 455; Hull, above n 32, 94; Maurice E Stucke and Ariel Ezrachi, 'How Digital Assistants Can Harm Our Economy, Privacy, and Democracy' 32 *Berkeley Technology Law Journal* 1239, 1286. Cf Productivity Commission, Australian Government, 'Data Availability and Use' (Inquiry Report No 82, 31 March 2017) 80 (arguing that in the case of some services "such as social media, consumers can choose whether or not to use the class of product or service at all, without adversely affecting their quality of life").

[54] Whittington and Hoofnagle, 'Unpacking Privacy's Price', above n 13, 1363-1365.

[55] See ACCC Digital Platforms Report, above n 3, 417 (on unilateral changes to Google's policy on combining user data with user data collected via DoubleClick).

[56] Solove, 'Privacy Self-Management', above n 15, 1882-1883 ("people operate under woefully incorrect assumptions about how their privacy is protected"); Privacy Commissioner of Canada Consent and Privacy Report, above n 28, 9; Whittington and Hoofnagle, 'Unpacking Privacy's Price', above n 13, 1355-1357.

Australian consumers believe the existence of a privacy policy means suppliers will not share their personal information with anyone else.[57] Many consumers believe the law prevents companies from "misusing" their personal data.[58] Researchers have demonstrated consumers' substantial misunderstanding of privacy options and whether they have in fact exercised these options.[59]

However, even well-informed and diligent consumers have severely limited power to exercise control over their personal information.[60] A key reason that suppliers are able to impose their own terms on consumers is that the extent of these terms and related complex data practices are frequently hidden from consumers. Privacy policies have become a tool used to manipulate rather than inform.

A number of regulators and researchers have commented on the methods by which privacy policies hide concerning practices from consumers and diminish their importance.[61] These policies often headline with comforting reassurances ("We care about your privacy"; "We never sell your personal information") and list obvious, uncontroversial data practices first ("We use

[57] ACCC, 'Digital Platforms Inquiry: Preliminary Report' (December 2018) 174. See also 'CPRC Emerging Issues Report', above n 6, 29, which revealed almost 1 in 5 Australian consumers held this belief, and a further 22% of Australian consumers "did not know enough to answer this question": 'CPRC Emerging Issues Report', above n 6, 29. See also Chris Jay Hoofnagle and Jennifer King, Research Report 2 (2008), http://ssrn.com/abstract=1262130 (majority of Californian adults believed existence of a privacy policy means there are specific limitations on what a company may collect or disclose); Joseph Turow, Lauren Feldman and Kimberley Meltzer, 'Open to Exploitation: American Shoppers Online and Offline' (University of Pennsylvania, Annenberg Public Policy Center, 2005) (75% believe privacy policy means the site will not share information with other websites and companies).

[58] 'CPRC Emerging Issues Report', above n 6, 59.

[59] See also Leslie K John, 'Uninformed Consent' (2018) *The Big Idea: Harvard Business Review*.

[60] See, eg, 'CPRC Emerging Issues Report', above n 6; Jessica Rich, 'BCP's Office of Technology Research and Investigation: The Next Generation in Consumer Protection' (Federal Trade Commission, 23 March 2015); Hull, above n 32, 91.

[61] See, eg, ACCC Digital Platforms Report, above n 3, 399-434; Stigler Center Digital Platforms Report, above n 6, 31; Norwegian Consumer Council, 'Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy' (Report, June 2018); Office of Privacy Commissioner of Canada, 'Joint Investigation of Facebook Inc by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia' (Report, 25 April 2019); Lindh and Nolin, above n 47, 6-11.

your personal information to provide you with the service").[62]

Terms which would be more concerning to consumers appear much later in these lengthy documents,[63] expressed in broad, vague or incomplete language ("We may collect your personal information for research, marketing, for efficiency purposes …" or "We may also share your personal information with … someone with whom we share some common commercial interest").[64] These terms do not reveal the actual practices of the supplier, such as how many entities will have access to the information, where those entities are located and how they are regulated, or unexpected uses of the information.[65]

They tend to be phrased in permissive language, diminishing the reality of the practices ("We may disclose …"), give examples of beneficial uses which distract attention from more concerning uses,[66] and create a broad licence for suppliers to use personal data for numerous purposes without attracting potential liability.[67] Research amply demonstrates that consumers have enormous difficulty understanding the import of these terms,[68] and the choice of wording makes it hard to believe this was accidental.[69]

---

[62] Lindh and Nolin, above n 47, 7, term this "hands-off rhetoric".

[63] A commonly cited study found that it would take the average person 244 hours (six working weeks) per year to read all the privacy policies presented for their approval or acquiescence: A M McDonald and L F Cranor, "The Cost of Reading Privacy Policies" (2008) 4 *Journal of Law and Policy for the Information Society* 540.

[64] See ACCC Digital Platforms Report, above n 3, 405; Solove, 'Privacy Self-Management', above n 15, 1885; J Valentino-De Vries, N Singer and A Krolik, 'Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret' (The New York Times, 10 December 2018); Stigler Center Digital Platforms Report, above n 6, 31.

[65] ACCC Digital Platforms Report, above n 3, 418-421; 'CPRC Day in the Life of Data Report', above n 46, 31; Solove, 'Privacy Self-Management', above n 15, 1889 ("there are also scores of entities that traffic in personal data without people ever being aware"). See also United Kingdom Information Commissioner's Office, 'Privacy Regulators Study Finds Internet of Things Shortfalls' (Media Release, 22 September 2016) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/privacy-regulators-study-finds-internet-of-things-shortfalls/>.

[66] Lindh and Nolin, above n 47, 7.

[67] Whittington and Hoofnagle, 'Unpacking Privacy's Price', above n 13, 1358.

[68] Consumers have commented that privacy policies are phrased "in words that we cannot even think in", that "you need to have a master's degree to understand"; or it seems "they write it purposely so that normal people cannot understand it": 'CPRC Day in the Life of Data Report', above n 46, 21, 25.

[69] See Norwegian Consumer Council, 'Every Step You Take: How Deceptive Design Lets Google Track Users 24/7' (November 2018); Gillian K Hadfield, Robert Howse and Michael J Trebilcock, 'Information-Based Principles for

In their overall presentation, many privacy policies give the impression that suppliers are using these documents as a marketing opportunity to manipulate, confuse and overwhelm consumers into acceding to their data practices, rather than to inform.[70] The inappropriateness of this style is evident if we compare analogous situations – it would clearly be unacceptable for a snack food manufacturer to use a similar approach in providing standard nutritional information (see Figure 1 below). By contrast, online suppliers regularly take advantage of a social atmosphere to benefit from the human desire to disclose information to forge social connections.[71] The disclosure of our personal information to complete strangers who will use it for commercial purposes is not salient in these settings.[72]

Where a supplier does provide consumers with any means of protecting their privacy, the relevant processes generally require action by the consumer (less privacy is the default),[73] and introduce unnecessary complexity where the consumer attempts to limit or opt out of the disclosure of information.[74]

To be clear, the issue is not just the presentation of the terms themselves but the lack of

---

Rethinking Consumer Protection Policy' (1998) 21 *Journal of Consumer Policy*, 131, 143 ("Looking at the strategic response that firms are likely to make to disclosure regulations, it is not hard to predict that, given that the information they are being forced to disclose is of strategic value and that any representations made in compliance with a disclosure regulation will in turn form the basis for liability if untrue and misleading, sellers will attempt to minimize disclosure and liability by complying through obfuscation and complex or difficult to decipher (or even receive) statements.")

[70] See Stigler Center Digital Platforms Report, above n 6, 31.

[71] See Solove, 'Privacy Self-Management', above n 15, 1895 ("many websites are designed to encourage exposure while minimizing awareness of the risks"); Leslie K John, 'Uninformed Consent' (2018) *The Big Idea: Harvard Business Review*.

[72] Bruce Schneier, *Data and Goliath* (Norton, 2015) 239.

[73] Norwegian Consumer Council, 'Deceived by Design', above n 61, 13-15. On the power of defaults ("opt outs") over consumer behaviour, and welfare-enhancing defaults, see Michael S Barr, Sendhil Mullainathan and Eldar Shafir, 'A One-Size-Fits-All Solution', *New York Times* (Online, 26 December 2007).

[74] ACCC Digital Platforms Report, above n 3, 424-434; Norwegian Consumer Council, 'Deceived by Design', above n 61, 19; 'CPRC Day in the Life of Data Report', above n 46, 25. See further Ryan Nakashima, 'AP Exclusive: Google Tracks Your Movements, Like it or Not' (AP News, 14 August 2018); Mary Hanbury, 'Alexa Can Now Delete Your Recorded Voice Commands, But Amazon Hasn't Made it Easy' (Business Insider Australia, 30 May 2019).

transparency about current and future data practices and the ability to understand the consequences of these practices.[75] It is not the case, as some scholars have asserted, that consumers "are generally able to assess the risks of disclosure or other misuse of their information, and to assess the expected costs to themselves if such misuse should occur", even with revelations by regulators.[76] Nor is the acceptance of privacy terms simply a matter of "present bias" (that is, consumers overvalue the immediate benefits of free online services relative to future consequences of overbroad privacy terms).[77] Given the lack of candour and transparency on the part of suppliers, consumers have little hope of understanding the content and future consequences of these decisions even if they are diligent and concerned.[78] How can we compare future costs to present benefits when we are plainly prevented from understanding the future costs?[79]

[75] Hull, above n 32, 91 ("data mining conspires to make consent meaningless because the uses to which data will be put are not knowable to the user—or perhaps even the company— at the time of consent"); Whittington and Hoofnagle, 'Unpacking Privacy's Price', above n 13, 1359-1360.

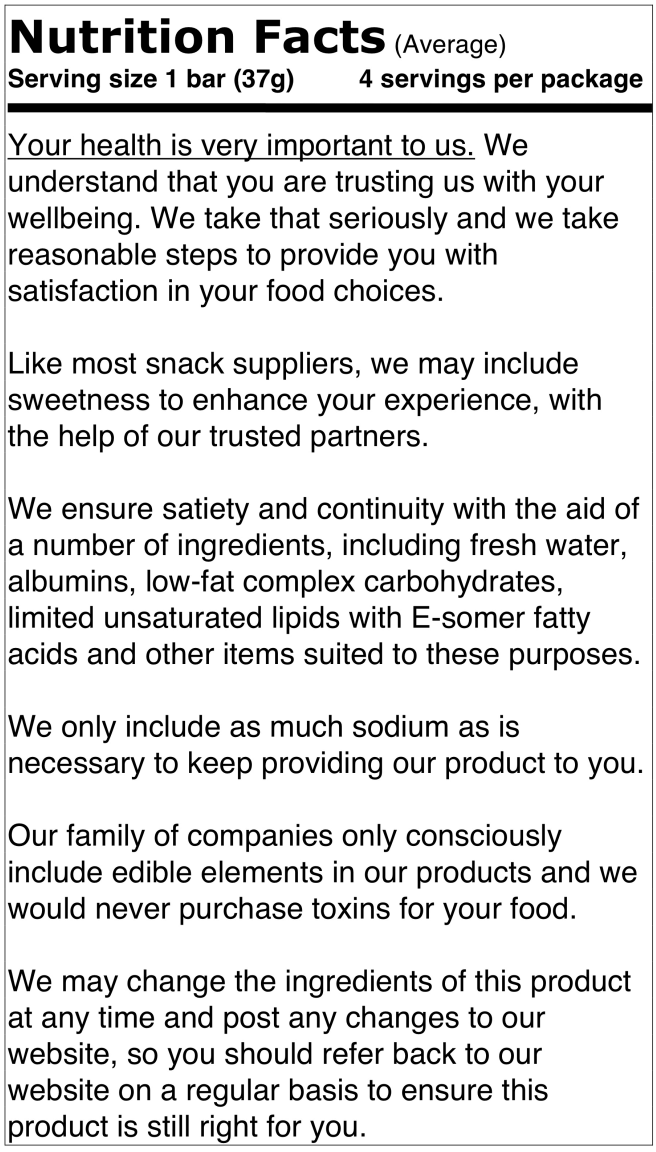
[76] Manne and Sperry, above n 8, 3.

[77] Leslie K John, 'Uninformed Consent' (2018) *The Big Idea: Harvard Business Review*; Oxera, 'Too Much Information? The Economics of Privacy' (Oxera Agenda, October 2014) 3. See A Acquisti and J Grossklags, 'Privacy Attitudes and Privacy Behavior' in J Camp and R Lewis (eds), *Economics of Information Security* (Kluwer, 2004) 165-178.

[78] See Privacy Commissioner of Canada Consent and Privacy Report, above n 32, 9.

[79] Hull, above n 32, 93 ("users do not and cannot plausibly be expected to know enough—neither about the uses to which their information might be put, nor about the specific benefits and harms that might result from those uses, nor about the likelihood that such harms might result—for consent to be meaningful"); Solove, 'Privacy Self-Management', above n 15, 1881 ("It is virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer without an understanding of the potential downstream uses …"). There is also the difficulty that the benefit may be far more limited than consumers realise –eg, targeted ads may be no better than contextual ads: Katherine Strandburg, 'Free Fall: The Online Market's Consumer Preference Disconnect' [2013] *University of Chicago Legal Forum* 95, 172.

Figure1: If Nutritional Information were Drafted Like Privacy Policies



Nutrition Facts (Average)

Serving size 1 bar (37g) **4 servings per package**

Your health is very important to us. We understand that you are trusting us with your wellbeing. We take that seriously and we take reasonable steps to provide you with satisfaction in your food choices.

Like most snack suppliers, we may include sweetness to enhance your experience, with the help of our trusted partners.

We ensure satiety and continuity with the aid of a number of ingredients, including fresh water, albumins, low-fat complex carbohydrates, limited unsaturated lipids with E-somer fatty acids and other items suited to these purposes.

We only include as much sodium as is necessary to keep providing our product to you.

Our family of companies only consciously include edible elements in our products and we would never purchase toxins for your food.

We may change the ingredients of this product at any time and post any changes to our website, so you should refer back to our website on a regular basis to ensure this product is still right for you.

Consumers are often unaware that they have purportedly consented to terms which provide permission for the supplier to:

- aggregate information from multiple sources (online and offline) to create detailed consumer profiles,[80] and/or place the consumer within consumer segments, which can negatively affect the future opportunities of the consumer;
- track the consumer's physical location, and proximity to others, beyond what is required for the provision of the service;[81]
- collect and retain the consumer's biometric data – for example, heart rate, blood pressure, physical activity – beyond that which is necessary for the consumer's purposes;[82]
- use the personal information for purposes not reasonably within the expectation of consumers;[83]
- disclose the personal information to other entities not reasonably within the expectation of consumers;[84]
- store personal information longer than necessary or indefinitely;
- transfer personal data in a sale of business, or as a separate asset, without being obliged to impose restrictions on the purchaser of that information;
- exchange the consumer's personal information with data aggregators, data brokers and/or data analytics firms;[85] and
- exclude or severely limit the liability of suppliers for unauthorised use or disclosure of the consumer's personal information.[86]

[80] 'CPRC Day in the Life of Data Report', above n 46, 7-8, 29.

[81] Research has shown the majority of Australian consumers do not want their location data shared with third parties: P Nguyen and L Solomon, 'Consumer Data and the Digital Economy' (Report, Consumer Policy Research Centre, 2018) 60.

[82] Uri Gal, 'The Age of Big Data is Going to Change How We Behave' (The Conversation, 12 October 2016).

[83] See ACCC Digital Platforms Report, above n 3, 399-400, 414-422.

[84] Hull, above n 32, 91.

[85] 'CPRC Day in the Life of Data Report', above n 46, 8-11.

[86] Hoofnagle and Whittington, 'Free: Accounting for the Costs', above n 14, 625.

Revelations about some of the actual data practices of suppliers generally come only from sporadic media reports following major data breaches.[87] These reports give rise to some distrust but concerned consumers often feel there is no practical means of protecting their information or making any real difference. Many become desensitized by repeated reports of data breaches.[88] Resignation and despair are evident, with consumers expressing the sense that constant data collection is inescapable.[89]

Regardless of an individual consumer's subjective attitude to privacy and suppliers' data practices, these concealed practices impose objective costs and detriments on consumers, including those described in the following section.

Objective consumer detriments from concealed data practices and degraded data privacy

Increasing the "Attack Surface" and Resultant Risks of Hacking, Accidental Disclosure and Illegal Use of Personal Information

Weak privacy protections increase the "attack surface" of the consumer's personal information. The more personal information is collected and stored, the more broadly it is disclosed, and the longer it is stored, the more likely it will be hacked, accidentally disclosed or used for illegal purposes.[90] This is not simply a question of the quality of the supplier's data security systems.

---

[87] Leslie K John, 'Uninformed Consent' (2018) *The Big Idea: Harvard Business Review*.

[88] Acquisti, 'The Economics of Personal Data and Privacy', above n 7, 13.

[89] 'CPRC Day in the Life of Data Report', above n 46, 21; 'CPRC Emerging Issues Report', above n 6, 4; Joseph Turow, Michael Hennessy and Nora Draper, 'The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them up to Exploitation' (Report, Annenberg School for Communication, University of Pennsylvania, June 2015) https://www.asc.upenn.edu/sites/default /files/TradeoffFallacy_1.pdf ("more than half do not want to lose control over their information but also believe this loss of control has already happened"). See further Stucke and Ezrachi, 'Digital Assistants', above n 53, 1292-1293.

[90] See, eg, ACCC, 'Digital Platforms Inquiry: Preliminary Report' (December 2018) 200, on improper disclosures of personal data of Facebook users in the Cambridge Analytica breach; *Data on 540 Million Facebook Users Exposed*, (BBC Online, 4 April 2019) <https://www.bbc.com/news/technology-47812470>; L Newman, 'A New Google+ Blunder Exposed Data From 52.5 Million Users' (Wired online, 12 October 2018).

Data security experts acknowledge that even highly secure systems are almost certain to be breached at some stage.[91] Absent a hack, data may be improperly accessed (including by the supplier's own employees or contractors),[92] exposed or used due to technical glitches or operator error.[93] These risks are greatly increased by the fact that this personal information may later be controlled by a subsequent purchaser of the supplier's business,[94] or data brokers, aggregators or associates, who are not contractually obliged to protect the consumer's information.[95] The extent of data collected, the duration of its storage and the extent of its disclosure are all factors which, *in themselves*, increase the vulnerability of the data.

Identity theft is a key risk created by increased collection and disclosure of personal information.[96] Following a data breach, perpetrators may wait an extended period to commit identity theft against the consumer, sometimes using the opportunity of a further breach which reveals additional information. When identity theft occurs, the victim may spend years attempting to clear their name of debt, bankruptcy and criminal activity, suffering repeated losses in their quality of life, reputation, finances and time.[97] This difficulty becomes extreme in

<https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/ >.

[91] Bruce Schneier, 'Data is a Toxic Asset, So Why Not Throw It Out?' (CNN online, 1 March 2016) <https://edition.cnn.com/2016/03/01/opinions/data-is-a-toxic-asset-opinion-schneier/index.html>.

[92] See, eg, Amended Statement of Claim, *Tracy Evans v Health Administration Corporation & Anor* (NSWSC 2017/00374456), filed 27 March 2018, claiming for damage caused by a contractor of NSW Ambulance Service accessing, compiling, and selling the medical records of ambulance employees without their knowledge or consent.

[93] Hoofnagle and Whittington, 'Free: Accounting for the Costs', above n 14, 644-48; Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 University of Pennsylvania Law Review 477, 515.

[94] Whittington and Hoofnagle, 'Unpacking Privacy's Price', above n 13, 1363-1364.

[95] See Hoofnagle and Whittington, 'Free: Accounting for the Costs', above n 14, 628, 633; 'CPRC Day in the Life of Data Report', above n 46, 8-11.

[96] See Danielle Keats Citron, 'Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age' (2007) 80 *Southern California Law Review* 241, 246-256; Acquisti, 'The Economics of Personal Data and Privacy', above n 7, 15-17. In 2016, 11% of Australians had been the victim of identity theft: P Jorna and R G Smith, 'National Identity Security Strategy: Identity Crime and Misuse in Australia 2017' (AIC Statistical Report, 2019) 36.

[97] See P Jorna and R G Smith, 'National Identity Security Strategy: Identity Crime and Misuse in Australia 2017' (AIC Statistical Report, 2019) (reporting that impacts on victims of identity fraud include refusal of credit, refusal of

the case of biometric identity theft, where a person's very physical features – their iris scans or fingerprints – are stolen from digital databases and used to impersonate.[98]

The increased exposure of personal information to attack should be recognised as a detriment to the individual even before harm of this kind crystallises. Increased vulnerability to serious harm is detriment in itself. The law recognises, for example, that medical malpractice which increases a patient's vulnerability to a disease or disorder causes damage to the patient before the disease or disorder is actually contracted.[99] So too unfair data practices which increase a consumer's vulnerability to hacking and other unauthorised data access are detrimental to the consumer.[100]

Data breaches may be an inescapable fact of twenty-first century existence. This does not mean that we should resign ourselves to the harm. Rather, the practices which provide the opportunity for this harm – the collection, storage, use and disclosure of personal information – should be minimized and kept proportionate to the real benefits they are likely to create for consumers.

government benefits, mental and emotional distress, financial difficulties resulting in repossession of house, land or motor vehicles, legal action, wrongful accusation of criminal conduct and reputational damage).

[98] Citron, above n 96, 254 fn 71 ("A thief's use of an individual's biometric data to commit identity theft will create enormous problems for victims seeking to prove the theft, as all identity-theft victims face a certain amount of difficulty in proving that fraudulent expenses are not their own. … But the likely assumption that one's fingerprint does not lie compounds that difficulty for an individual who suffers financial theft as a result of the leak of the individual's biometric.").

[99] Daniel J Solove and Danielle Keats Citron, 'Risk and Anxiety: A Theory of Data-Breach Harms' (2018) 96 *Texas Law Review* 737, 761-762.

[100] Ibid.

Disclosure of Personal Information the Consumer Does Not Wish to Disclose

Modern data practices allow suppliers to place the consumer under the microscope,[101] without making consumers aware of the scrutiny. Consumers may be aware that they are disclosing their name, address, mobile phone number, product preferences and credit card details. They are much less likely to be aware of suppliers tracking their subsequent internet browsing history and the way they navigate websites, down to scroll speed, hovering over images and clicks; or the fact that the data they provide is combined with further personal information collected from other suppliers and data aggregators to permit more detailed scrutiny of,[102] and inferences about, the consumer's characteristics, behaviour and tendencies.[103] New developments may even allow early detection of the onset of diseases, such as Parkinson's and Alzheimer's, from consumers' "tremors when using a mouse, repeat queries and average scrolling velocity".[104]

The original information disclosed by the consumer may seem innocuous. It may seem less innocuous when combined with continued, unanticipated tracking of the consumer's behaviour and aggregation of that information with other data, including age, gender, occupation, social media activity, purchasing history, details of children and spouses and other more sensitive

[101] Stigler Center Digital Platforms Report, above n 6, 7 ("what digital businesses can learn by using high-dimensional, large datasets to explore every nook and cranny of consumers' many behavioral shortcomings and biases in real time").

[102] Eg, few consumers would be aware that Acxiom has marketed a product which allows suppliers to request only a postcode from the customer at the point of sale and combine that postcode with the sale transaction data to provide the merchant with the customer's undisclosed address: Whittington and Hoofnagle, 'Unpacking Privacy's Price', above n 13, 1361-1362.

[103] 'CPRC Emerging Issues Report', above n 6, 11-12, 60; 'CPRC Day in the Life of Data Report', above n 46, 29-30. See also Hoofnagle and Whittington, 'Free: Accounting for the Costs', above n 14, 610, 636-37; Stigler Center Digital Platforms Report, above n 6, 25.

[104] Sumathi Reddy, 'Clues to Parkinson's and Alzheimer's From How You Use Your Computer: A Study Involving the Microsoft Search Engine Bing Shows How Artificial Intelligence Might Detect Medical Conditions Traditional Medicine Misses', *Wall Street Journal* (online, 29 May 2018). See further Citron, above n 96, 253-255 (on the potential for retina scans and fingerprints to reveal diseases and genetic disorders).

information.[105] This information can also be used to make disadvantageous inferences about the consumer, as explained below.

Combining personal data from multiple sources is made possible by a data ecosystem which is almost entirely invisible and unknowable for consumers.[106] Data aggregators compile immense quantities of personal information about individual consumers, using data acquired from suppliers with whom the consumer has dealt as well as data acquired from other data brokers and aggregators with whom the consumer has never had any dealings.[107] This personal information can be used to make inferences about consumers' intimate characteristics,[108] and profile and sort consumers, particularly to compile lists of consumers for sale to other suppliers and data brokers.[109]

Importantly, the aggregation of personal data may also be used to *re-identify* sensitive information which the consumer disclosed in other contexts in the belief that this sensitive information was disclosed on a de-identified or anonymous basis.[110] This unanticipated

[105] 'CPRC Emerging Issues Report', above n 6, 13-15; Hoofnagle and Whittington, 'Free: Accounting for the Costs', above n 14, 637-639. Solove, 'Privacy Self-Management', above n 15, 1889 ("people … greatly struggle to factor in how their data might be aggregated in future. … Unexpectedly, this data might be combined and analyzed to reveal sensitive facts about the person. The person never disclosed these facts nor anticipated that they would be uncovered. The problem was that the person gave away too many clues."). See also Brief for Technology Companies as Amici Curiae in Support of Neither Party, *Carpenter v United States*, No 16-402, 2017 WL 3530959 (14 August 2017) 25 ("digital devices and services produce and record data that, alone or in the aggregate, has the potential to reveal highly sensitive information about all aspects of our private lives").

[106] Solove, 'Privacy Self-Management', above n 15, 1889 ("there are also scores of entities that traffic in personal data without people ever being aware"); Leslie K John, 'Uninformed Consent' (2018) *The Big Idea: Harvard Business Review*.

[107] Federal Trade Commission, United States, 'Data Brokers: A Call for Transparency and Accountability' (Report, May 2014); 'CPRC Day in the Life of Data Report', above n 46, 8-11; Hoofnagle and Whittington, 'Free: Accounting for the Costs', above n 14, 633; Acquisti, 'The Economics of Personal Data and Privacy', above n 7, 8.

[108] See Citron, above n 96, 253-255 (on the potential use of biometrics to reveal diseases and genetic disorders).

[109] Ibid. See also Privacy Commissioner of Canada Consent and Privacy Report, above n 28, 6-7.

[110] See Luc Rocher, Julien M Hendrickx and Yves-Alexandre de Montjoye, 'Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models' (2019) 10 *Nature Communications* 3069; Privacy Commissioner of Canada Consent and Privacy Report, above n 28, 15-16 (risk of re-identification increases over time); Crémer, De Montjoye and Schweitzer, above n 4, 77-78, 86. See also Joseph A Cannataci, 'Report of the Special Rapporteur on the Right to Privacy to the General Assembly of the United Nations' (Advanced Unedited Report, A/73/45712, 17 October 2018) [61]-[67].

collection and combination of information can reveal far more intimate details of the consumer's sexual activity, sexual orientation, religion, political views, level of debt, consumption of alcohol, tobacco and other drugs, diseases, disorders, insecurities, behavioural biases, and financial vulnerability, details the consumer would never have chosen to disclose to the supplier in question or other suppliers who may use the services of a data broker.[111]

Personal Information Used to Discriminate, Manipulate and Exclude

Consumers are not generally aware of how they have been profiled or the lists in which they have been included.[112] The ACCC pointed out in its Digital Platforms Report that Facebook advertising categories in Australia included "opposition to immigration"; "far left politics"; "vaccine controversies; and "climate change denial".[113] Quantium, a data broker, states that it divides Australian households into 15 distinct customer segments, including "Affluent Adventurers", "Countryside Elite", "Suburban Thrift" and "Prosperous Families", "based entirely on real-world people and their real-world transactions".[114] In its 2014 investigation into the data broker industry, the US Federal Trade Commission revealed some of the euphemistically named lists which are traded between data brokers and suppliers, including "Diabetes Interest"; "Cholesterol Focus"; "Financially Challenged"; and "Urban Scramble".[115]

The aggregation and disclosure of consumers' personal information in the process of consumer profiling and segmenting can cause significant financial detriment. Data collected about a consumer without their knowledge can be used to discriminate against the consumer on the

[111] See 'CPRC Emerging Issues Report', above n 6, 23-24, 32-33; Hull, above n 32, 92; 'CPRC Day in the Life of Data Report', above n 46, 15, 36.

[112] Hoofnagle and Whittington, 'Free: Accounting for the Costs', above n 14, 633-634.

[113] ACCC Digital Platforms Report, above n 3, 446.

[114] Quantium, 'Q.Segments Crowds Brochure', (Quantium website) accessed 4 August 2019, <https://www.quantium.com/wp-content/uploads/2018/07/Q.Segments_Crowds_brochure_2018.pdf>.

[115] Federal Trade Commission, United States, 'Data Brokers: A Call for Transparency and Accountability' (Report, May 2014) 47.

basis of their online and offline behaviour.[116] This information can be used to draw unexpected and adverse inferences about the consumer's credit risk on the basis of items they purchase or places they visit,[117] or to charge the consumer more on the basis of their perceived ability to pay.[118] It may mean, for example, that the consumer is charged higher interest rates or insurance premiums;[119] shown more expensive search results;[120] quoted higher prices for the same product;[121] or completely excluded from certain offers.[122]

Suppliers are also known to use profiling, micro-targeting and manipulation[123] to take advantage of consumer needs, habits, addictions and vulnerabilities.[124] As Pasquale has

[116] See Stucke and Ezrachi, 'Digital Assistants', above n 53, 1263-1270. Cf the description of a hypothetical "virtuous" digital assistant that "could warn users when behavioral discrimination is at play, when outside options are ignored, when price alignment seems out of order, or when personal data is collected. They may even deploy countermeasures to maximize user welfare in the face of such strategies … They can promote users' interest—aware of their preferences and safeguarding their autonomy.": at 1287.

[117] See Hull, above n 32, 91 (on estimates of the likelihood of default and credit delinquency based on purchases of felt pads to protect furniture versus visits to Sharxx Pool Bar and obesity).

[118] Acquisti, 'The Economics of Personal Data and Privacy', above n 7, 17. See Rafi Mohammed, 'How Retailers Use Personalised Prices to Test What You are Willing to Pay' (Harvard Business Review online, 20 October 2017).

[119] See Productivity Commission, Australian Government, 'Data Availability and Use' (Inquiry Report No 82, 31 March 2017) 86-89 (on data sharing in the context of insurance companies' risk analysis and marketing).

[120] See, eg, Dana Mattioli, 'On Orbitz, Mac Users Steered to Pricier Hotels', *The Wall Street Journal* (online, updated 23 August 2017).

[121] See Christopher Townley, Eric Morrison and Karen Yeung, 'Big Data and Personalised Price Discrimination in EU Competition Law' (King's College London Dickson Poon School of Law, Legal Studies Research Paper Series: Paper No 2017-38) 1-2.

[122] Federal Trade Commission, 'Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues' (Report, January 2016) 9-12; 'CPRC Emerging Issues Report', above n 6, 24-25; 'CPRC Day in the Life of Data Report', above n 46, 36; Stacy-Ann Elvy, "Commodifying Consumer Data in the Era of the Internet of Things" (2018) 59 *Boston College Law Review* 423, 449-451. See further Office of the Privacy Commissioner of Canada, 'The Age of Predictive Analytics: From Patterns to Predictions' (Report, August 2012).

[123] See Susser, Roessler and Nissenbaum, above n 5 ('In our view, manipulation is hidden influence … manipulating someone means intentionally and covertly influencing their decision-making, by targeting and exploiting their decision-making vulnerabilities. Covertly influencing someone … means influencing them in a way they aren't consciously aware of, and in a way they couldn't easily become aware of were they to try and understand what was impacting their decision-making process.').

[124] European Data Protection Supervisor, above n 3, 8-9. See further Damian Clifford, 'Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side?' (forthcoming in Lilian Edwards, Burkhard Schafer and Edina Harbinja (eds), Future Law Series (Edinburgh University Press) (on the use of emotion detection technology to create "emotionally tailored profiles" adding "a layer of manipulation" and

testified, lists have been compiled – lists of real people who suffer from depression, impotence, sexually transmitted diseases, Alzheimer's disease and dementia, people who are victims of sexual assault.[125] Such lists may be used to exploit people in their most vulnerable moments for financial gain. Data analytics have also been used to manipulate individuals for the purpose of research, without their knowledge or consent.[126]

Calo has explained the harm caused by "vulnerability-based marketing" built on these practices, which exploits the particular vulnerabilities of consumers, as revealed by their personal information.[127] Some firms are taking this further, deliberating *engineering* moments of vulnerability tailored to the individual and exploiting these vulnerabilities for financial gain.[128]

> "A manufacturer of highly addictive painkillers has been using data-matching techniques to track people's Google health searches and target them with ads that increase in intensity until they respond. … It was continuing to promote the use of opioids to treat chronic pain even though current science and medical guidelines suggest they should be avoided and can potentially make chronic pain worse."
> Alison Branley, 'Google Search Data Used by Pharma Giant to Bombard Users with Ads for Addictive Opioids' (ABC Online, 13 July 2019)

interference with autonomy with "the ability to target individuals on the basis of their emotional status and personalise the nature of the appeal to match").

[125] Frank Pasquale, Written Testimony Before the United States House of Representatives Committee on Energy and Commerce: Subcommittee on Digital Commerce and Consumer Protection, 'Algorithms: How Companies' Decisions About Data and Content Impact Consumers' (29 November 2016) 3-4.

[126] See Hull, above n 32, 92.

[127] Ryan Calo, "Digital Market Manipulation" (2014) 82 *George Washington Law Review* 995; Ryan Calo and Alex Rosenblat, "The Taking Economy: Uber, Information and Power" (2017) 117 *Columbia Law Review* 1623. See also See Stigler Center Digital Platforms Report, above n 6, 22-23, 35-36.

[128] Ibid. See also Susser, Roessler and Nissenbaum, above n 5 (on the larger threats to individual autonomy).

"At Woolworths Rewards, we have a big member database. We also have big data. Every time someone shops, scans and saves, we collect data to learn a little bit more about them.
… we've developed a state of the art "personalisation engine" that analyses our data …
To match our offers to each member, we asked their shopping data a series of questions – Have they bought it before? How often? And at what price? Do they even care about price? … Our engine essentially asks each member 70 million questions each and every week."
"WOW Personalisation", YouTube video, https://www.quantium.com/media/ accessed 5 August 2019

4. Are concealed data practices a competition law issue?

Concealed data practices potentially give rise to claims under privacy law (although the prospects of redress are limited in Australia),[129] or consumer law, including misleading or deceptive conduct, unconscionable conduct and/or unfair contract terms.[130] They also demonstrate a need for consumer protection and/or privacy regulation to be strengthened to provide consumers with greater protection, information and choices.[131]

But do the effects of concealed data practices also warrant consideration under competition law? This section outlines the two main responses to this question and proposes a third.

[129] See Australian Privacy Foundation, Submission to ACCC Digital Platforms Inquiry (February 2019) 5-10. And in the United States: Stigler Center Digital Platforms Report, above n 6, 6.

[130] See, eg, Carmen Langhanke and Martin Schmidt-Kessel, 'Consumer Data as Consideration' (2015) 6 *EuCML* 218; Mark Briedis, Jane Webb and Michael Fraser, 'Improving the Communication of Privacy Information for Consumers: Issues, Options and Recommendations' (Report, February 2016).

[131] See ACCC Digital Platforms Report, above n 3, Chap 7 (regarding the ACCC's recommendations to amend the *Privacy Act 1988* (Cth) and the Australian Consumer Law to address these market failures).

4.1 Data privacy is a non-economic objective outside the true goals of competition law

Some commentators claim the quality of privacy protections offered in the course of digital services is a matter of individual preference, which should be left to the individual consumer.[132] According to these views, certain consumers may have a subjective sensitivity to privacy issues, but there is no satisfactory way of taking this into account in the objective, economic assessments of competition law.[133] Even if privacy protection is a worthy social goal, the argument goes, it is a goal that falls outside the objectives of competition law.[134]

On this view, antitrust is concerned with improving consumer welfare in the form of economic efficiency. It does so by protecting the competitive process, which generally improves that efficiency, measured in terms of price and output levels of the relevant product. Data privacy is seen as a non-economic objective which does not sit comfortably with economic assessments of competition.[135]

Some continue to assert that there is, in any case, a "privacy paradox" at work.[136] That is, while consumers repeatedly claim in surveys that they are increasingly concerned about their online privacy, their behaviour in continuing to deal with suppliers that offer privacy-intrusive terms indicates that privacy is not in fact a high priority for consumers in these transactions. Accordingly, there may be no real need for regulatory intervention of any kind.

---

[132] See Acquisti, 'The Economics of Personal Data and Privacy', above n 7, 4, citing E M Noam, 'Privacy and Self-Regulation: Markets for Electronic Privacy' in US Department of Commerce, 'Privacy and Self-Regulation in the Information Age' (1997); Manne and Sperry, above n 8, 5-6.

[133] Sokol and Comerford, above n 7, 1156-1161; Manne and Sperry, above n 8, 3, 5-6.

[134] Sokol and Comerford, above n 7, 1156-1161.

[135] See Geoffrey Manne and Ben Sperry, 'Debunking the Myth of a Data Barrier to Entry for Online Services' (Truth on the Market Blog, 26 March 2015).

[136] See Patricia A Norberg, Daniel R Horne and David A Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviours' (2007) 41 *Journal of Consumer Affairs* 100 (explaining the concept of a "privacy paradox" and research to explain the phenomenon); Susan Athey, Christian Catalini and Catherine Tucker, 'The Digital Privacy Paradox: Small Money, Small Costs, Small Talk' (NBER Working Paper No 23488, 2017).

4.2 Data privacy is relevant to competition policy and we should place a value on consumer data

Others have challenged the view that consumers are engaging in an informed bargain in respect of their data privacy. Recognising that personal information is collected about consumers and used to fund the provision of zero- or low-priced services, some scholars have suggested that consumers are in fact "paying" or bartering for these services with their personal information.[137] That is, while the marketed price is at or near zero, the true price of the services is represented by the value of the personal information collected about that consumer and the value of the permitted uses of that information.[138] If the value of the consumer's information were known, it may become apparent that a competitive price would not be zero but a negative price: the supplier would *pay* the consumer in money or other benefits to use the service and permit collection of their personal information.[139] However, in reality, neither the precise extent of the data collection and use, nor the value of the consumer's information (in absolute terms or relative to the value of the service), are generally known by the consumer.[140]

By way of analogy, we might suppose that, although the services to consumers appear to be free, there is actually an undeclared charge of an indeterminate amount against the consumer's bank account each time they use the service. The consumer has lost some of his or her information privacy and the supplier has gained access to, and use of, personal information, but

[137] See Hoofnagle and Whittington, 'Free: Accounting for the Costs', above n 14, 625; Gianclaudio Malgieri and Bart Custers, 'Pricing Privacy: The Right to Know the Value of Your Personal Data' (2018) 34 *Computer Law & Security Review* 289. Consumers also provide their attention (to advertisements) in exchange for online content: John M Newman, 'The Myth of Free' (2018) 86 *George Washington Law Review* 513, 551-555; Evans, 'Attention Platforms', above n 7.

[138] See OECD, 'Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value' (White Paper, 2013) 18-33. See Stigler Center Digital Platforms Report, above n 6, 32-33.

[139] See Stigler Center Digital Platforms Report, above n 6, 32-33; UK Competition and Markets Authority, 'The Commercial Use of Consumer Data: Report on the CMA's Call for Information' (Report, June 2015) paras 2.106-2.107.

[140] Hoofnagle and Whittington, 'Free: Accounting for the Costs', above n 14, 610; Stigler Center Digital Platforms Report, above n 6, 45; Acquisti, Taylor and Wagman, 'The Economics of Privacy', above n 14, 447-448 (on attempts to value, and permit consumers to trade in, personal information).

the value respectively lost and gained cannot be quantified. The debate has often been framed along these lines. In this context, many point out that the value of the personal information divulged per transaction may be very low for supplier.[141] The true value for the supplier lies in accumulating vast quantities of high quality personal data and applying proprietary algorithms to that data. Further, the value of the same type and amount of personal information may vary greatly from consumer to consumer, depending on their personal privacy preferences.[142] One cannot put a price tag on the personal data disclosed to receive the free service.

4.3 Degraded data privacy creates objective consumer detriment and undermines the competitive process

There is a more apt way to conceptualise these uses of consumer data. By an alternative analogy, we might suppose that, as part of the terms of service, the consumer is required to install certain software on their computer which facilitates the service and creates value for the supplier, but also makes the consumer's computer much more vulnerable to hacking. For most consumers, the creation of this vulnerability is completely invisible and they will never learn the cause of the risk or the actual harm. What we *do* know is the overall quality of the service is reduced by this requirement because of the *costs* it creates for consumers.[143] The value of the service could even be reduced to the extent that the service is, on balance, detrimental to the consumer.[144]

---

[141] See Körber, above n 8, 3, 9-10.

[142] Körber, above n 8, 10.

[143] Cf Katherine Strandburg, 'Free Fall: The Online Market's Consumer Preference Disconnect' [2013] *University of Chicago Legal Forum* 95, 151 (proposing the analogy of "obtaining free medical care in exchange for participating in a trial of a new medical treatment", considering how difficult it is for users to measure the disutility associated with the transaction). See Gal and Rubinfield, above n 16, fn 65.

[144] The "Health Engine" app appeared to provide Australian patients with a simple means of booking appointments with multiple healthcare providers, but, without patients' knowledge, was also selling information concerning patients' medical conditions and symptoms to law firms that intrusively and persistently pursued patients with offers to represent them in personal injuries claims: Pat McGrath, Clare Blumer and Jeremy Story Carter, 'Medical Appointment Booking App Health Engine Sharing Clients' Personal Information with Lawyers' (ABC News Online, 26 June 2018). The "We-Vibe" "smart" vibrator collected "extraordinarily intimate and personal" usage information without the knowledge of its users and was able to be accessed so that hackers could take control of the vibrator and activate it remotely, according to a class action brought against Standard Innovation: Kimiko de Freytas-

In a similar way, weak privacy protections cause objective detriment to consumers. This detriment is not a matter of personal preference. Objectively speaking, degraded data privacy imposes future costs on consumers,[145] including increased risks of data breach, identity theft, hacking and fraud; exposure of sensitive information the consumer would not wish to disclose through unanticipated collection and tracking, and/or re-identification of de-identified information; and exposure to manipulation-based marketing, profiling, segmenting or scoring which can lead to discrimination,[146] exclusion or disadvantage more generally for the consumer.

The existence of these detriments does not mean consumers should not disclose their personal information. It does mean, in the antitrust context, that terms requiring the collection and disclosure of personal information impose objective costs on consumers which should be taken into account, along with the benefits provided by the service or platform in question, when assessing competition in a given market.

Concealed data practices undermine the competitive process

These practices do not only impose costs on the individual concerned. They also undermine the competitive process which competition law aims to protect. This weakening of the competitive process occurs both in the initial market – the market in which the personal information is collected – and in markets where that personal information is subsequently used contrary to the reasonable expectations of the consumer.

Tamura, 'Maker of "Smart" Vibrators Settles Data Collection Lawsuit for $3.75 Million' (The New York Times, 14 March 2017). The "Brightest Flashlight Free" app appeared to provide a free flashlight on mobile phones, without revealing to users that it also transmitted device data "including precise geolocation along with persistent device identifiers, to third parties, including advertising networks": *Golden Shores Technologies LLC* (US Federal Trade Commission) <https://www.ftc.gov/sites/default/files/documents/cases/131205goldenshorescmpt.pdf>.

[145] See Acquisti, 'The Economics of Personal Data and Privacy', above n 7, 5; Acquisti, Taylor and Wagman, 'The Economics of Privacy', above n 14, 483-484.

[146] Federal Trade Commission, 'Big Data: A Tool for Inclusion or Exclusion?' (Report, January 2016).

Raising the quality-adjusted price and chilling competition on privacy quality

Decreasing privacy quality / raising the quality-adjusted price

In the initial market, concealed data practices both reduce the quality of the services to consumers and stifle competition by rivals on privacy quality.

The degradation of consumer data privacy can be seen as a reduction in the quality of the service, or, to express it another way, an increase in the quality-adjusted price of the service.[147] The extent to which a firm can retain customers while degrading its customers' data privacy without offsetting benefits is one measure of market power.[148] Where a dominant firm imposes weak privacy protections on consumers (effectively charging a higher quality-adjusted price), this may be seen as exploitative conduct: conduct that takes advantage of the firm's dominant position and freedom from competitive constraints to the detriment of consumers.[149]

In the European Union, such exploitative conduct may be captured by the law against abuse of dominance under Article 102 of the *Treaty on the Functioning of the European Union* and similar national laws.[150] For example, in Germany, the Bundeskartellamt imposed far-reaching restrictions on Facebook's data practices on the ground that Facebook had used its position of dominance, and particularly its indispensability to consumers, to impose "exploitative business terms" on its users. These included terms permitting Facebook to aggregate personal information regarding its users across different services owned by Facebook (including WhatsApp and Instagram) and to track users across different websites and apps outside the

[147] Stigler Center Digital Platforms Report, above n 6, 34.

[148] Howard A Shelanski, 'Information, Innovation, and Competition Policy for the Internet' (2013) 161 *University of Pennsylvania Law Review* 1663, 1689.

[149] See Shelanski, above n 148, 1687, on the exercise of market power by reductions in quality.

[150] See Viktoria H S E Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in an Era of Big Data' (Working Paper, June 2019) 9-11 (arguing that excessive data collection might be seen as analogous to excessive pricing under Art 102 TFEU); Katharine Kemp, *Misuse of Market Power: Rationale and Reform* (Cambridge University Press, 2018) 60 (on exploitative abuses).

Facebook platforms, even when users had "blocked web tracking in their browser or device settings".[151]

Requirement for exclusionary conduct

In a number of jurisdictions, however, purely exploitative conduct does not contravene unilateral anticompetitive conduct laws.[152] Rather, a dominant firm will only contravene if it engages in *exclusionary* conduct: that is, conduct which excludes or suppresses rivalry on the part of its competitors or potential competitors. This is the case under the law against monopolization in the United States and arguably under Australia's misuse of market power law. In these jurisdictions, the law is not concerned with the mere possession of a dominant position or substantial market power, but with firms *preserving or entrenching that substantial market power by means other than superior efficiency*.[153] If rival firms are free to outcompete the incumbent with a superior offer, the market itself will produce the most efficient outcome.

According to this approach, if a dominant firm engages in purely exploitative conduct, other firms will be attracted to the market to offer a lower price or higher quality service to consumers. In the absence of exclusionary conduct, the market will self-correct.[154] Some argue that this market correction will occur in respect of the privacy quality of digital services *if* consumers actually value privacy quality. However, concealed data practices combine with a number of features of digital markets to explain why it is highly unlikely that digital markets will self-correct to a competitive level of privacy quality.[155]

---

[151] Bundeskartellamt, Germany, 'Bundeskartellamt prohibits Facebook from combining user data from different sources: Background information on the Bundeskartellamt's Facebook proceeding' (7 February 2019).

[152] See Katharine Kemp, *Misuse of Market Power: Rationale and Reform* (Cambridge University Press, 2018) 60.

[153] Explained further in Katharine Kemp, *Misuse of Market Power: Rationale and Reform* (Cambridge University Press, 2018) 58, 64.

[154] Ibid 52-55.

[155] Furman Report, above n 4, 42-45, 60; Stucke and Grunes, above n 45, 52-57.

Barriers to entry and competitive advantages in digital markets

At the outset, digital markets tend to exhibit several features which make it very difficult for new rivals to challenge dominant incumbents. Digital markets often have high barriers to entry where successful entry relies on achieving large scale to benefit from direct network effects (that is, the service is more valuable to users if it captures a large number of other users),[156] increasing returns to scale (the service produces higher returns per user as the number of users increase)[157] and economies of scope.[158] Network effects can be such that, beyond a certain level of penetration, these markets are prone to "tip" to one player that succeeds in competing for the market as a whole.[159] New entry may also be hindered by the economies of scope enjoyed by incumbents operating over multiple markets.[160] These features of digital markets can contribute to market dominance, and help to explain the increasingly enduring market power enjoyed by firms in a number of digital markets, including online search (Google), social media (Facebook), e-commerce (Amazon), digital advertising (Google and Facebook), and mobile app downloads (Apple and Google).[161]

Barriers to entry and competitive advantages increased by concealed data practices

A rival attempting to offer a product with enhanced privacy quality in a digital market is likely to face these substantial barriers to entry at the outset. But where concealed data practices exist, success for the privacy-enhancing rival is much less likely, both due to the competitive

[156] Stigler Center Digital Platforms Report, above n 6, 15. See also Crémer, De Montjoye and Schweitzer, above n 4, Chap 2; Furman Report, above n 4, 32-38; Bundeskartellamt, above n 2, 4. See further Michael L Katz and Carl Shapiro, 'Network Externalities, Competition, and Compatibility' (1985) 75 *American Economic Review* 424.

[157] Stigler Center Digital Platforms Report, above n 6, 13-14.

[158] Stucke and Ezrachi, 'Digital Assistants', above n 53, 1289-1290.

[159] Shelanski, above n 148, 1682; Stigler Center Digital Platforms Report, above n 6, 6-9, 12; *Novell, Inc v Microsoft Corp*, 505 F 3d 302, 308 (4th Cir 2007) ("once dominance is achieved, threats come largely from outside the dominated market, because the degree of dominance of such a market tends to become so extreme").

[160] Stigler Center Digital Platforms Report, above n 6, 14.

[161] Furman Report, above n 4, 31.

advantages enjoyed by the incumbent as a result of weak data protections and the concealed nature of data practices.

Importantly, suppliers in these markets are often multisided platforms: that is, the service brings together two or more distinct communities of users, for example, social media users and advertisers, shoppers and merchants, or online search users and advertisers.[162] Multisided platforms exhibit indirect network effects: one (or more) category of users values the service more highly (and will therefore pay higher prices to use the platform) the more members of *another* category of users make use of the platform.[163] Advertisers value an online search engine more highly, for example, the more consumers use that search engine.[164]

Consumers' personal data plays a critical role in these multisided platforms and the preservation of an incumbent's dominant position.[165] For example, a social media platform has an incentive harvest increasingly broad and deep personal data on its users.[166] This will cause the platform's advertising customers to value the platform more highly and pay higher advertising fees to benefit from highly detailed profiling and segmenting of the platform's users as well as the users' attention to their advertising.[167] The social media platform may then use

[162] See Jean-Charles Rochet and Jean Tirole, 'Platform Competition in Two-Sided Markets' (2003) 4 *Journal of the European Economic Association* 1; Jean Tirole, *Economics for the Common Good* (Princeton University Press, 2017) 378-385; 'Common Understanding of G7 Competition Authorities on "Competition and the Digital Economy"' (July 2019) 5.

[163] See Bundeskartellamt, above n 2, 4-5; *United States v Microsoft*, 253 F 3d 34, 55 (DC Cir 2001).

[164] Whittington and Hoofnagle, 'Unpacking Privacy's Price', above n 13, 1353-1354. Commentators point out that the dynamics of multisided sided platforms have a particular effect on optimal pricing on different sides of the platform. Eg, advertisers may be willing to pay advertising fees well above the competitive level in return for access to more search engine users and their data, while that advertising revenue subsidises the provision of services on the search engine user side of the platform at zero monetary price. See David S Evans and Richard Schmalensee, 'Matchmakers: The New Economics of Multisided Platforms' (Harvard Business Review Press, 2016) 93-100.

[165] Stigler Center Digital Platforms Report, above n 6, 16.

[166] See Part 2 above. Stucke and Ezrachi, 'Digital Assistants', above n 53, 1288 ("The super platforms already possess far more personal data than any startup could readily and affordably obtain.").

[167] Cf Manne and Sperry, above n 8, 5-6 (arguing there is "no obvious reason why monopolists would have an incentive to degrade privacy"). See explanation of indirect network effects in Bundeskartellamt, above n 2, 4-5.

the increased advertising revenue, the 'learning by doing' effects of access to a huge variety and depth of personal data,[168] and its own in-depth knowledge of its users' personal traits, interests and biases to make the platform more attractive, and tie its users to its service.[169] This results in more consumers using the service. If the social media platform continues to adopt concealed data practices in respect of this increasing number of consumers, it has even greater breadth and depth of personal data with which to attract advertising revenue and information about customers to increase the attractiveness and stickiness of its platform,[170] without deterring consumers from using the platform on the basis of its data practices, and so the cycle continues.

In the process, users suffer objective costs and detriments as a result of the concealed data practices, which make consumers more susceptible to criminal activity, discrimination, exclusion, manipulation and humiliation. In this way, concealed data practices can aid in *creating or extending market power, by means other than superior efficiency*.[171]

Concealed data practices hinder privacy-enhancing rivals. Consumers cannot place a value on the improved privacy quality offered by a rival when they cannot make any real comparison between the privacy terms and practices of the incumbent and its rivals. Further, taking into account other features of the incumbent service, the rival would have to offer consumers an apparently lower quality, or higher priced, service since the rival could not pay for other

[168] Stucke and Grunes, above n 45, 170-181; Stucke and Ezrachi, 'Digital Assistants', above n 53, 1249-1251, 1286-1287.

[169] Stucke and Ezrachi, 'Digital Assistants', above n 53, 1251-1254.

[170] See Stucke and Ezrachi, 'Digital Assistants', above n 53, 1255-1266. See also Shelanski, above n 148, 1678-1682 (on customer data as an input of production, as a strategic asset which can help to entrench market power, and as a commodity which provides a valuable revenue stream).

[171] Stigler Center Digital Platforms Report, above n 6, 12-13, 60. See also Furman Report, above n 4, 59 (explaining the concept of platforms with "strategic market status" or enduring power over a strategic market bottleneck: "Platforms that achieve dominance can hold a high degree of power over how their users access the market, and each other. This dominance can result in harm to consumers directly, with clear evidence of issues relating to quality, such as with the ranking of search results, and data privacy."); Stucke and Ezrachi, 'Digital Assistants', above n 53, 1243 (raising the possibility that digital assistants' "critical gatekeeper position in a multi-sided market" might reduce consumer welfare, increase market power and limit competition).

attractions with advertising revenue gained by monetising consumers' personal information.[172] Consumers will not pay more to avoid a cost which cannot be assessed.[173] Privacy-enhancing rivals are therefore impeded in their ability to compete on privacy quality because the nature and extent of the detriment caused by their rivals' privacy-degrading practices is hidden.[174]

In the absence of this competitive pressure from rivals, dominant firms may impose exploitative privacy terms on consumers.[175] The data dynamics of online markets may in fact spur a "race to the bottom" in privacy quality as privacy-enhancing competition is not rewarded, while all suppliers are incentivised to degrade consumer data privacy in the interests of increased advertising revenue and other means of monetising consumer data.[176] The central problem is not that consumers fail to read privacy policies, but that concealed data practices currently prevent this from being an effective means of comparing the privacy quality offered by different suppliers.

[172] See Evans, 'Attention Platforms', above n 7, 20-21 (on suppliers' reduced ability to invest in the product in the absence of greater access to consumer data and therefore advertising revenue).

[173] Stigler Center Digital Platforms Report, above n 6, 21, 45 ("When facing a zero-money price, and when quality is difficult to observe, consumers are not receiving salient signals about the social value of their consumption because the price they believe they face does not reflect the economics of the transaction, and they are ignorant of those numbers.").

[174] See Shelanski, above n 148, 1690 (on the fact that data practices are not generally observable for consumers).

[175] Stigler Center Digital Platforms Report, above n 6, 21, emphasis in original ("Surmounting the existing barriers to entry created by consumer behavior, cost structure, public policy, and any past anticompetitive conduct is extremely difficult. This fact has direct effects on consumers: *without entry or the credible threat of entry, digital platforms need not work hard to serve consumers because they do not risk losing their consumers to a rival*.").

[176] See Stucke and Grunes, above n 45, 56; ACCC, 'Digital Platforms Inquiry: Preliminary Report' (December 2018) 217-218 (on decreased competition on privacy quality as rivals compete by adopting more invasive data practices); ACCC Digital Platforms Report, above n 3, 423-424; Shelanski, above n 148, 1690 (on the potential lack of incentives for "comparatively pro-consumer [privacy] policies"). See also Bruce Schneier, *Data and Goliath* (Norton, 2015) 242-243 (on the need for incentives to create new business models that do not depend on consumer surveillance).

"[A] few "gatekeeper" firms are in a position to control the tracking and linking of those behaviors across platforms, online services, and sites—for billions of users. As a result, chronicles of peoples' actions, desires, interests, and mere intentions are collected by third parties, often without individuals' knowledge or explicit consent, with a scope, breadth, and detail that are arguably without precedent in human history." Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54 *Journal of Economic Literature* 442, 444.

Increasing inequality of bargaining power and information asymmetries in other markets

Concealed data practices make consumers increasingly transparent while obscuring an increasingly opaque universe of suppliers.[177] In this way, concealed data practices also cause harm to the competitive process by undermining the vital role played by consumers, both in the initial market where the information is collected and in markets for *other* products (in dimensions other than privacy quality) where the personal information is subsequently used contrary to the reasonable expectations of the consumer. A consumer's personal information may be used by suppliers in a number of markets, who take advantage of these information asymmetries to focus on consumer manipulation[178] at the expense of competition on the merits.

Effective competition is competition which drives superior efficiency and innovation and is responsive to consumers. Effective competition depends on consumers having access to accurate information and the ability to bargain for, and switch to, a better deal. Concealed data practices substantially reduce consumers' bargaining power by increasing information asymmetries between suppliers and consumers in the bargaining process,[179] and allowing

[177] See further Acquisti, 'The Economics of Personal Data and Privacy', above n 7, 17.

[178] See the definition of "online manipulation" by Susser, Roessler and Nissenbaum, above n 123.

[179] Concealed data practices also impose immediate cost on consumers having regard to the time required to attempt to interpret vague and lengthy privacy terms and their consequences, and the difficulty and complexity of

suppliers to engage in manipulation-based marketing in a way traditional advertising does not permit.[180] This weakens the competitive process by reducing the likelihood that well informed, empowered consumers will select the most efficient suppliers; those that best meet the needs and wants of consumers in respect of the relevant product.

In short, where the collected information is used by suppliers against the consumer in subsequent transactions, the supplier may focus on aggregating personal information about the individual consumer and manipulating the individual purchasing environment in an effort to extract maximum consumer surplus and create obstacles to comparison and switching, rather than presenting the best value proposition to the consumer.[181]

"[T]he platform's detailed, personalized, minute-by-minute control over their interface … enables platforms to create a façade of competition, choice, and autonomy when in fact users are being directed with behavioral techniques." Stigler Center Digital Platforms Report, above n 6, 37.

5. The significance of concealed data practices for competition authorities

Concealed data practices therefore create objective costs and detriments for consumers, and undermine the competitive process, including by chilling privacy-enhancing competition. This weakening of competition may not amount to a contravention of antitrust legislation in itself. However, the effect of concealed data practices on the competitive process should be taken

exercising control over their privacy. See Gillian K Hadfield, Robert Howse and Michael J Trebilcock, 'Information-Based Principles for Rethinking Consumer Protection Policy' (1998) 21 *Journal of Consumer Policy* 131, 141, 144-146, 152; Acquisti, 'The Economics of Personal Data and Privacy', above n 7, 18.

[180] See Stigler Center Digital Platforms Report, above n 6, 22-23, 35-36.

[181] "A platform can analyze a user's data in real time to determine when she is in an emotional "hot state" and then offer targeted sales": Stigler Center Digital Platforms Report, above n 6, 7, 36-37. See also Susser, Roessler and Nissenbaum, above n 5.

into account by competition regulators in the following respects.

First, where concealed data practices are present, it should not be assumed that consumers have demonstrated a preference for the data privacy terms on which the relevant products are provided.[182] It is not appropriate to rely on "revealed preferences" about privacy terms where consumers have grossly inadequate information about the terms offered and their consequences, and often no real choice in privacy terms.[183]

A consumer's supposed acceptance of privacy terms in the presence of concealed data practices has several features which make it unlikely that this acceptance represents the consumer's true interests, or "normative preference". These features include the fact that the choice is passive (in the form of implied consent or default settings); the complexity of the decision and its effects; limited personal experience of the consequences of this choice (data practices and their consequences are generally not revealed); and third-party marketing of the choice in question (particularly where privacy policies are framed to manipulate consumers to accede to privacy intrusive practices).[184]

It is also inappropriate to discount expressed consumer preferences by reference to the "privacy paradox".[185] The difference between consumers' explicit concerns and their supposed acceptance of privacy-intrusive terms may be readily explained by the manipulative and/or coercive effects of concealed data practices, as well as their tendency to hinder privacy-enhancing competition.

---

[182] Cf Productivity Commission, Australian Government, 'Data Availability and Use' (Inquiry Report No 82, 31 March 2017) 91 (arguing in the case of "large social media providers", "large firms will tend to self-regulate … according to prevailing public attitudes").

[183] See Stigler Center Digital Platforms Report, above n 6, 45. Cf Manne and Sperry, above n 8, 5-6. See John Beshears, James J Choi, David Laibson and Brigitte C Madrian, 'How Are Preferences Revealed?' (2008) 92 *Journal of Public Economics* 1787 ("Economists usually assume that these revealed preferences are also *normative preferences* – preferences that represent the economic actor's true interests.").

[184] Beshears et al, above n 183, 1788-1789.

[185] See fn 136 above.

Second, diminished competition on privacy quality as a result of concealed data practices should be taken into account in any assessment of the state of competition, and market power,[186] in the relevant market. In markets where services are offered at zero monetary price, it is vital to consider other aspects of competition including innovation and the quality of services provided in any competition assessment.[187]

Commentators have argued in favour of competition authorities taking into account the benefits consumers gain from zero-priced services – the positive impacts of competition on innovation and quality.[188] Competition authorities should equally take into account the negative impacts on quality competition, which critically includes the quality of privacy terms offered and privacy-enhancing innovation.[189]

These detriments should not be overlooked on the basis that they cannot be precisely quantified in dollar terms.[190] "[T]he lack of explicit prices does not mean the harms are any less real."[191] In the context of markets with zero monetary prices, consumer benefits are not

[186] Stucke and Ezrachi, 'Digital Assistants', above n 53, 1294 ("Competition officials often adopt a price-centric approach to assess market power, namely whether the firm can charge supracompetitive prices. Rarely do they assess market power primarily in the form of non-price effects such as quality.").

[187] Furman Report, above n 4, 42-45; European Commission, 'Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions' (Press Release, 6 December 2016) <https://europa.eu/rapid/press-release_IP-16-4284_en.htm> ("Privacy related concerns … can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor."); Dissenting Statement of Commissioner Pamela Jones Harbour, In the Matter of Google / DoubleClick, FTC File No 071-0170.

[188] See, eg, Evans, 'Attention Platforms', above n 7.

[189] Stucke and Ezrachi, 'Digital Assistants', above n 53, 1284-1285, 1293 ("Interventions will have to balance the benefits which flow from advanced technology and artificial intelligence against the welfare risks …").

[190] See Pamela Jones Harbour and Tara Isa Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets' (2010) 76 *Antitrust Law Journal* 769, 792-793 (arguing that "[i]t would be entirely inappropriate to ignore consumers' concerns about privacy-based competition, simply because product market definition might prove difficult").

[191] Benjamin Edelman and Damien Geradin, 'An Introduction to the Competition Law and Economics of "Free"' (2018) *Competition Policy International Antitrust Chronicle* 1, 10.

generally quantifiable either.[192] But competition authorities should take both into account, and consider the proportionality of any plausible detriments against the plausible benefits.[193]

In this respect, competition authorities will need to further develop and become more familiar with analytical tools which can take account of impacts on quality, particularly where price is not the key indicator of the health of competition.[194]

Third, where there is limited competition on privacy quality in a market as a result of concealed data practices, a further restriction on privacy competition may more readily amount to a substantial lessening of competition (SLC).[195] Various provisions of Part IV of the *Competition and Consumer Act 2010* (Cth) may be infringed where conduct or an acquisition has the effect or likely effect of SLC.[196] Alleged contraventions of these provisions may be based on reduced competition on privacy quality. For example, if a dominant firm engages in conduct which excludes privacy-enhancing apps from its platform, this may give rise to a claim of misuse of market power under section 46(1).[197] Where a firm with market power acquires a new rival that has been innovating on privacy quality or a rival that offers superior privacy quality, there may be a claim that the merger results in SLC under section 50.[198]

---

[192] Cf Evans, 'Attention Platforms', above n 7 (arguing for an estimate of the value of content on attention platforms based on the opportunity costs of the time users spend in front of that ad-supported content).

[193] Cf Manne and Sperry, above n 8, 3, (arguing that "[a] non-price effects analysis involving product quality across multiple dimensions becomes exceedingly difficult if there is a tradeoff in consumer welfare between the dimensions. … Any such analysis would necessarily involve a complex and imprecise comparison of the relative magnitudes of harm/benefit to consumers who prefer one type of quality to another.").

[194] See 'Common Understanding of G7 Competition Authorities on "Competition and the Digital Economy"' (July 2019) 4; Stigler Center Digital Platforms Report, above n 6, 8, 45, 66-67. See also Furman Report, above n 4, 42-45. On the difficulty of assessing the counterfactual in such scenarios, see Stucke and Ezrachi, 'Digital Assistants', above n 53, 1296.

[195] See Harbour and Koslov, above n 190, 794-795 (arguing that, in unilateral conduct investigations, the competition authority should consider whether achieving a dominant market position might reduce the firm's incentives to compete on privacy dimensions or to innovate on new privacy-protective technologies).

[196] See, eg, *Competition and Consumer Act 2010* (Cth), ss 45(1), 46(1), 47(10), 50.

[197] See Stucke and Ezrachi, 'Digital Assistants', above n 53, 1256-1263 (on the gatekeeper role digital assistants perform in respect of upstream services). Or downgrading interoperability: Stucke and Ezrachi, 'Digital Assistants', above n 53, 1295.

[198] Mike Isaac, *Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger*, (New York Times, 25

The existence of concealed data practices on the part of firms with market power in these scenarios would indicate that there is already weakened competition on privacy quality. A further reduction in this privacy competition should be treated as more substantial in the presence of existing concealed data practices than the same conduct in a market where there is healthy competition on privacy quality.[199]

Fourth, investigations of conduct which is alleged to suppress privacy competition may have the beneficial side effect that the competition regulator acts essentially as an expert intermediary, interpreting the state of privacy competition for the benefit of consumers.

Ohlhausen and Okuliar have argued that antitrust laws and antitrust regulators are not well-adapted to addressing privacy concerns.[200] The points outlined above indicate several ways competition regulators can sensibly take account of privacy issues in competition law assessments. Further, Ben-Shahar and Schneider have explained that, where consumers have little prospect of interpreting specialist information, and particularly that which is revealed as a result of mandated disclosure, expert intermediaries may be necessary to interpret the

---

January 2019) <https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html>. See Robert H Lande, 'The Microsoft-Yahoo Merger: Yes, Privacy Is an Antitrust Concern', *FTC:Watch* (25 February 2008) 1 ("Antitrust is actually about consumer choice, and price is only one type of choice. The ultimate purpose of the antitrust laws is to help ensure that the free market will bring to consumers everything they want from competition. This starts with competitive prices, of course, but consumers also want an optimal level of variety, innovation, quality, and other forms of nonprice competition. Including privacy protection."). See further Argentesi et al, Lear, 'Ex-post Assessment of Merger Control Decisions in Digital Markets: Final Report' (Report by Lear for UK Competition and Markets Authority, 9 May 2019) (providing case reviews of UK merger decisions in digital markets and considering whether too much weight has been put on the risk of incorrect intervention compared to the risk of incorrect clearance).

[199] See further Crémer, De Montjoye and Schweitzer, above n 4, 51 ("[I]n the context of highly concentrated markets characterised by strong network effects and subsequently high barriers to entry (a setting where impediments to entry which will not be easily corrected by markets), one may want to err on the side of disallowing types of conduct that are potentially anti-competitive, and to impose the burden of proof for showing pro-competitiveness on the incumbent. This may be even more true where platforms display a tendency to expand their dominant positions in ever more neighbouring markets, growing into digital ecosystems which become ever more difficult for users to leave.").

[200] See Maureen K Ohlhausen and Alexander P Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015) 80 *Antitrust Law Journal* 121.

available information and empower consumers in their decision-making.[201]

In certain circumstances, competition regulators may act as one form of learned intermediary, where consumers are severely disadvantaged in their ability to interpret the quality of privacy terms and their consequences as a result of concealed data practices. Legitimate complaints under Part IV of the *Competition and Consumer Act*, for example, provide an opportunity for the ACCC to use its resources and information gathering powers to interpret the state of competition on privacy quality, improve transparency and intervene in the interests of competition where necessary.

Conclusion

Data-driven businesses are altering the frontiers of influence, by their ubiquity, scale and subtlety. In a world of digital assistants, pervasive social media, wearable devices and location-based marketing, this influence now stretches to our homes, our families, our bodies and our movements. Inevitably, increased surveillance and manipulation of consumers for commercial purposes raises issues for consumer protection and privacy regulation. The concealed data practices described in this paper also cause objective detriment to consumers and undermine the competitive process on privacy quality and beyond. Competition authorities should have regard to these concealed data practices in rejecting claims of "revealed preferences"; assessing the quality of competition on privacy, in zero-priced digital markets in particular; and assessing the significance of any lessening of competition by the exclusion or absorption of privacy-enhancing rivals. These considerations fall squarely within the established objectives of competition law, in protecting the competitive process in the interests of consumer welfare.

[201] Omri Ben-Shahar and Carl E Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press) 3-5, 185-190. See also Gillian K Hadfield, Robert Howse and Michael J Trebilcock, 'Information-Based Principles for Rethinking Consumer Protection Policy' (1998) 21 *Journal of Consumer Policy*, 131, 159.