European Competition Journal

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/recj20

Concealed data practices and competition law: why privacy matters

Katharine Kemp

To cite this article: Katharine Kemp (2020) Concealed data practices and competition law: why privacy matters, European Competition Journal, 16:2-3, 628-672, DOI: 10.1080/17441056.2020.1839228

To link to this article: https://doi.org/10.1080/17441056.2020.1839228

Published online: 05 Nov 2020.

EUROPEAN COMPETITION JOURNAL
2020, VOL. 16, NOS. 2–3, 628–672
https://doi.org/10.1080/17441056.2020.1839228

Routledge
Taylor & Francis Group

Concealed data practices and competition law: why privacy matters

Katharine Kemp[a,b]*

[a]Academic Lead, UNSW Grand Challenge on Trust, Sydney, Australia; [b]Senior Lecturer, Faculty of Law, UNSW Sydney, Sydney, Australia

ABSTRACT

The degradation of consumer data privacy in the digital environment causes objective detriment to consumers and undermines the competitive process. Consumers are frequently unaware of the extent to which their personal data is collected and disclosed, and purposes for which it is used. A key reason is that firms often understate and obscure their actual data practices, preventing consumers from making informed choices. This article defines, and provides examples of, "concealed data practices", which create objective costs and detriments for consumers, making them more susceptible to criminal activity, discrimination, exclusion, manipulation and humiliation. Aside from consumer protection and privacy regulatory responses, these practices should be of critical concern to competition authorities given their role in chilling privacy competition; preserving substantial market power by means other than superior efficiency; and deepening information asymmetries and imbalances in bargaining power. The article outlines five ways competition authorities should take account of these factors.

ARTICLE HISTORY Received 15 October 2020; Accepted 16 October 2020

KEYWORDS Data privacy; competition law; digital platforms; multisided markets; abuse of dominance

I. 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

CONTACT Katharine Kemp k.kemp@unsw.edu.au Faculty of Law, UNSW Sydney, Kensington, NSW 2052, Australia

*Academic Lead, UNSW Grand Challenge on Trust; Senior Lecturer, Faculty of Law, UNSW Sydney. I am grateful to Graham Greenleaf, David Howarth, Megan Richardson, Philip Marsden and Katherine Strandburg for helpful comments on earlier drafts, and to Roseanna Bricknell for research assistance; with the usual disclaimers.

regulation should apply. The United States Federal Trade Commission last year 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 not misled.[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 regulators should also take account of privacy concerns under competition law.[4] This article 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 to competition authorities.

There are larger issues at stake in the broader debate about increasing digital surveillance and corporate data practices.[5] These issues ultimately

[1]Federal Trade Commission, 'FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making' (24 July 2019) <www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history> accessed 16 October 2020. See also Office of the Australian Information Commissioner, Australian Government, 'Commissioner Launches Federal Court Action Against Facebook' (9 March 2020) <www.oaic.gov.au/updates/news-and-media/commissioner-launches-federal-court-action-against-facebook> accessed 16 October 2020.

[2]Facebook Inc i.a. – The Use of Abusive Business Terms pursuant to Section 19(1) GWB (B6-22/16, Bundeskartellamt, Administrative Proceedings, 6 February 2019); Bundeskartellamt, Germany, 'Bundeskartellamt prohibits Facebook from combining user data from different sources: Background information on the Bundeskartellamt's Facebook proceeding' (7 February 2019). The Federal Court of Justice annulled the decision of the Düsseldorf Higher Regional Court which had suspended the effect of the Bundeskartellamt's order: 'Federal Court of Justice provisionally confirms allegation of Facebook abusing dominant position' (Courtesy Translation of Press Release No 080/2020, published by the German Federal Court of Justice, 23 June 2020).

[3]See, eg, Government of Canada, 'Strengthening Privacy for the Digital Age' (Discussion Paper, 2019); House of Lords Select Committee on Communications, 'Regulating in a Digital World' (2nd Report of Session 2017–19, March 2019); Australian Competition & Consumer Commission, 'Digital Platforms Inquiry: Final Report' (2019) (hereinafter *ACCC Digital Platforms Report*); Stigler Center for the Study of the Economy & the State & The University of Chicago Booth School of Business, 'Stigler Committee on Digital Platforms: Final Report' (2019) (hereinafter *Stigler Center Digital Platforms Report*); Competition & Markets Authority, United Kingdom, 'Online Platforms and Digital Advertising: Market Study Final Report' (2020) (hereinafter *UK CMA Online Platforms Report*). 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' (2019); Digital Competition Expert Panel, United Kingdom, 'Unlocking Digital Competition' (March 2019) (hereinafter *Furman Report*); Philip Marsden and Rupprecht Podszun, 'Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement' (Konrad Adenauer Stiftung 2020). See also 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* (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,

go to the very nature of the society we live in and our fundamental human rights in that society. This article 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, with growing proposals for how consumers might gain a greater share in the benefits of data.[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, including online search, social networks, fast and convenient connections with relevant products, news and entertainment, real-time information on healthier lifestyle choices, and, more recently, disease tracking.[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

Autonomy and Manipulation' (2019) 8 Internet Policy Review 1; Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press 2016); Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (2020) 173–177 (hereinafter *Norwegian Consumer Council, 'Out of Control'*).

[6]See Phuong Nguyen and Lauren Solomon, Consumer Policy Research Centre, 'Consumer Data and the Digital Economy: Emerging Issues in Data Collection, Use and Sharing Report' (2018) 20–21 (hereinafter *CPRC Emerging Issues Report*); Stigler Center Digital Platforms Report (n 3) 29, 34–37, 48; European Commission, Communication 'Shaping Europe's digital future', COM(2020) 67 final, 2.

[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 1129, 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' (Working Paper, January 2019) 3, 21–24; Alessandro Acquisti, 'The Economics of Personal Data and the Economics of Privacy' (OECD 2010) 8–11; Anindya Ghose and D Daniel Sokol, 'Unlocking Platform Technology to Combat Health Pandemics' (2020) Yale Journal on Regulation (arguing for the extensive use of commercially acquired personal data to trace contacts during the pandemic). See also Part III.B(1) *infra* on the impacts of disease tracking data practices during the COVID-19 pandemic.

[8]Torsten Körber, 'Is Knowledge (Market) Power? On the Relationship between Data Protection, "Data Power" and Competition Law' (2016) 9–10, 18 <https://ssrn.com/abstract=3112232> accessed 16 October 2020; 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 also Sokol and Comerford (n 7) 1144–1145; Maureen K Ohlhausen and Alexander P Okuliar, 'Competition,

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, data protection and privacy regulation, to the extent that 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]

Consumer Protection, and the Right [Approach] to Privacy' (2015) 80 Antitrust Law Journal 121, 154 ("perhaps the most important point is that attempting to distort the antitrust laws to pursue subjective noncompetition harms is *unnecessary* and would take us back to a less sophisticated approach to law enforcement").

[9]Manne and Sperry (n 8) 5–6. See also Justus Haucap, 'Data Protection and Antitrust: New Types of Abuse Cases? An Economist's View in Light of the German *Facebook* Decision' (February 2019) CPI Antitrust Chronicle 5 (arguing that "empirical evidence suggests that (many) people do not feel exploited when their data is used. Quite in contrast, a fair number of people tends to willingly share data in order to obtain benefits such as improved services."); Bobbie Johnson, 'Privacy No Longer a Social Norm, Says Facebook Founder' *The Guardian* (11 January 2010). *Cf* Dina Srinivasan, 'The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy' (2019) 16 Berkeley Business Law Journal 39, 74–81 (on Facebook's circumvention of individuals' attempts to evade surveillance by deleting cookies, resetting identifiers or "Do Not Track" registration).

[10]See Manne and Sperry (n 8) 3–4. See also 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; Körber (n 8) 10, 16–18.

[11]Measured in terms of price and output levels of the relevant product. See Sokol and Comerford (n 7) 1145, 1156-1158; Ohlhausen and Okuliar (n 8) 152–154.

[12]See Manne and Sperry (n 8); Sokol and Comerford (n 7) 1156–1161; Haucap (n 9) 3–4; Ohlhausen and Okuliar, (n 8) 152–154. See also 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 HSE Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in an Era of Big Data' (Working Paper, June 2019) 9–11; Maurice E Stucke, 'Should We Be Concerned About Data-Opolies?' (2018) 2 Georgetown Law Technology Review 275, 294–295. 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 Organisation for Economic Co-operation and Development (OECD), 'Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value' (Economics Paper, 2013) 6, 34 (on proposals for "data lockers"); Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The

This article 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 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 article, 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"

Economics of Privacy' (2016) 54 Journal of Economic Literature 442, 447–448 (on attempts to value, and permit consumers to trade in, personal information); Nicholas Economides and Ioannis Lianos, 'Restrictions on Privacy and Exploitation in the Digital Economy: A Competition Law Perspective' (NET Institute Working Paper No 19–15, October 2019) 14, 72 (on "collective action to restore the conditions of a well-functioning data market" where "the purchaser of personal information is forced to offer … the full value of the personal information to the company"); Aline Blankertz, 'Designing Data Trusts: Why We Need to Test Consumer Data Trusts Now' (Stiftung Neue Verantwortung Report, February 2020). Compare 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*); Lina M Khan and David E Pozen, 'A Skeptical View of Information Fiduciaries' (2019) 133 Harvard L Rev 497, 519–520 (on consumers' inability to comprehend even the "basic contours" of the supposed bargain with digital platforms).

[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', (n 7) 4 (explaining arguments as to why privacy is a source of economic inefficiencies).

[16]See Michal S Gal and Daniel L Rubinfeld, 'The Hidden Costs of Free Goods: Implications for Antitrust Enforcement' (2016) 80 Antitrust Law Journal 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").

[17]See Part IV.B(4)-(5) *infra*. See also 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' (n 7) 19–20.

[18]See Part III *infra*.

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

This article proceeds as follows. Part II provides an explanation of the roles of notice and consent in data protection and privacy regulation and the challenges to these concepts in the digital era. Part III 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 IV considers the two main responses by competition law 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 V sets out five ways in which these factors should be taken into account by competition authorities.

[19] See Anita Allen, *Unpopular Privacy: What Must We Hide?* (OUP 2011) Chap 7. See also 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] Allen (n 19) 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> accessed 16 October 2020.

[22] Personal correspondence with Graham Greenleaf, on file with the author. See Moore (n 21) 1–2 (drawing comparisons with slavery).

[23] See, eg, Megan Richardson, *The Right to Privacy: Origins and Influence of a Nineteenth-Century Idea* (CUP 2017) (on whether there is a right to privacy in Australia).

II. 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 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, regulation is to a substantial degree based on the concepts of notice and consent; in the United States, commonly "notice and choice".[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. In the United States and numerous other jurisdictions,

[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; Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press 2010) chap 4.

[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 E 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* (OUP 2014) 5. In Europe, the term "data protection law" tends to be used to describe a range of rights, 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* (OUP 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 & Entertainment Law Journal 181, 195–198; Solove, 'Privacy Self-Management' (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 (hereinafter 'Privacy Commissioner of Canada Consent and Privacy Report'); Working Party on Security and Privacy in Digital Economy, OECD, 'Summary of the OECD Privacy Expert Roundtable: Protecting Privacy in a Data-Driven Economy: Taking Stock of Current Thinking' (Report DSTI/ICCP/REG(2014)3, 21 March 2014) 14–15 (noting the EU's departure from the 'notice and choice' model); World Economic Forum, 'Redesigning Data Privacy: Reimagining Notice & Consent for Human-Technology Interaction' (White Paper, July 2020) 10–11.

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] 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 the EU, concepts of notice and consent also play a role, albeit in the context of other data protection obligations which exist regardless of any agreement with the data subject, in view of the individual's fundamental rights to data protection. While "consent" is only one of six legal grounds for data processing under the General Data Protection Regulation (GDPR), and restricted by the higher standards for consent established by the relevant regulations, it remains a key aspect of justifying data processing or intrusions upon an individual's privacy under both the GDPR and the ePrivacy Directive, and a justification data processors frequently rely upon in practice.[30] As the World Economic Forum recently noted, "[d]espite two decidedly different trajectories, Notice & Consent has clearly become part of both the EU and US data protection and privacy landscapes."[31]

The "notice and choice" approach to privacy regulation in a number of other countries 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

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

[30]See, eg, Privacy and Electronic Communications Directive 2002/58/EC (ePrivacy Directive), Art 5.1, 6.3, 9.1; Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal 115, 139–143.

[31]World Economic Forum (n 28) 10; Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal 115, 121.

[32]See, eg, Privacy Act 1988 (Australia), ss 6, 15, sched 1 (Australian Privacy Principle 1). 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 (referring to "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 2016) 5.

[33]See Solove, 'Privacy Self-Management' (n 15) 1889, 1895–1896; Privacy Commissioner of Canada Consent and Privacy Report, (n 28) 2; Nissenbaum, (n 25) 81–82 (2010) (explaining that, on one view, "privacy is to be understood as a form of autonomy: specifically, it is self-determination with respect to information about oneself").

privacy destiny. The approach has therefore been described as "privacy self-management".[34]

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 data 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 traditional markets, technology and the

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

[35]See, eg, Finn Brunton and Helen Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest* (2015) 45–54; Julie Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press, 2012); Hull (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 (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' (February 2012); World Economic Forum, 'Redesigning Data Privacy: Reimagining Notice & Consent for human-technology interaction' (White Paper, July 2020).

[37]See Solove, 'Privacy Self-Management' (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 (n 28) 6.

[38]See Bruce Schneier, *Data and Goliath* (Norton 2015) 92–103; Wolfie Christl and Sarah Spiekermann, 'Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy' (2016).

[39]See, eg, Productivity Commission, Australian Government, 'Data Availability and Use' (Inquiry Report No 82, 31 March 2017); Department of Prime Minister & Cabinet, Commonwealth of Australia, 'New Australian Government Data Sharing and Release Legislation' (Issues Paper for Consultation, 4 July 2018); Ghose and Sokol (n 7) (arguing for the extensive use of commercially acquired personal data to trace contacts during the pandemic).

[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; Norwegian Consumer Council, 'Out of Control' (n 5) 5–6; Natasha Singer and Choe Sang-Hun, 'As Coronavirus Surveillance Escalates, Personal Privacy Plummets' *New York Times* (New York, 23 March 2020).

use of data determine commercial success in digital markets. Suppliers have been enjoined to "measure everything" in the interests of customer profiling, targeted marketing, customization, 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 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 realized potential mental illness could be added to a permanent profile attached to our identity.

[41] See also Acquisti, 'The Economics of Personal Data and Privacy' (n 7) 8; Wolfie Christl, 'Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions' (2017) 25 (hereinafter Christl, 'Corporate Surveillance').

[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]; Viktor Mayer-Schönberger and Thomas Ramge, 'Reinventing Capitalism in the Age of Big Data' (2018) 77–78, 84–85.

[43] See Zuboff (n 5). See also Susser, Roessler and Nissenbaum (n 5); Srinivasan (n 9).

[44] Stigler Center Digital Platforms Report (n 3) 36–37, 47–48 (on increasing returns to scale of data collection). Cf. Acquisti, 'The Economics of Personal Data and Privacy' (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' (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] For example, 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' (Consumer Policy Research Centre, 2019) 6 (hereinafter 'CPRC Day in the Life of Data Report'); CPRC Emerging Issues Report (n 6) 11–12; ACCC Digital Platforms Report (n 3) 388–389. See also Privacy Commissioner of Canada Consent and Privacy Report (n 28) 8 (on the internet of things).

[47] See Whittington and Hoofnagle, 'Unpacking Privacy's Price' (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 Educational Research Journal 1, 5–11.

III. Concealed data practices and consequent detriment to consumers

A. Concealed data practices and privacy terms

"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]See Srinivasan (n 9) 41 (eg, Facebook has even collected "the text users type, but then delete, into status updates, timeline posts, and comments, before hitting an enter button"). 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 (n 7) 1133–34; Körber (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' (n 14) 625.

[49]See Privacy Commissioner of Canada Consent and Privacy Report (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, 'Data Brokers: A Call for Transparency and Accountability Report' (2014); Office of the Australian Information Commissioner, Australian Government, 'Commissioner Launches Federal Court Action Against Facebook' (9 March 2020) <https://www.oaic.gov.au/updates/news-and-media/commissioner-launches-federal-court-action-against-facebook>; Norwegian Consumer Council, 'Out of Control' (n 5). See also United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age Report' (30 June 2014).

[50]See, eg, UK CMA Online Platforms Report (n 3) 177–181; ACCC Digital Platforms Report (n 3) chap 7; Crémer, De Montjoye & Schweitzer (n 4); Autorité de la Concurrence and Bundeskartellamt, 'Competition Law and Data' (10 May 2016) 25–28.

[51]Hoofnagle and Whittington, 'Free: Accounting for the Costs' (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, and adept at structuring the deal so that more financially valuable assets are procured from consumers than consumers would prefer."); World Economic Forum, "Redesigning Data Privacy: Reimagining Notice & Consent for human-technology interaction" (White Paper, July 2020).

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 Australian consumers believe the existence of a privacy policy means suppliers will not share their personal information with anyone else, and consumer surveys in

[52]See Margaret Jane Radin, 'Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law' (2014) 13–16; Hull (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).

[53]See ACCC Digital Platforms Report (n 3) 455; Hull (n 32) 94; Maurice E Stucke and Ariel Ezrachi, 'How Digital Assistants Can Harm Our Economy, Privacy, and Democracy' (2017) 32 Berkeley Technology Law Journal 1239, 1286; Christl, 'Corporate Surveillance' (n 41) 5; Srinivasan (n 9) 45, 49–54. See also Samson Y Esayas, 'Competition in (Data) Privacy: "Zero"-Price Markets, Market Power, and the Role of Competition Law' (2018) 8 International Data Privacy Law 181, 195–196 (pointing out that the significance of the subsequent amendment of privacy terms may in itself be obscured by the supplier, citing the example of changes to WhatsApp Privacy Policy following Facebook's acquisition of WhatsApp); ACCC, 'ACCC Alleges Google Misled Consumers About Expanded Use of Personal Data' (Media Release, 27 July 2020) (on Google's amendment of its privacy terms to remove its promise not to combine DoubleClick and Google datasets without active opt-in consent). *Cf* Productivity Commission, Australian Government, 'Data Availability and Use' (Inquiry Report No 8, 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' (n 13) 1363–1365; ACCC Digital Platforms Report, (n 3) 397, 603.

[55]See ACCC Digital Platforms Report (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' (n 15) 1886 ("people operate under woefully incorrect assumptions about how their privacy is protected"); Privacy Commissioner of Canada Consent & Privacy Report (n 28) 9; Whittington and Hoofnagle, 'Unpacking Privacy's Price' (n 13) 1355–1357; UK CMA Online Platforms Report (n 3) 166–172.

the US have produced similar results.[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 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

[57]ACCC, 'Digital Platforms Inquiry: Preliminary Report' (December 2018) 174. See also CPRC Emerging Issues Report (n 6) 29 (revealing almost one in five Australian consumers held this belief, and a further 22% of Australian consumers "did not know enough to answer this question"). See also Chris Jay Hoofnagle and Jennifer King, 'What Californians Understand About Online Privacy' (2008) 2 <http://ssrn.com/abstract=1262130> accessed 16 October 2020 (the 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 displaying a 'privacy policy' means the site will not share information with other websites and companies).

[58]CPRC Emerging Issues Report (n 6) 59.

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

[60]See, eg, CPRC Emerging Issues Report (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 (n 32) 91.

[61]See, eg, Norwegian Consumer Council, 'Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy' (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 (25 April 2019); ACCC Digital Platforms Report (n 3) 399–434; Lindh and Nolin (n 47) 6–11; Norwegian Consumer Council, 'Out of Control' (n 5) chap 5.

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

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

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 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]

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.[71] By contrast, online

[64] See France CNIL, 'The CNIL's restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC' (21 January 2019) (explaining the "generic and vague" descriptions of Google's "massive and intrusive" operations); Norwegian Consumer Council, 'Out of Control' (n 5) 63 (citing the example of the privacy terms for the "Perfect 365" app); ACCC Digital Platforms Report (n 3) 405; Solove, Privacy Self-Management (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' *New York Times* (New York, 10 December 2018).

[65] ACCC Digital Platforms Report (n 3) 418–421; CPRC Day in the Life of Data Report (n 46) 31; Solove, 'Privacy Self-Management', (n 15) 1889 ("there are also scores of entities that traffic in personal data without people ever being aware"); Norwegian Consumer Council, 'Out of Control' (n 5) 142–143. See also Privacy Commissioner of New Zealand, 'International Study Finds Privacy Shortfalls in Internet of Things Devices' (28 September 2016) <https://privacy.org.nz/news-and-publications/statements-media-releases/international-study-finds-privacy-shortfalls-in-internet-of-things-devices/> accessed 16 October 2020.

[66] Lindh and Nolin (n 47) 7.

[67] Whittington and Hoofnagle, 'Unpacking Privacy's Price' (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 (n 46) 21, 25.

[69] See Norwegian Consumer Council, 'Every Step You Take: How Deceptive Design Lets Google Track Users 24/7' (2018); Gillian K Hadfield, Robert Howse and Michael J Trebilcock, 'Information-Based Principles for 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 Norwegian Consumer Council, 'Deceived by Design' (n 61).

[71] See <https://twitter.com/Katharine_Kemp/status/1155965727012057089> accessed 16 October 2020.

suppliers regularly take advantage of a social atmosphere to benefit from the human desire to disclose information to forge social connections.[72] The disclosure of our personal information to complete strangers who will use it for commercial purposes is not salient in these settings.[73] Where a supplier does provide consumers with any means of protecting their privacy, the relevant processes frequently require action by the consumer (less privacy is the default),[74] and introduce unnecessary complexity (and outright obstruction) where the consumer attempts to limit or opt out of the disclosure of information.[75]

To be clear, the issue is not just the presentation of the terms themselves but the lack of transparency about current and future data practices and consumers' inability to understand the consequences of these practices.[76] 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.[77] 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).[78] 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

[72]See Solove, 'Privacy Self-Management' (n 15) 1895 ("many websites are designed to encourage exposure while minimizing awareness of the risks").

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

[74]Norwegian Consumer Council, 'Deceived by Design' (n 61) 13–15; Norwegian Consumer Council, 'Out of Control' (n 5) 69. 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* (New York, 26 December 2007).

[75]See Norwegian Consumer Council, 'Out of Control' (n 5) 105, 128, 134 (on privacy policies which provide that even if the individual opts out of location data collection, location will be inferred by other means, eg, from Internet Protocol (IP) addresses and other data); Srinivasan (n 9) 74–81 (on Facebook's circumvention of individuals' attempts to evade surveillance by deleting cookies, resetting identifiers or "Do Not Track" registration); ACCC 'Digital Platforms Report' (n 3) 424–434; Norwegian Consumer Council, 'Deceived by Design' (n 61) 19; CPRC Day in the Life of Data Report (n 46) 25. See further Ryan Nakashima, 'Google Tracks Your Movements, Like it or Not' *A.P. 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) <https://www.businessinsider.com.au/amazon-has-a-new-feature-to-delete-alexa-recordings-2019-5> accessed 16 October 2020.

[76]Hull (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"); Norwegian Consumer Council, 'Out of Control' (n 5) 49–50 (on "purpose creep"); Whittington and Hoofnagle, 'Unpacking Privacy's Price' (n 13) 1359–1360.

[77]*Contra* Manne and Sperry (n 8) 3.

[78]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* (2004) 165–178.

diligent and concerned.[79] How can we compare future costs to present benefits when we are plainly prevented from understanding the future costs?[80]

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,[81] and/or place the consumer within consumer segments, which can negatively affect the future opportunities of the consumer;
- track the consumer's physical location (including location indoors), and proximity to others, beyond that which is required for the provision of the service;[82]
- 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;[83]
- use the personal information for purposes not reasonably within the expectation of consumers;[84]
- disclose the personal information to other entities not reasonably within the expectation of consumers;[85]

[79] See Privacy Commissioner of Canada Consent & Privacy Report (n 28) 9; Norwegian Consumer Council, 'Out of Control' (n 5) 11 ("The extent of tracking and complexity of the adtech industry is incomprehensible to consumers, meaning that individuals cannot make informed choices about how their personal data is collected, shared and used"); Khan and Pozen (n 14) 519–520.

[80] See Hull (n 32) 93 ("[U]sers 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' (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. See further Khan and Pozen (n 14) 510–515 (on behavioural advertising).

[81] CPRC Day in the Life of Data Report (n 46) 7–8, 29.

[82] Norwegian Consumer Council, 'Out of Control' (n 5) 67 (citing the example of an "ovulation calculator and period tracker" app which collects location data supposedly "to show you important information about your cycle at the right time and place"); at 96 (on location indoors, including the floor of the building).

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

[84] See ACCC Digital Platforms Report (n3) 399–400, 414–422; Norwegian Consumer Council, 'Out of Control' (n 5) 49–50 (citing the example of the Indian fintech company using data collected from mobile music apps to help lenders decide whether to approve loan applications; and political data company, Data Propria, which states that "each voter's smartphone is the ultimate voter file").

[85] Hull (n 32) 91; Norwegian Consumer Council, 'Out of Control' (n 5) 159 (referring to the adtech services provider, Smaato, which states in its privacy policy that it will share data with "Demand Partners and TCF Vendors" and lists more than 1,000 companies as partners).

- 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;[86] and
- exclude or severely limit the liability of suppliers for unauthorized use or disclosure of the consumer's personal information.[87]

Revelations about some of the actual data practices of suppliers generally come only from sporadic media reports following major data breaches.[88] 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.[89] Resignation and despair are evident, with consumers expressing the sense that constant data collection is inescapable.[90]

Regardless of an individual consumer's subjective attitude to privacy and suppliers' data practices, these concealed data practices create objective costs for consumers. The following part describes three categories of objective costs which privacy-degrading data practices impose on consumers.

B. Objective consumer detriments from concealed data practices and degraded data privacy

1. Increased 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

[86]CPRC Day in the Life of Data Report (n 46) 8–11; Katharine Kemp, 'Submission in Response to the Australian Competition & Consumer Commission Ad Tech Inquiry Issues Paper' (26 April 2020) 22–26.
[87]See Hoofnagle and Whittington, 'Free: Accounting for the Costs' (n 14) 625.
[88]Leslie K John, 'Uninformed Consent' *The Big Idea: Harvard Business Review* (2018).
[89]Acquisti, 'The Economics of Personal Data and Privacy' (n 7) 13.
[90]CPRC Day in the Life of Data Report (n 46) 21; CPRC Emerging Issues Report (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' (Annenberg School for Communication, University of Pennsylvania, June 2015) <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 also Stucke and Ezrachi, 'Digital Assistants' (n 53) 1292–1293; 'Fuel of the Future: Data is Giving Rise to a New Economy' *The Economist* (6 May 2017) (on consumers "showing symptoms of what is called 'learned helplessness'").

more likely it will be hacked, accidentally disclosed or used for illegal purposes.[91] This is not simply a question of the quality of the supplier's data security systems. Data security experts acknowledge that even highly secure systems are almost certain to be breached at some stage.[92] Absent a hack, data may be improperly accessed (including by the supplier's own employees or contractors),[93] exposed or used due to technical glitches or operator error.[94] 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,[95] or data brokers, aggregators or associates, who are not contractually obliged to protect the consumer's information.[96] 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 to improper access and re-identification.

This has been amply demonstrated in the course of the COVID-19 pandemic, during which the revelation of purportedly anonymous details of patients infected with the coronavirus led to the vilification of individuals as a result of predictable, unsafe exposure of their data. For example, South Korean authorities published supposedly anonymous "detailed location histories on each person who tested positive [to COVID-19] … such as details about when people left for work, whether they wore masks in the subway, the name of the stations

[91] 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) <www.bbc.com/news/technology-47812470> accessed 16 October 2020; Lily Newman, 'A New Google+ Blunder Exposed Data From 52.5 Million Users' *Wired* (12 October 2018) <www.wired.com/story/google-plus-bug-52-million-users-data-exposed/> accessed 16 October 2020; Lily Hay Newman, '1.2 Billion Records Exposed Online in a Single Server' *Wired* (22 November 2019).

[92] 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> accessed 16 October 2020.

[93] 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); Dan Oakes, 'Federal Court Data Breach Sees Names of Protection Visa Applicants Made Public' *ABC online* (31 March 2020) <www.abc.net.au/news/2020-03-31/federal-court-in-protection-visa-data-breach-published-names/12102536> accessed 16 October 2020.

[94] Hoofnagle and Whittington, 'Free: Accounting for the Costs' (n 14) 644–48; Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 University of Pennsylvania L. Rev. 477, 515.

[95] Whittington and Hoofnagle, 'Unpacking Privacy's Price' (n 13) 1363–1364.

[96] See Hoofnagle and Whittington, 'Free: Accounting for the Costs' (n 14) 628, 633; CPRC Day in the Life of Data Report (n 46) 8–11; Azeen Ghorayshi and Sri Ray, 'Grindr is Letting Other Companies See User HIV Status and Location Data' *BuzzFeed* (2 April 2018); Norwegian Consumer Council, 'Out of Control' (n 5) 108–110 (citing the example of online dating app, OkCupid, sending "exceedingly personal details about individuals" to data analytics company Braze, including "sexual desires, drug and alcohol use, political views").

where they changed trains, the massage parlours and karaoke bars they frequented and the names of the clinics where they were tested for the virus" with the result that "internet mobs exploited patient data … to identify people by name and hound them".[97] Similarly, in New York, Mayor Bill de Blasio broadcast sufficient details about the second person in the state to test positive that a newspaper was able to refer to him by name several hours later.[98]

Identity theft is another key risk created by increased collection and disclosure of personal information.[99] 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, some victims may spend years attempting to clear their name of debt, bankruptcy and criminal activity, suffering repeated losses to their quality of life, reputation, finances, time and health.[100] This difficulty becomes extreme in 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.[101]

The increased exposure of personal information to attack or improper exposure should be recognized as a detriment to the individual even before harm of this kind crystallises. Increased vulnerability to serious harm is detriment in itself. The law recognizes, 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

[97]Natasha Singer and Choe Sang-Hun, 'As Coronavirus Surveillance Escalates, Personal Privacy Plummets' *New York Times* (New York, 23 March 2020).

[98]Ibid.

[99]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' (n 7) 15–17. P Jorna and RG Smith, 'National Identity Security Strategy: Identity Crime and Misuse in Australia 2017' (A.I.C. Statistical Report, 2019) 36 (explaining that, in 2016, 11% of Australians had been the victim of identity theft).

[100]See P Jorna and RG Smith (n 99) (reporting that impacts on victims of identity fraud include refusal of credit, refusal of 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); Katelyn Golladay and Kristy Holtfreter, 'The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes' (2017) 12 Victims & Offenders 741; Helen Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life (2010) 78.

[101]Citron (n 99) 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."); Matthew B Kugler, 'From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms' (2019) 10 UC Irvine Law Rev. 107, 132.

disorder is actually contracted.[102] So too privacy-degrading data practices which increase a consumer's vulnerability to hacking and other unauthorized data access are detrimental to the consumer.[103]

Data breaches may be an inescapable fact of twenty-first century existence. This does not mean that consumers should resign themselves to the harm. In well-functioning markets, 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.

2. Disclosure of personal information the consumer does not wish to disclose

Modern data practices allow suppliers to place the consumer under the microscope,[104] 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,[105] and inferences about, the consumer's characteristics, behaviour; health and tendencies.[106] 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".[107]

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

[103]Ibid.

[104]Stigler Center Digital Platforms Report (n 3) 30 ("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").

[105]For example, 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' (n 13) 1361–1362. See Norwegian Consumer Council, 'Out of Control' (n 5) 160–62 (explaining "ID syncing" which allows companies to combine data about an individual's activities across different devices).

[106]CPRC Emerging Issues Report (n 6) 11–12, 60; CPRC Day in the Life of Data Report (n 46) 29–30. See also Hoofnagle and Whittington, 'Free: Accounting for the Costs' (n 14) 636–37; Norwegian Consumer Council, 'Out of Control' (n 5) 12–13, 123 (citing the example that revealing that a consumer uses the Grindr dating app "is in itself a strong indicator of sexual preferences, as the app is geared towards homosexual, bisexual, and trans people").

[107]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* (29 May 2018). See also Citron (n 99) 253–255 (on the potential for retina scans and fingerprints to reveal diseases and genetic disorders).

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 information.[108] 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.[109] 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.[110] This personal information can be used to make inferences about consumers' intimate characteristics,[111] and profile and sort consumers, particularly to compile lists of consumers for sale to other suppliers and data brokers.[112]

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.[113] This unanticipated collection and

[108]CPRC Emerging Issues Report (n 6) 13–15; Hoofnagle and Whittington, 'Free: Accounting for the Costs' (n 14) 637–639; Solove, 'Privacy Self-Management' (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, at 25 (14 August 2017) ("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").

[109]Solove, 'Privacy Self-Management' (n 15) 1889 ("there are also scores of entities that traffic in personal data without people ever being aware").

[110]Federal Trade Commission, 'Data Brokers' (n 49); CPRC Day in the Life of Data Report (n 46) 8–11; Hoofnagle and Whittington, 'Free: Accounting for the Costs' (n 14) 633; Acquisti, 'The Economics of Personal Data and Privacy' (n 7) 8.

[111]See Citron (n 99) 253–255 (on the potential use of biometrics to reveal diseases and genetic disorders).

[112]Ibid. See also Privacy Commissioner of Canada Consent & Privacy Report (n 28) 6–7. *See also* Part III.B (3) *infra*.

[113]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 & Privacy Report (n 28) 15–16 (risk of re-identification increases over time); Crémer, De Montjoye and Schweitzer (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]; Chris Culnane and Kobi Leins, 'Misconceptions in Privacy Protection and Regulation' (2019) 36 Law in Context 49; Yves-Alexandre de Montjoye, Cesar A Hidalgo, Michel Verleysen and Vincent D Blondel, 'Unique in the Crowd: The Privacy Bounds of Human Mobility' <www.nature.com/articles/srep01376> accessed 16 October 2020.

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.[114]

3. 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.[115] In its 2014 investigation into the data broker industry, the 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".[116] 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".[117] 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".[118]

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 basis of their online and offline behaviour.[119] This information can be

[114]See CPRC Emerging Issues Report (n 6) 23–24, 32–33; Hull (n 32) 92; CPRC Day in the Life of Data Report (n 46) 15, 36. See further Acquisti, Taylor and Wagman (n 14) 444:

> [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.

[115]Hoofnagle and Whittington, 'Free: Accounting for the Costs' (n 14) 633–634; Norwegian Consumer Council, 'Out of Control' (n 5) 5–6; Federal Trade Commission, 'Data Brokers' (n 49) iv.

[116]Federal Trade Commission, 'Data Brokers' (n 49) 47.

[117]ACCC Digital Platforms Report, *supra* note 3, 446. See also Norwegian Consumer Council, 'Out of Control' (n 5) 47–48 (noting harmful consumer segments, including "interested in treason" and "children interested in alcohol").

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

[119]See Danielle Keats Citron and Frank A Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington Law Review 1, 1 (on data being used to "assess whether we are good credit risks, desirable employees, reliable tenants, valuable customers – or deadbeats, shirkers,

used to draw unexpected and adverse inferences about the consumer's credit risk on the basis of items they purchase, places they visit or people they associate with;[120] to provide inferior service based on their perceived "low value";[121] or to charge the consumer more on the basis of their perceived ability to pay.[122] It may mean, for example, that the consumer is charged higher interest rates or insurance premiums;[123] shown more expensive search results;[124] quoted higher prices for the same product;[125] or completely excluded from certain offers.[126] Data

menaces and 'wastes of time'"); Stucke and Ezrachi, 'Digital Assistants' (n 53) 1263–1270. *Compare* 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." ibid at 1287.

[120] See Hull (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).

[121] See Wolfie Christl, 'How Companies Use Personal Data Against People: Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information' (Working Paper, October 2017) 19, 28 (citing the examples of prioritization in call centres and ticketing).

[122] See Acquisti, 'The Economics of Personal Data and Privacy' (n 7) 17; Rafi Mohammed, 'How Retailers Use Personalised Prices to Test What You are Willing to Pay' *Harvard Business Review Online* (20 October 2017); Aniko Hannak et al., 'Measuring Price Discrimination and Steering on E-commerce Web Sites' (Proceedings of the 14th ACM/USENIX Internet Measurement Conference, Vancouver, Canada, November 2014) <cbw.sh/static/pdf/imc151_hannak.pdf>; Fabien Cros, 'Behavioural Pricing is the Ultimate in Personalisation' *Decision Marketing* (20 April 2020) (explaining and recommending methods of behavioural or personalised pricing using the data a company collects on its customers' behaviour). See 'WOW Personalisation', YouTube video <www.quantium.com/media/> accessed 16 October 2020:

> 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 …

[123] See Productivity Commission, Australian Government, 'Data Availability and Use' (Inquiry Report No 82, 2017) 86–89 (on data sharing in the context of insurance companies' risk analysis and marketing). See further Christl, 'How Companies Use Personal Data Against People' (n 121) 36–37 (including potential to increase price if data reveals mobile phone battery is low or the consumer has already booked a hotel for travel).

[124] See, eg, Dana Mattioli, 'On Orbitz, Mac Users Steered to Pricier Hotels' *Wall Street Journal* (23 August 2012); Hannak et al. (n 122).

[125] 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; Cognitive Scale <cognitivescale.com/wp-content/uploads/2018/11/policy-adjustment.pdf> accessed 16 October 2020, explains how "additional sources of rich data" including "consumer behaviour" and "consumer life events" can be used to "improve product profitability" for insurers by "re-pricing their policies and making other adjustments". Cognitive Scale also offers a product to help healthcare providers predict which patients will have "potentially high value bad debt accounts with more than 80 percent accuracy": <cognitivescale.com/wp-content/uploads/2018/03/amplify-bad-debt-risk-management.pdf> accessed 16 October 2020.

[126] Federal Trade Commission, 'Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues' (2016) 9–12; CPRC Emerging Issues Report (n 6) 24–25; CPRC Day in the Life of Data Report (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

collected in one context may be used for completely unrelated purposes, including automated decision-making "in crucial areas such as finance, insurance, employment, and law enforcement".[127]

Suppliers are also known to use profiling, micro-targeting and manipulation[128] to take advantage of consumer needs, habits, addictions and vulnerabilities.[129] As Pasquale has 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.[130] Such lists may be used to exploit people in their most vulnerable moments for financial gain.[131] Data analytics have also been used to manipulate individuals for the purpose of research, without their knowledge or consent.[132] Calo has explained the harm caused by "vulnerability-based marketing" built on these practices, which exploits the particular vulnerabilities of individual consumers, as revealed by their personal

Canada, 'The Age of Predictive Analytics: From Patterns to Predictions' (2012); Christl, 'How Companies Use Personal Data Against People' (n 121) 21–22 (on denial by automated systems).

[127]Christl, 'Corporate Surveillance' (n 41) 79. Data can also be used in future, unexpected contexts to pay casual or "gig" workers less for their work: see Christl, 'How Companies Use Personal Data Against People' (n 121) 31–32, 41.

[128]See Susser, Roessler and Nissenbaum (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."); Economides and Lianos (n 14) 66–72 (on the importance of competition authorities determining acceptable sources of evidence and appropriate tests for "behavioural manipulation").

[129]European Data Protection Supervisor (n 3) 8–9. See also Damian Clifford, 'Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side?' in Lilian Edwards, Burkhard Schafer and Edina Harbinja (eds), Future Law Series (2020) (on the use of emotion detection technology to create "emotionally tailored profiles" adding "a layer of manipulation" and 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"); Sam Levin, 'Facebook Told Advertisers It Can Identify Teens Feeling "Insecure" and "Worthless"' *The Guardian* (2 May 2017).

[130]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' 3–4 (29 November 2016). See also Kashmir Hill, 'Data Broker was Selling Lists of Rape Victims, Alcoholics and "Erectile Dysfunction Sufferers"' *Forbes* (19 December 2013); Norwegian Consumer Council, 'Out of Control' (n 5) 21–22 (on the "thousands of health-related audience segments for sale" on data broker Adobe's website); Christl, 'Corporate Surveillance' (n 41) 41 (on lists of "US Muslims" and "Unassimilated Hispanic Americans"). Data broker, DMDatabases, eg, advertises consumer mailing lists on the basis of drug addiction; gambling addiction; sexual addiction; bladder control; breast cancer; prostate cancer; cellulite; juvenile diabetes; haemorrhoids; herpes; HIV/AIDS; hormone imbalances; "impotence/erectile"; Parkinson's disease; vaginal infections; ADD; memory problems; "no sex drive"; mood swings; Viagra; "Clinical Depression Sufferers Mailing List" (over 1.8 million); and "Diabetics Mailing List" (over 12 million) <https://dmdatabases.com/databases/consumer–mailing> accessed 16 October 2020.

[131]Ryan Calo and Alex Rosenblat, 'The Taking Economy: Uber, Information & Power' (2017) 117 Columbia Law Review 1623, 1628 (explaining companies can then "reach consumers at their most vulnerable, nudge them into overconsumption, and charge each consumer the most she may be willing to pay").

[132]See Hull (n 32) 92; Christl, 'How Companies Use Personal Data Against People' (n 121) 31 (on Facebook mood experiments).

information.[133] Some firms are taking this further, using their ability to "unilaterally shape the networked environments and experiences of everyday life"[134] to deliberately *engineer* moments of vulnerability tailored to the individual and exploiting these vulnerabilities for financial gain.[135]

IV. Are concealed data practices a competition law issue?

A. Diverse views on the relevance of privacy in competition law

Concealed data practices potentially give rise to claims under privacy law (although the prospects of redress are limited in the US and elsewhere),[136] or consumer law, including misleading or deceptive conduct, unconscionable conduct and/or unfair contract terms.[137] They also demonstrate a need for consumer protection and/or privacy regulation to be strengthened to address the market failure resulting from the information asymmetry between firms and users, providing consumers with greater protection, information and choices.[138]

[133]Ryan Calo, 'Digital Market Manipulation' (2014) 82 George Washington Law Review 995; Calo and Rosenblat (n 131). See also Stigler Center Digital Platforms Report (n 3) 240–241; Christl, 'How Companies Use Personal Data Against People' (n 121) 35–36 (on "habit forming triggers"); Norwegian Consumer Council, 'Out of Control' (n 5) 46–47, 103.

[134]Christl, 'How Companies Use Personal Data Against People' (n 121) 41.

[135]Ibid. See also Alison Branley, 'Google Search Data Used by Pharma Giant to Bombard Users with Ads for Addictive Opioids' *ABC News* (13 July 2019):

> 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.

See also Susser, Roessler and Nissenbaum (n 5) (on the threats to individual autonomy).

[136]See Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal 115, 132–138, 155, 170–171 (arguing that the "US legal system favors its data processors over its privacy consumers"); Corey Ciocchetti, 'The Privacy Matrix' (2007) 12 Journal of Technology Law & Policy 245, 249–251; Stigler Center Digital Platforms Report (n 3) 29, 209; Australian Law Reform Commission, Australian Government, 'Serious Invasions of Privacy in the Digital Era' (Issues Paper, 2013) paras 136–138, 16; Australian Privacy Foundation, 'Submission to ACCC Digital Platforms Inquiry' (February 2019) 5–10. *Compare* Norwegian Consumer Council, 'Out of Control' (n 5) 162–180 (on the potential for action under the EU General Data Protection Regulation).

[137]See, eg, Daniel J. Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (2014) 114 Columbia Law Review 583; 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' (2016); ACCC, 'Google Allegedly Misled Consumers on Colleciton and Use of Location Data' (Media Release, 29 October 2019); ACCC, 'Health Engine in Court for Allegedly Misusing Patient Data and Manipulating Reviews' (Media Release, 8 August 2019); ACCC, 'ACCC Alleges Google Misled Consumers About Expanded Use of Personal Data' (Media Release, 27 July 2020).

[138]See ACCC Digital Platforms Report (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).

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.

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.[139] 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.[140] Even if privacy protection is a worthy social goal, the argument goes, it is a goal that falls outside the objectives of competition law.[141]

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.[142]

Some continue to assert that there is, in any case, a "privacy paradox" at work.[143] 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, since consumers' actions indicate they in fact value convenience over privacy. Privacy-enhancing alternatives do not achieve scale because the majority of consumers do not value them.

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

[140]Sokol and Comerford (n 7) 1156–1161; Manne and Sperry (n 8) 5–6.

[141]Sokol and Comerford (n 7) 1156–1161.

[142]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).

[143]See Patricia A Norberg, Daniel R Horne and David A Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors' (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); Haucap (n 9) 3; *cf.* generally Srinivasan (n 9) (arguing that Facebook circumvented its users' attempts to achieve privacy through false statements, misleading conduct and using technology to circumvent consumers' privacy choices). See further Part V *infra*.

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. Recognizing 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.[144] 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.[145] 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.[146] 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.[147]

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 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.[148] The true value for the supplier lies in accumulating vast quantities of high

[144]See Hoofnagle and Whittington, 'Free: Accounting for the Costs' (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' (n 7) 15-16.

[145]See OECD, 'Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value' (Economics Paper, 2013) 18–33; Economides and Lianos (n 14) 14, 72 (on "collective action to restore the conditions of a well-functioning data market" where "the purchaser of personal information is forced to offer … the full value of the personal information to the company"); Stigler Center Digital Platforms Report (n 3) 30, 55.

[146]See Stigler Center Digital Platforms Report (n 3) 54–56; UK Competition & Markets Authority, 'The Commercial Use of Consumer Data: Report on the CMA's Call for Information' (2015) paras 2.106-2.107.

[147]Hoofnagle and Whittington, 'Free: Accounting for the Costs' (n 14) 610; Stigler Center Digital Platforms Report (n 3) 55; Acquisti, Taylor and Wagman, 'The Economics of Privacy' (n 14) 447–448 (on attempts to value, and permit consumers to trade in, personal information).

[148]See Körber (n 8) 3, 9–10.

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.[149] One cannot put a price tag on the personal data disclosed to receive the free service.

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

There is a more apt way to conceptualize 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 quality of the service is reduced by this requirement because of the *costs* it creates for consumers.[150] The value of the service could even be reduced to the extent that the service is, on balance, detrimental to the consumer.[151]

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

[149]Körber (n 8) 10. See Haucap (n 9) 3 (arguing that "we may need to broadly distinguish between two types of potential users: Those who really care about their personal data and their privacy and those who do not, but happily share their data. If users of a particular Internet service do not mind if their personal data is used by the service provider, this means that they do not receive disutility from sharing personal data and having data sets combined.")

[150]*Compare* Strandburg (n 80) 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 Rubinfeld (n 16) fn 65.

[151]For example, 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* (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-Tamura, 'Maker of "Smart" Vibrators Settles Data Collection Lawsuit for $3.75 Million' *New York Times* (New York, 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 2013) <www.ftc.gov/sites/default/files/documents/cases/131205goldenshorescmpt.pdf> accessed 16 October 2020.

consumers,[152] 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, exclusion or disadvantage more generally for the consumer.[153]

The existence of these detriments does not mean consumers should not disclose their personal information. It does mean, in the competition law 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.

B. Concealed 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.

1. 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 differently, an increase in the quality-adjusted price of the service.[154] The extent to which a firm can retain customers while degrading its customers' data privacy without offsetting benefits is one indicator of market power.[155] Where a dominant firm imposes weak privacy protections on consumers (a higher quality-adjusted price), this may be seen as exploitative

[152]See Part III.B supra. See Acquisti, 'The Economics of Personal Data and Privacy', (n 7) 5; Acquisti, Taylor and Wagman, 'The Economics of Privacy' (n14) 483–484.

[153]See Federal Trade Commission, 'Big Data: A Tool for Inclusion or Exclusion?' (2016); Christl, 'Corporate Surveillance' (n 41) 4–5.

[154]Stigler Center Digital Platforms Report (n 3) 55; Srinivasan (n 9) 46–81 (arguing that Facebook reduced the quality of its zero-priced social media product by reducing users' privacy and privacy choices as it gained market power).

[155]Howard A Shelanski, 'Information, Innovation, and Competition Policy for the Internet' (2013) 161 University of Pennsylvania Law Review 1663, 1689; Esayas (n 53) 192, 197.

conduct: conduct that takes advantage of the firm's dominant position and freedom from competitive constraints to the detriment of consumers.[156]

In the EU, 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.[157] 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 Facebook platforms, even when users had "blocked web tracking in their browser or device settings".[158]

2. Requirement for exclusionary conduct

In a number of other jurisdictions, however, purely exploitative conduct is unlikely to contravene unilateral anticompetitive conduct laws.[159] Rather, a dominant firm will arguably 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.[160] The law is not concerned with the mere possession of a dominant position or substantial market power, but with firms *preserving or entrenching that*

[156]See Economides and Lianos (n 14) 39–42; Srinivasan (n 9) 97–98; Shelanski (n 155) 1687 (on the exercise of market power by reductions in quality).

[157]See Robertson (n 13) 9–11 (arguing that excessive data collection might be seen as analogous to excessive pricing under Art 102 TFEU); Esayas (n 53) 198; Katharine Kemp, *Misuse of Market Power: Rationale and Reform* (CUP 2018) 60 (describing the distinction between exclusionary and exploitative abuses).

[158]Bundeskartellamt, Germany, 'Bundeskartellamt prohibits Facebook from combining user data from different sources: Background information on the Bundeskartellamt's Facebook proceeding' (7 February 2019); Bundeskartellamt, Germany, 'Federal Court of Justice provisionally confirms allegation of Facebook abusing dominant position' (Courtesy Translation of Press Release No 080/2020 published by the German Federal Court of Justice, Jun. 23 2020) (annulling the decision of the Düsseldorf Higher Regional Court which had suspended the effect of the Bundeskartellamt's Feb. 2019 order). *Cf* Haucap (n 9) 4–5 (arguing that increased collection of users' personal data tends to benefit most users rather than exploiting users).

[159]See Kemp, *Misuse of Market Power* (n 157) 60. *Cf.* generally Srinivasan (n 9).

[160]See 15 USC § 2 (2012) (penalizing any person or corporation who engages in monopolizing conduct); *United States v. Grinnell Corp.*, 384 U.S. 563, 570–571 (1966); Phillip E Areeda and Herbert Hovenkamp, 3 *Antitrust Law: An Analysis of Antitrust Principles and Their Application* ¶ 618 (3d ed. 2008) (explaining that a court's imposition of "something more" on § 2 of the Sherman Act is generally assumed to mean conduct that qualifies as an exclusionary practice).

substantial market power by means other than superior efficiency.[161] If rival firms are not prevented from outcompeting the incumbent with a superior offer, the market itself is considered likely to 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.[162] 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 (described below) to explain why it is highly unlikely that digital markets will self-correct to a competitive level of privacy quality.[163]

3. Barriers to entry and competitive advantages in digital markets

At the outset, it is well known that 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),[164] increasing returns to scale (the service produces higher returns per user as the number of users increase)[165] and economies of scope (the platform can achieve lower costs per user of a service as the number of *services* it offers increases).[166] 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

[161]Explained further in Kemp, *Misuse of Market Power* (n 157) 58, 64. See also Srinivasan (n 9) 45, 90–94 (arguing that Facebook's pattern of future promises, false statements and misleading conduct secured monopoly power other than by "competition on the merits").

[162]Kemp, *Misuse of Market Power* (n 157) 52–55.

[163]Furman Report (n 4) 42–45, 60; Stucke and Grunes (n 45) 52–57; Esayas (n 53) 197 (explaining that, even if a degradation in privacy quality leads some well-informed consumers to desert, additional revenue from increased personal data collection combined with obfuscation by the supplier imposing degraded privacy terms, may mean that the degradation in quality is nonetheless profitable); Srinivasan (n 9) 46–81 (arguing Facebook acquired monopoly power through a pattern of false statements, misleading conduct and use of hidden technologies).

[164]See Stigler Center Digital Platforms Report (n 3) 38–39. See also Crémer, De Montjoye & Schweitzer (n 4) chap 2; Furman Report (n 4) 32–38; Bundeskartellamt (n 2) 4; Michael L Katz and Carl Shapiro, 'Network Externalities, Competition, and Compatibility' (1985) 75 American Economic Review 424; Economides and Lianos (n 14) 24 (on the network effects exhibited in online search).

[165]Stigler Center Digital Platforms Report (n 3) 36–37.

[166]Stucke and Ezrachi, 'Digital Assistants' (n 53) 1289–1290; Stigler Center Digital Platforms Report (n 3) 37.

the market as a whole.[167] New entry may also be hindered by the economies of scope enjoyed by incumbents operating over multiple markets.[168]

Major digital platforms also enjoy advantages of scope in respect of consumer data, given that they are able to combine datasets relating to overlapping consumers across multiple markets, creating a depth of information on individual consumers which allows the platform to earn more revenue from advertising and increase the "stickiness" of the platform for existing and potential users.[169] These features of digital markets can contribute to market dominance, and help to explain the limited success of new entrants and 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).[170]

4. Barriers to entry and competitive advantages increased by concealed data practices

A rival attempting to offer a product with superior 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 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 advertizers, shoppers and merchants, or online search users and advertizers.[171] Multisided platforms exhibit indirect network

[167]Shelanski (n 155) 1682; Stigler Center Digital Platforms Report (n 3) 34–35; *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"). See Marsden and Podszun (n 4) 25–31 (on the treatment of "unnatural tipping" under German law).

[168]Stigler Center Digital Platforms Report (n 3) 37.

[169]ACCC Digital Platforms Report (n 3) 73–84 (on the advantages of scope in respect of consumer data which contribute to the market power enjoyed by both Google and Facebook). See further Daniele Condorelli and Jorge Padilla, 'Data-Driven Envelopment with Privacy-Policy Tying' (Unpublished paper, 30 August 2020) 2–5 (on privacy policy tying). See also Part IV.B(4) *infra*.

[170]Furman Report (n 4) 31; Norwegian Consumer Council, 'Out of Control' (n 5) 121–122.

[171]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* (2017) 378–385; 'Common Understanding of G7 Competition Authorities on "Competition and the Digital Economy"' (July 2019) 5; David S Evans and Richard Schmalensee, *Matchmakers: The New Economics of Multisided Platforms* (2016) 14–19.

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.[172] Advertizers value an online search engine more highly, for example, the more consumers use that search engine.[173]

Consumers' personal data plays a critical role in these multisided platforms and the preservation of an incumbent's dominant position.[174] For example, a social media platform has an incentive to harvest increasingly broad and deep personal data on its users.[175] This aggregation of personal data 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.[176] The social media platform may then use the increased advertising revenue, the "learning by doing" effects of access to a huge variety and depth of personal data,[177] 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.[178] 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,[179] without deterring consumers from using the platform on the basis of its data practices, and so the cycle

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

[173]Whittington and Hoofnagle, 'Unpacking Privacy's Price' (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, advertizers 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 Evans and Schmalensee (n 171) 93–100.

[174]Stigler Center Digital Platforms Report (n 3) 40–41, 43; Economides and Lianos (n 14) 14; Khan and Pozen (n 14) 517–518; Condorelli and Padilla (n 169) (on the relevance of 'privacy policy tying' to monopoly protection).

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

[176]See Stucke (n 13) 286. *Cf*. Manne and Sperry (n 8) 5–6 (arguing there is "no obvious reason why monopolists would have an incentive to degrade privacy"). See also Bundeskartellamt (n 2) 4–5 (explaining indirect network effects).

[177]Stucke and Grunes (n 45) 170–181; Stucke and Ezrachi, 'Digital Assistants' (n 53) 1249–1251, 1286–1287.

[178]Stucke and Ezrachi, 'Digital Assistants' (n 53) 1251–1254; Esayas (n 53) 185–186, 187.

[179]See Stucke and Ezrachi, 'Digital Assistants' (n 53) 1255–1266; Stucke (n 13) 282–283 (on the data-driven network effect of "learning by doing" for search engines). See also Economides and Lianos (n 14) 14; Shelanski (n 155) 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).

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*.[180]

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.[181] The extent of the costs imposed by the concealed data practices of incumbents are not reflected in the zero monetary price commonly charged in digital markets, bearing in mind that concealed data practices may in fact be sufficiently detrimental that the price should be negative: that is, suppliers would have to pay consumers to use the product in question.[182]

Taking into account other features and functionality of the incumbent service engaged in concealed data practices, a privacy-enhancing rival would have to offer consumers an apparently lower quality, or higher priced, service since the rival could not pay for other attractions with advertising revenue gained by monetizing consumers' personal information.[183] Consumers will not pay more to avoid a cost which cannot be assessed.[184] 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 by the combined effect of concealed data practices and the lack of implied quality information in zero-price markets.[185]

[180]See Stigler Center Digital Platforms Report (n 3) 43; Furman Report (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' (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); Acquisti, Talyor and Wagman (n 14) 444.

[181]Norwegian Consumer Council, 'Out of Control' (n 5) 5–6.

[182]See (n 151) *supra*.

[183]See Evans, 'Attention Platforms' (n 7) 20–21 (on suppliers' reduced incentive to invest in the product in the absence of greater access to consumer data and therefore advertising revenue); Esayas (n 53) 187–188.

[184]Stigler Center Digital Platforms Report (n 3) 67 ("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.").

[185]*See* Shelanski (n 155) 1690 (on the fact that data practices are not generally observable for consumers); Norwegian Consumer Council, 'Out of Control' (n 5) 6 ("20 months after the GDPR has come into effect, consumers are still pervasively tracked and profiled online and have no way of knowing which entities process their data and how to stop them"); Christl, 'How Companies Use Personal

In the absence of this competitive pressure from rivals, dominant firms may impose exploitative privacy terms on consumers.[186] 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 monetizing consumer data.[187] 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.

5. 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.[188] 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.[189] A consumer's personal information may be used by suppliers in a number of markets, who take advantage of these

Data Against People' (n 121) 48–49 (arguing weak privacy regulation and enforcement impedes the emergence of digital innovation "of practices, technologies, and business models that preserve autonomy, democracy, social justice, and human dignity").

[186]Stigler Center Digital Platforms Report (n 3) 43, 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.*"); Srinivasan (n 9) 97 (arguing that Facebook enjoys monopoly power and "extracts the cost of widespread digital surveillance despite users' preference to the contrary"); Bundeskartellamt, Germany, 'Bundeskartellamt prohibits Facebook from combining user data from different sources: Background information on the Bundeskartellamt's Facebook proceeding' (7 February 2019).

[187]See Stucke and Grunes (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 (n 3) 423–424; Norwegian Consumer Council, 'Out of Control' (n 5) 7; Shelanski (n 155) 1690 (on the potential lack of incentives for "comparatively pro-consumer [privacy] policies"); Srinivasan (n 9) 100 (regarding the potential "domino effect" of deception by a dominant firm); Esayas (n 53) 190–191 (on consumer cynicism due to privacy-degrading practices impeding privacy competition). See also Bruce Schneier, *Data and Goliath* (2015) 242–243 (on the need for incentives to create new business models that do not depend on consumer surveillance).

[188]See further Acquisti, 'The Economics of Personal Data and Privacy' (n 7) 17; Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' 11 (2013) North Western Journal of Technology & Intellectual Property 239, 255 ("Transacting with a big data platform is like a game of poker where one of the players has his hand open and the other keeps his cards close").

[189]See Nicolas Petit, *Big Tech and the Digital Economy: The Moligopoly Scenario* (2020, forthcoming) (describing the ways in which large platforms increasingly compete across multiple markets).

information asymmetries to focus on consumer manipulation[190] 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,[191] and allowing suppliers to engage in manipulation-based marketing in a way traditional advertising does not permit.[192] 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.[193]

V. 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

[190] See the definition of "online manipulation" by Susser, Roessler and Nissenbaum (n 128).

[191] 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 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' (n 7) 17–18.

[192] See Stigler Center Digital Platforms Report (n 3) 240–241; Strandburg (n 80) 137–141; Khan and Pozen (n 14) 511; Katharine Kemp, 'Submission to the Australian Competition & Consumer Commission Ad Tech Inquiry Issues Paper' (26 April 2020) 5–7.

[193] Stigler Center Digital Platforms Report (n 3) 59 ("A platform can analyze a user's data in real time to determine when she is in an emotional 'hot state' and then offer a good that the user would not purchase when her self-control was higher"). See also Susser, Roessler and Nissenbaum (n 5); Stigler Center Digital Platforms Report (n 3) 60:

> [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.

chilling privacy-enhancing competition. This weakening of competition may not amount to a contravention of competition legislation in itself. However, the effect of concealed data practices on the competitive process should be taken into account by competition regulators in the following respects.

A. "Privacy paradox" arguments conceal the denial of consumer choice

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.[194] 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.[195] 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".[196] First, firms' claims that consumers have "chosen" certain privacy terms are often not based on any active choice of terms by the consumer, but on consent which is taken to be implied by the consumer's use of a service combined with the publication of vague, lengthy privacy policies; privacy-degrading default settings chosen by the firm; and/or the firm's obstruction or preclusion of privacy-enhancing choices. Second, the relevant decision and its effects are generally highly complex, due to the firm's presentation of privacy terms, the extent of the relevant data practices and the

[194] *Cf.* Productivity Commission, Australian Government, 'Data Availability and Use' (Inquiry Report No 82, 2017) 91 (arguing in the case of "large social media providers", "large firms will tend to self-regulate … according to prevailing public attitudes"); Haucap (n 9) 3, arguing:

> While it is true that many people, when asked in public, maintain that they are concerned about how their personal data is used and that they are rather protective about how their data is used, these stated preferences are not revealed in their actual behavior. … As, however, preferences revealed through actual behavior are typically taken to better reflect individuals' true preferences than surveys, it appears that many people willingly share their data in order to obtain better services. Given these findings, it is difficult to conceive how users can be exploited if they willingly share their data.

[195] See Part III.A *supra*. See also Srinivasan (n 9) 72–73 (on Facebook's invisible and pervasive surveillance of individuals who choose not to use Facebook, via third party websites). *Contra* Manne and Sperry (n 8) 5–6. On the application of revealed preference theory in economics, 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.").

[196] Beshears et al (n 195) 1788–1789.

difficulty in determining present and future consequences of those data practices. Third, the consumer has limited personal experience of the consequences of this choice, since data practices and their consequences are generally not revealed. Fourth, firms frequently actively market the choice in question, particularly where privacy policies are framed to manipulate consumers to accede to privacy intrusive practices.[197]

It is therefore generally inappropriate to discount expressed consumer preferences by reference to the "privacy paradox".[198] 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.

B. Privacy quality in the assessment of competition and market power

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,[199] 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.[200] 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.[201] Competition

[197]See ibid. See also Esayas (n 53) 189.

[198]See (n 143).

[199]Stucke and Ezrachi, 'Digital Assistants' (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."); Esayas (n 53) 182–184, 192–194 (arguing for "time spent on the platform" as a proxy for market power (share) that reflects a firm's ability to reduce users' data privacy); ibid at 197 (arguing that information asymmetries and "confusology" should be taken into account in determining the extent to which consumers can, or cannot, constrain the data practices of the incumbent); Srinivasan (n 9) 87–88 (similarly arguing in favour of "time spent" as a measure of market power).

[200]Furman Report (n 4) 42–45; Commission, 'Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions' (Press Release, 6 December 2016) <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. *Contra.* Robert Bork, 'Antitrust and Google' *Chicago Tribune* (6 April 2002). Importantly, dissimilarity in privacy terms or technologies need not result in a conclusion that the products are complements rather than substitutes: Esayas (n 53) 194.

[201]See, eg, Evans, 'Attention Platforms' (n 7); Haucap (n 9) 4–5.

authorities should equally take into account the negative impacts of concealed data practices on quality competition described in Part III(B) above, which critically includes the quality of privacy terms offered and privacy-enhancing innovation.[202]

These detriments should not be overlooked on the basis that they cannot be precisely quantified in dollar terms.[203] "[T]he lack of explicit prices does not mean the harms are any less real."[204] In the context of markets with zero monetary prices, consumer benefits are not generally quantifiable either.[205] But competition authorities should take both into account, and consider the proportionality of any plausible detriments against the plausible benefits.[206] 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.[207]

C. Further restrictions on privacy more readily constitute an anticompetitive effect

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

[202]Stucke and Ezrachi, 'Digital Assistants' (n 53), 1284–1285, 1293 ("Interventions will have to balance the benefits which flow from advanced technology and artificial intelligence against the welfare risks … "); David S Evans, 'Deterring Bad Behavior on Digital Platforms' (Working Paper, 17 September 2019) 49–51; Esayas (n 53) 183.

[203]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").

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

[205]*Contrast* Evans, 'Attention Platforms' (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).

[206]See, eg, Evans, 'Deterring Bad Behavior' (n 202) 50–51 (arguing that the question of whether an excluded rival is "as efficient competitor" as the incumbent could take into account the "non-price terms it can offer consumers" as an element of the rival's efficiency). *Cf.* Manne and Sperry (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.").

[207]See 'Common Understanding of G7 Competition Authorities on "Competition and the Digital Economy"' (July 2019) 4; Stigler Center Digital Platforms Report (n 3) 31–32, 87–88; Esayas (n 53) 183 ("the proxies used to assess market power remain largely price-centric or fail to cater to data privacy interests"); Stucke (n 13) 287 (on a potential "SSNDPP" test or "small, but significant, nontransitory decrease in privacy protection"); Stucke and Ezrachi, 'Digital Assistants' (n 53) 1296 (on the difficulty of assessing the counterfactual in such scenarios).

competition.[208] Various prohibitions are triggered where conduct or an acquisition has the effect or likely effect of substantially lessening competition or eliminating effective competition. These contraventions may be based on substantially reduced competition on privacy quality, just as they may be based on reduced competition on price.[209] For example, a cartel might reduce competition on privacy quality by adopting a code of conduct which limits potentially privacy-enhancing offerings by its members.[210]

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, the merger may result in a substantial lessening of competition.[211] A merger could soften privacy competition by allowing the dominant acquiring firm to impose its weaker data governance on the target firm,[212] or eliminate a privacy-enhancing rival.[213] In the context of unilateral conduct, if a dominant digital platform engages in conduct which, for example, excludes privacy-enhancing apps from its platforms (potentially over multiple markets), this may give rise to a claim of abuse of dominance or monopolization.[214]

The existence of concealed data practices on the part of firms in possession of market power in these scenarios would indicate that there is

[208]See Harbour and Koslov (n 203) 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).

[209]See Furman Report (n 4) 42–45 (stating that "the misuse of consumer data and harm to privacy is arguably an indicator of low quality caused by a lack of competition. It may also be a method for achieving and cementing market power").

[210]Evans, 'Deterring Bad Behavior' (n 202) 50–51.

[211]See Mike Isaac, 'Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger' *New York Times* (New York, 25 January 2019) <www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html>; Robert H Lande, 'The Microsoft-Yahoo Merger: Yes, Privacy Is an Antitrust Concern' (25 February 2008) FTC:Watch 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."); Esayas (n 53) 187. *See also* Argentesi et al, Lear, 'Ex-post Assessment of Merger Control Decisions in Digital Markets: Final Report' (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).

[212]See Evans, 'Deterring Bad Behavior' (n 202) 50–51; Esayas (n 53) 185 (on the Microsoft/LinkedIn merger decision). Where the dominant acquiring firm engages in concealed data practices, it not only imposes its weaker data standards on the target firm, but also conceals this fact from consumers and so removes a source of consumer information about those weaker standards.

[213]As in the case of the Whats App/Facebook Merger: Esayas (n 53) 191, 195–197.

[214]See Stucke and Ezrachi, 'Digital Assistants' (n 53) 1256–1263 (on the gatekeeper role digital assistants perform in respect of upstream services); Esayas (n 53) 182–183, 188–189 (citing the examples of Google's exclusion of ad blocking software, Disconnect, and research-based privacy tool, AdNauseam). Or downgrading interoperability: Stucke and Ezrachi, 'Digital Assistants' (n 53) 1295.

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.[215]

D. Interpreting the state of privacy competition and potential ex ante regulation

Market investigations, and investigations of conduct which is alleged to suppress competition on privacy quality, 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.[216] 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 available information and empower consumers in their decision-making.[217]

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. Market investigations and investigations regarding complaints of anticompetitive conduct in

[215]See Crémer, De Montjoye and Schweitzer (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.

The privacy terms of an excluded rival may also be relevant to whether that rival was an "as efficient competitor" (Evans, 'Deterring Bad Behavior' (n 202) 50–51). Strict privacy terms imposed by an incumbent may constitute vigorous competition on quality or a pretext for exclusionary conduct: *Toronto Real Estate Board v. Commissioner of Competition* [2017] FCA 236 (1 December 2017) [160]-[165], [174].

[216]See Ohlhausen and Okuliar (n 8) 152–155.

[217]Omri Ben-Shahar and Carl E Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (2016) 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; Christl, 'How Companies Use Personal Data Against People' (n 121) 50 (on the role "authorities, advocates, journalists" and others can play in addressing questionable practices and raising awareness through research, investigation and legal action).

respect of privacy quality provide an opportunity for the competition regulator 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.[218]

In the EU especially, there are also increasing proposals for information-gathering and remedial powers in the absence of enforcement action. The "ex ante regulatory framework", proposed as part of the Digital Services Act package, could enable "targeted collection of information by a dedicated regulatory body at EU level" including information on the platforms' data practices and their impact on consumers.[219] The ex ante regulatory framework could also permit the regulator to impose "tailor-made remedies" responding to the fast-evolving online platform environment. This framework is specifically aimed at large online platforms that benefit from significant network effects and act as gatekeepers. A parallel development which may not be restricted to such platforms is the proposal for a "New Competition Tool" (NCT). Market investigations under the NCT have the potential to yield information about the data practices of firms and the quality of competition on privacy quality in the absence of enforcement action under Articles 101 or 102, and lead to timely remedies for structural competition problems without the need for lengthy litigation, findings of contravention or the imposition of fines.[220] One such remedy is discussed in the following section.

[218]See, eg, Bundeskartellamt (n 2) explaining Facebook's alleged exploitative data practices:

> [T]his is what many users are not aware of: Among other conditions, private use of the network is subject to Facebook being able to collect an almost unlimited amount of any type of user data from third party sources, allocate these to the users' Facebook accounts and use them for numerous data processing processes. Third-party sources are Facebook-owned services such as Instagram or WhatsApp, but also third party websites which include interfaces such as the "Like" or "Share" buttons. … It is not even necessary, eg, to scroll over or click on a "Like" button. Calling up a website with an embedded "Like" button will start the data flow. Millions of such interfaces can be encountered on German websites and on apps.

See also ACCC, 'Statement of Issues: Google LLC – Proposed Acquisition of Fitbit Inc' (18 June 2020) (expressing the preliminary view that Google's commitment not to use Fitbit "health and wellness data" for advertising purposes was "not binding on Google and experience also suggests that intentions stated by an acquiring party at the time of an acquisition may well change over time"); 'US: DOJ to Review Google's Fitbit Acquisition for Antitrust Flags' (11 December 2019) Competition Policy International.

[219]Commission, 'Digital Services Act package – ex ante regulatory instrument regulatory instrument of very large online platforms acting as gatekeepers' (4 June 2020) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers>.

[220]Commission, 'Single Market – new complementary tool to strengthen competition enforcement' (4 June 2020); Massimo Motta and Martin Peitz, 'Intervention Triggers and Underlying Theories of Harm: Expert Advice for the Impact Assessment of a New Competition Tool' (European Commission 2020) 14–21; Marsden and Podszun (n 4).

E. Consumer-centred data portability

Where concealed data practices prevent consumers from making meaningful choices about the ways in which firms collect and use their personal data, the creation of data portability rights is one tool which may be used to aid consumers in regaining some control over that data and accessing better offers from competitors. By mandating the portability of data via an application programming interface (API), for example, data portability regimes can assist in reducing consumers' switching costs, increasing choice, and offsetting the power of dominant incumbents.[221] Particularly when combined with an appropriately-framed right to erase personal data held by the incumbent, data portability rights may also serve a disciplining function by permitting consumers to remove their personal data from the firm's future control where they become aware of unacceptable risk or misuse.

Examples of such data portability rights in action can be found in the UK Open Banking regime and the Australian "consumer data right", currently being implemented in the banking sector.[222] Both mandate transfers of personal data at the consumer's request via APIs. In Australia, the government intends that the consumer data right will be rolled out sector by sector across the economy, with rules tailored to each sector.[223] In Europe, specific data portability remedies beyond banking and financial services are also being considered in the context of the proposed ex ante regulatory framework for large online platforms and the NCT. Marsden and Podszun, for example, have recommended "data access, data portability, interoperability, [and] enhanced consumer control" as some of the remedies which could be imposed to improve competition on privacy quality following a market investigation under the NCT.[224]

Bearing in mind their objectives, it is critical that data portability regimes are designed to protect and increase consumers' control over their personal data, rather than creating a data trading platform for firms. It is inevitable that some firms faced with the prospect of loosening their grip on consumers' personal data through mandated data

[221]See, eg, ACCC, 'Explanatory Statement: Proposed Competition and Consumer (Consumer Data Right) Rules 2019' (August 2019) 5.

[222]The Treasury, Australian Government, 'Consumer Data Right: Overview' (September 2019) <https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf> accessed 16 October 2020 (hereinafter *Australian Consumer Data Right Overview*); Marsden and Podszun (n 4) 65–68.

[223]Ibid iv.

[224]Marsden and Podszun (n 4) 68; 75–76. See also Motta and Peitz (n 220) 34; Condorelli and Padilla (n 169) 16 (arguing that 'unrestricted portability may end up damaging consumers' but 'a requirement to offer portability of data only levied on the dominant operator would both restore incentives to entry and eliminate those to foreclose').

portability will look for opportunities to exploit the mechanism for their own purposes. From our experience of concealed data practices to date, absent adequate protections, firms will have incentives to take advantage of these regimes to extract and share more consumer data for their own commercial purposes under the cloak of complex, opaque privacy terms. Some have expressed legitimate concerns about the effects of major digital platforms combining banking data received via data portability regimes with extensive personal data collected from the platforms' own interactions with the consumer, as well as third party sources.[225] The prospect of some firms being advantaged in this way has led to calls for "reciprocity" between firms in their data portability obligations. In the context of the implementation of the consumer data right in the banking sector in Australia, for example, banks complain that platforms "will be able to use the regime to get insights about banking without allowing the banks any *quid pro quo*, such as data that could provide insights on customers' retail, or social media, behaviours".[226]

If a data portability regime is to empower consumers, however, it should not be premised on expectations of "reciprocity" or "quid pro quo" between firms seeking to track their customers "behaviours" more pervasively across multiple sectors and spheres of life. Such an approach would deepen the information asymmetries and imbalances in bargaining power these measures purport to offset. Data portability remedies should be carefully framed with sufficient consumer controls, transparency and regulatory oversight to ensure that the consumer is sovereign in these transfers, and not simply a more trusting pawn facilitating the flow of personal data between powerful firms.[227]

VI. Conclusion

Data-driven businesses are altering the frontiers of influence, by their ubiquity, scale and subtlety. In a world of digital assistants, pervasive

[225]See, eg, Oscar Borgogno and Giuseppe Colangelo, 'The Data Sharing Paradox: BigTechs in Finance' (2020) *European Competition Journal*.

[226]James Eyers, 'CBA Calls for Consumer Data Right Extension to Global Tech Players' *The Australian Financial Review* (Sydney, 20 July 2020) <https://www.afr.com/companies/financial-services/cba-calls-for-consumer-data-right-extension-to-global-tech-players-20200717-p55d4n> accessed 16 October 2020. See further Nicholas Megaw and Rochelle Toplensky, 'Santander Chair Calls EU Rules on Payments Unfair' *Financial Times* (17 April 2018) <https://www.ft.com/content/d9f819f2-3f39-11e8-b7e0-52972418fec4> accessed 16 October 2020; Borgogno and Colangelo (n 225) 14–16.

[227]See Financial Rights Legal Centre and Consumer Action Law Centre, 'Submission to Senate Select Committee on Financial Technology and Regulatory Technology' (December 2019) 5–8 <https://financialrights.org.au/wp-content/uploads/2020/02/191223_FinTechInquiry_Sub_FINAL-1.pdf> accessed 16 October 2020.

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 article also cause objective detriment to consumers and undermine the competitive process on privacy quality and beyond. New proposals to increase consumer benefits from data innovations are to be applauded. Competition authorities should also have regard to concealed data practices in rejecting claims of "revealed preferences"; assessing the quality of competition on privacy, in zero-priced digital markets in particular; assessing the significance of any lessening of competition, including by the exclusion or absorption of privacy-enhancing rivals; and empowering consumers through consumer-centred data portability. These considerations fall squarely within the established objectives of competition law, in protecting the competitive process in the interests of consumer welfare.

Disclosure statement

No potential conflict of interest was reported by the author(s).