Data privacy, fairness and privacy harms in an algorithm and AI enabled world

Peter Leonard[1]

There is growing consensus that the Australian Privacy Act, in common with similar statutes in other jurisdictions, needs a major overhaul.

The current review by the Australian Attorney-General's Department (**AGD**) of the Australian federal Privacy Act 1988 (C'th) (**Australian Privacy Act**)[2] provides an opportunity to:

- improve mechanisms to protect data privacy of Australians,
- reduce friction of cross-border dealings, by improving alignment of Australian data privacy regulation with international regulatory best practice, and
- accommodate societally beneficial secondary and derived uses of data.

Australia has the opportunity to select and tailor the best features of new data privacy statutes from around the world and to ensure that the Australian Privacy Act belatedly becomes fit for purpose in the 21st century.

There are many current initiatives for reform of data privacy laws in comparable jurisdictions that should inform overhaul of the Australian Privacy Act. They include:

- comprehensive review in the United Kingdom of whether UK GDPR should diverge from EU GDPR, with the stated objective of better enabling innovation in the UK,[3]
- proposals in the European Union to supplement EU GDPR with a Digital Markets Act and a Digital Services Act, and an associated package of initiatives to address applications of artificial intelligence and advanced data analytics[4], and

---

[1] Copyright © Peter Leonard (Data Synergies Pty Limited) 2022. Peter Leonard is a business consultant and lawyer advising data-driven businesses and government agencies. Peter is principal of Data Synergies and a Professor of Practice at UNSW Business School (Information Systems and Technology Management, and Management and Governance). Peter is immediate past chair of the AI Ethics Technical Committee of the Australian Computer Society and the Privacy and Data Committee of the Law Society of New South Wales. Peter was a founding partner of Gilbert + Tobin. He serves on the NSW Government's AI Review Committee and Information and Privacy Advisory Committee, and a number of corporate and advisory boards.

[2] See Australian Attorney-General's Department, Privacy Act Review Discussion Paper, October 2021, (**AGD Privacy Review Discussion Paper**) available at https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper. The Australian Privacy Act is available at https://www.legislation.gov.au/Details/C2021C00452

[3] UK Department for Digital, Culture, Media & Sport, Data: a new direction, September 2021; UK Information Commissioner's Office, Response to DCMS consultation "Data: A New Direction", 6 October 2021; see also UK Taskforce on Innovation Growth and Regulatory Reform, Final Report, May 2021

[4] EU Digital Markets Act at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en; EU Digital Services Act at https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package; EU Regulatory framework proposal on artificial intelligence at https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai; EU draft AI Act at https://eur-lex.europa.eu/procedure/EN/2021_106. For an analysis of the interaction between proposed provisions of the Digital Markets Act and GDPR, see Centre for Information Policy Leadership, "Bridging the DMA

- in the USA, proposals for a federal data privacy statute[5], development by the Unform Law Commission of a Uniform Personal Data Protection Act[6], and U.S. State by State enactment of data privacy statutes[7],
- substantial recent revisions of data privacy statutes in Singapore[8], Korea[9] and Japan[10], and a new statute in Quebec[11],
- proposed revisions to the Canadian federal privacy statute[12] and for a new data protection statute in India.[13]

Many consumer organisations and privacy advocates across the world criticise national privacy and data protection statutes, and enforcement of them, as inadequate and incomplete. Sometimes those criticisms are echoed within international organisations and national legislatures.[14] As stated by the Joint Committee on Human Rights of the UK Parliament in its Inquiry Report on The Right to Privacy (Article 8) and the Digital Revolution:

> *The evidence we heard during this inquiry ... has convinced us that the consent model is broken. The information providing the details of what we are consenting to is too complicated for the vast majority of people to understand. Far too often, the use of a service or website is conditional on consent being given: the choice is between full consent or not being able to use the website or service. This raises questions over how meaningful this consent can ever really be.*
>
> *Whilst most of us are probably unaware of who we have consented to share our information with and what we have agreed that they can do with it, this is undoubtedly doubly true for children. The law allows children aged 13 and over to give their own consent. If adults struggle to understand complex consent agreements, how do we*

---

and the GDPR", December 2021, available at https://www.huntonprivacyblog.com/2021/12/16/cipl-publishes-white-paper-on-the-interplay-between-the-draft-eu-digital-markets-act-and-the-gdpr/.

[5] For a summary, see IAPP, US Federal Privacy Legislation Tracker, https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/

[6] Uniform Personal Data Protection Act, as drafted by the U.S. Uniform Law Commission, linked at https://fpf.org/blog/uniform-law-commission-finalizes-model-state-privacy-law/

[7] US State Privacy Legislation Tracker, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

[8] Personal Data Protection Act (No 26 of 2012) of Singapore, https://sso.agc.gov.sg/Act/PDPA2012, as amended in November 2020

[9] Privacy Act No. 16930, February 4, 2020

[10] Act on the Protection of Personal Information; see further Takeshige Sugimoto, Akihiro Kawashima and Tobyn Aaron, "A New Era for Japanese Data Protection: 2020 Amendments to the APPI", 13 April 2021, https://fpf.org/blog/a-new-era-for-japanese-data-protection-2020-amendments-to-the-appi/

[11] Act respecting the protection of personal information in the private sector, CQLR c P-39.1, https://www.canlii.org/en/qc/laws/stat/cqlr-c-p-39.1/latest/cqlr-c-p-39.1.html

[12] Canada Bill C-11 (now lapsed following prorogue of the Canadian Parliament), https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading

[13] Joint Parliamentary Committee report on the Personal Data Protection Bill, 2019 presented to the Lok Sabha on 16 December 2021, available at http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf. An annexure sets out a consolidated and revised version of the Bill, proposed to be renamed 'the Data Protection Act, 2021

[14] Report of the United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age", September 2021

expect our children to give informed consent? Parents have no say over or knowledge of the data their children are sharing and with whom. There is no effective mechanism for a company to determine the age of a person providing consent. In reality a child of any age can click a 'consent' button.

The bogus reliance on 'consent' is in clear conflict with our right to privacy. The consent model relies on us, as individuals, to understand, take decisions, and be responsible for how our data is used. But we heard that it is difficult, if not nearly impossible, for people to find out whom their data has been shared with, to stop it being shared or to delete inaccurate information about themselves. Even when consent is given, all too often the limit of that consent is not respected. We believe companies must make it much easier for us to understand how our data is used and shared. They must make it easier for us to 'opt out' of some or all of our data being used. More fundamentally, however, the onus should not be on us to ensure our data is used appropriately - the system should be designed so that we are protected without requiring us to understand and to police whether our freedoms are being protected.

As one witness to our inquiry said, when we enter a building we expect it to be safe. We are not expected to examine and understand all the paperwork and then tick a box that lets the companies involved 'off the hook'. It is the job of the law, the regulatory system and of regulators to ensure that the appropriate standards have been met to keep us from harm and ensure our safe passage. We do not believe the internet should be any different. The Government must ensure that there is robust regulation over how our data can be collected and used, and that regulation must be stringently enforced.[15]

Notwithstanding such concerns, reform of data privacy law in various jurisdictions is slow and highly contested.

This paper considers why this is the case.

We then explore some of the key concerns enlivening debate as to the appropriate scope of reform of Australian data privacy law, with a particular focus upon proposals for reform of the Australian Privacy Act and comparable State and Territory data privacy and health information statutes.

We then review the role for data privacy impact assessment in improving accountability of regulated entities for their data privacy affecting acts and practices. Existing practices in data privacy impact assessment are of variable quality: we examine why this is the case and how this should lead to concern that proposed tools for AI and algorithmic impact assessment may

[15] Report of the UK House of Commons and House of Lords, Joint Committee on Human Rights, "The Right to Privacy (Article 8) and the Digital Revolution", HC 122, HL Paper 14, published on 3 November 2019; see also Manwaring, Kayleen, "Will Emerging Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation", Competition and Consumer Law Journal, 2018, Vol 26, Issue 2, pp 141-181; Agustin Reyna, "European Consumer Law in a Digital Economy: How EU Enforcers Are Rising to the Challenge", Antitrust (American Bar Association) , Vol. 36, No. 1, Fall 2021

not be properly developed and reliably applied by the broad range of entities already deploying and using automated decision-making.

This paper concludes with an opinionated design manifesto for reform of the Australian Privacy Act, to ensure that the statute becomes fit for purpose for the 21st century - albeit now over two decades into that century.

Building good statutes requires good policy foundations. We start by asking two foundational questions:

- *what should a data privacy statute do*?
- *what should a data privacy statute not do?,* because what needs to be legislated is more appropriately addressed in another statute, or because it is not yet realistically practicable to determine whether there is a need for regulation or how to regulate.

We also sound the caution that Australian data privacy regulation should align with international best practice. Many entities regulated under Australian data privacy laws already conduct operations in multiple jurisdictions, or have ambitions to do so. If Australia elects to chart its own course, Australian entities may be forced to incur substantial, regulation-induced, costs in adapting data architectures and analytics processes, and data handling practices, for cross-border dealings. In any event, there are emerging convergences in key settings in data privacy statutes in Australia, New Zealand, Singapore, Japan and Korea, most notably in relation to settings around use of privacy enhancing technologies and controlled data analytics environments that rely upon effective anonymisation. These convergences provide opportunities for further alignment and friction reducing measures, such as mutual recognition schemes, across those jurisdictions. Australian policy-makers should exercise particular caution to avoid, wherever reasonably practicable, devising regulatory measures that lead to Australia-specific, regulation-induced, costs for Australian entities in cross-border dealings.

Concerns as to collection and uses of data about consumers and the scope of data privacy law

Data policy concerns now range far beyond the scope of rights or interests of citizens to go about their private lives, including in public and semi-public places, without unjustified or unexpected collection and uses of data. The range of concerns as to collection and uses of data about consumers and other citizens continues to grow, and includes:

- the relative roles of consideration by regulated entities of social responsibility, business ethics or social licence, to moderate and control unjustified or unexpected collection and uses of data, and enactment and enforcement of 'hard law' with penalties and legal sanctions,
- the need to nurture digital trust of citizens, in order to ensure a vibrant digital economy,
- importance of digital inclusion and addressing accessibility of digital services by all,

- enabling societally beneficial uses of data,[16]
- considerations of social equity, and the reasonableness (or otherwise) of weighting of benefits for the many against detriments to a few,
- online safety and protection of children and other vulnerable people,
- for online services, addressing use by service providers of 'dark patterns' and behavioural psychology to encourage individuals to volunteer data or to not seek out privacy options and exercise them to shift settings to be more privacy protective,
- addressing the emerging panopticon of surveillance and 'profiling' of citizens,
- 'biased and discriminatory' algorithms and AI,
- 'unaccountable' algorithms and AI,
- lack of transparency of privacy intrusive acts and practices of businesses, governments, political parties and other political actors, and some not-for-profits,
- limitations in legal authority and practical ability of national actors and national regulation to address cross-border and global issues, including acts and practices of entities operating in other jurisdictions and dealing from outside the jurisdiction with citizens or residents within the jurisdiction,
- considerations of national political and economic sovereignty and protection from foreign political interference,
- addressing growing capabilities of hackers and other malicious actors to exfiltrate sensitive data about consumers and other citizens, and to disrupt supply chains and food security,
- whether, how and for which industry sectors, to facilitate portability of consumer data as a tool to empower consumers to compare offerings and switch between providers of products or services and thereby facilitate disruption of incumbents,
- whether or when to protect and promote 'national champions' against offshore service providers, including global digital platforms, or to otherwise use consumer data as a tool in 'industry policy' regulation to effect structural adjustments within a national economy.

Sometimes it is not even clear which of the above concerns, or whether other concerns, are enlivening a debate about data policy settings, or who needs to be engaged as relevant stakeholders to properly inform a debate.

Data policy debates are therefore no longer 'just about privacy', or principally about data derived from online activity of internet users.

Continuing relevance of and need for data privacy statutes and privacy-focussed regulators does not appear to be seriously contested. However, because operations of businesses, governments and other organisations are increasingly enabled by applications of advanced data analytics and AI, in many jurisdictions national policy makers are actively considering adjustments in the relative roles and functions of consumer protection, competition

[16] See further Janet Chan and Peter Saunders, "Big Data for Australian Social Policy", December 2021, https://2r6hgx20i76dmmstq2nmlon1-wpengine.netdna-ssl.com/wp-content/uploads/2021/12/Big-Data-for-Australian-Social-Policy.pdf

(antitrust) and data privacy (protection) regulators. Some jurisdictions have proposed re-siting of regulatory responsibilities in relation to data privacy. Competition (antitrust) and consumer protection statutes, and the regulators enforcing them, have steadily gained significant status relative to data protection (privacy) statutes. This trend is in part due to primary reliance by regulators upon provisions in competition statutes, or consumer protection statutes, to address policy concerns as to data handling practices of large online platforms and social media networks.[17] Competition powers are now often being used to require large online platforms to implement non-structural safeguards, including operational separation and accountability measures, under the supervision of competition regulators, and not data protection regulators.[18]

Protecting some interests of individuals in data privacy

The Australian Privacy Act 1988 is misleadingly labelled. The Act does not confer a legal right of individuals in and to data privacy. The Act addresses only a subset of the set of rights of privacy of individuals as commonly asserted and as referred to in international conventions and declarations of human rights.[19] The Privacy Act could be more accurately described as the *Data* Privacy Act, where legal protection of data privacy interests of citizens is intermediated by the Australian Information Commissioner.

The Australian Privacy Act is intended to empower individuals by informing them how data about them may be being collected, used and disclosed, and thereby enable them to exercise a choice. The mechanisms to give effect to these objects are variously called 'notice and consent', 'notice and choice', 'individual choice' or 'privacy self-management'. The underlying theory is that an affected individual is afforded 'transparency' as to privacy affecting acts and practices of a regulated entity, and may then make a choice about whether to deal with that entity. The statute:

[17] E.g. in the United Kingdom, "A New Pro-Competition Regime for Digital Markets", consultation paper for UK Parliament, no. CP 489 July 2021; in the U.S.A., David N. Cicilline (RI-01) and Ken Buck (CO-04), 'House Lawmakers Release Anti-Monopoly Agenda for "A Stronger Online Economy: Opportunity, Innovation Choice"', Media Release of 11 June 2021 and accompanying Bills as linked in that Release; House Judiciary Committee, "Judiciary Antitrust Subcommittee Investigation Reveals Digital Economy Highly Concentrated, Impacted By Monopoly Power", Media Release of 6 October 2020 and the Report (Investigation of Competition in the Digital Marketplace: Majority Staff Report and Recommendations) at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf

[18] See for example Rod Sims, ACCC Chair entitled "Competition in Australia faces big challenges" and delivered to the UniSA and ACCC Competition Law & Economics Workshop, 15 October 2021, at https://www.accc.gov.au/speech/competition-in-australia-faces-big-challenges; "UK watchdog in threat to break up US tech giants", UK News Today, 13 November 2021, https://todayuknews.com/banking/uk-watchdog-in-threat-to-break-up-us-tech-giants/; Competition and data protection in digital markets: a joint statement between the [UK] CMA and the [UK] ICO, 19 May 2021 at https://www.gov.uk/government/publications/cma-ico-joint-statement-on-competition-and-data-protection-law; UK Digital Regulation Cooperation Forum, Plan of work for 2021 to 2022, https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122;

[19] See the discussion of human rights law in Australia in Australian Human Rights Commission, Human Rights and Technology Final Report, March 2021

- provides a framework of legal principles that regulated entities are required to comply with as to permitted acts and practices in collecting and dealing with information about identified or identifiable individuals, and
- specifies when and how affected individuals must be informed how data about them may be being collected, used and disclosed.

The Act has limited coverage. Significant sectors of the Australian economy are exempted, including small business, politicians and political parties, media when conducting journalism, persons acting in a personal or domestic capacity, and State and Territory agencies.

Restrictions within the Privacy Act are overridden to the extent a particular act or practice is required by or under an Australia law or a court/tribunal order.[20] Legal compulsion under any other Federal, State or Territory statute, or by subpoena or other court order, prevails over restrictions in the Privacy Act. The Privacy Act does not require a regulated entity, or an authority compelling a disclosure, to weigh reasonable proportionality of the legal compulsion against interests of an affected individual in their data privacy. Some empowering statutes require weighing by an authority of proportionality, or other consideration of balancing factors. Many empowering statutes do not. Many empowering statutes do not require independent review, do not require review by senior management, or judicial consideration, of whether to exercise a proposed legal compulsion. A regulated entity is not required to consult with an affected individual before a disclosure, even where the relevant disclosure would not prejudice investigations or other activities of law enforcement agencies or national security organisations.

The Australian Privacy Act, and similar State and Territory statutes (which address privacy affecting activities of State and Territory government agencies, local government and some private sector providers of health services), address collection and handling of data about identifiable individuals, but not privacy harms that may raise from intrusive and excessive deployment and use of surveillance technologies and geo-tracking devices.[21] A variety of inconsistent State and Territory statutes provide some protections in relation to use of surveillance and tracking devices.[22] Surveillance technologies and geo-tracking devices may capture data about identifiable individuals that is then a collection of personal information regulated by the relevant data privacy statute.

---

[20] A number of the APPs provide an exception if an APP entity is 'required or authorised by or under an Australian law or a court/tribunal order' to act differently: see for example, APP 3.4(a), APP 6.2(b) and APP 12.3(g). Other provisions create an exception for an act that is 'required by or under an Australian law (other than this Act)' (s 16B(2)) or 'required by or under an Australian law, or a court order' (APP 11.2(d)), and do not include an act that is 'authorised'. See also the exceptions in section 16A for "permitted general situations" and in section 16B for "permitted health situations".

[21] See further Queensland Law Reform Commission, "Review of Queensland's Laws Relating to Civil Surveillance and the Protection of Privacy in the Context of Current and Emerging Technologies", Report No 77, February 2020;

[22] Ibid., see also Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era (DP 80), ALRC 2014 at Chapter 13 (Surveillance Devices); Peter Leonard, "Surveillance of Workplace Communications: What are the Rules?", Privacy Law Bulletin, August 2014; Daniel Stewart, Review of ACT Civil Surveillance Regulation, June 2016

A right to know, complain, and elect not to deal: not a legal right of privacy

Accordingly, the privacy statutes address collection and uses of data about individuals, not broader protection of privacy.[23] Instead of conferring a legally enforceable right of individuals in and to data privacy, the Act states as its first two 'objects':

- "to promote the protection of privacy of individuals", and
- "to recognise that the protection of privacy of individuals is balanced with the interests of entities in carrying out their functions or activities".[24]

The Act principally gives effect these objects by requiring affected individuals to be informed how personally identifying data about them will be collected, used and disclosed, and the purpose for which this will occur. Each regulated entity is required to assess the "reasonable necessity" of that act of practice to achieve that stated purpose, and to "balance" their self-interest in collecting and using that data with that entity's assessment of expectations of different sections of the public in "protection of privacy" and the extent to which those expectations are fair and reasonable.

Consistent with this regulatory theory, if data as collected is non-identifying, or as to be used has been transformed so that the data and outputs from analysis of that data is reliably and pervasively deidentified (effectively anonymised), the Act does not operate in relation to uses and disclosure of that effectively anonymised data. That noted, effectively anonymised data may still enable differentiation in treatment between unidentifiable individuals based upon inferences as to activities, interests, preferences and characteristics of those and other ('like') unidentifiable individuals: see further the discussion as to targeted advertising and profiling later in this paper.

The Privacy Act does not specify how a regulated entity should evaluate interests of individuals in protection of data privacy and at what level of privacy impact those interests should be adjudged to be legally protected, legitimate expectations of privacy. Sometimes it is suggested that the appropriate evaluation is whether a particular act or practice will cause a significant privacy harm to individuals. However, the Privacy Act does not state factors that a regulated entity should take into account in determining whether a particular act or practice is reasonably likely to effect a privacy harm.[25]

---

[23] Most data privacy statutes do not define "privacy" and there is as surprising diversity of definitions of "privacy". See further Julie E Cohen, "What is Privacy For" Harvard Law Review Vol. 126 (2013) p 1904-1933; Helen Nissenbaum, "Privacy in Context: Technology, Policy, and the Integrity of Social Life", Stanford, CA, Stanford Law Books, 2010

[24] The rights to privacy as stated in article 17 of the International Covenant on Civil and Political Rights is referenced in the preamble to the Privacy Act, but that right is not expressly conferred in the Australian Privacy Act or elsewhere in Australian domestic law. See objects in section 2A of the Australian Privacy Act, and the discussion of those objects in the Australian Attorney-General's Department Privacy Act Review Discussion Paper, October 2021, at pp 18-20

[25] As to privacy harms, see Peter Leonard, "Privacy Harms: A Paper for the Office of the Australian Information Commissioner", June 2020, available at https://www.oaic.gov.au/__data/assets/pdf_file/0012/1371/privacy-harms-paper.pdf.pdf. See also Normann Witzleb and Moira Paterson, "Privacy Risks and Harms for Children and Other Vulnerable Groups in the Online Environment", paper for the Office of the Australian Information

In any event, the Act requires regulated entities to conduct a balancing of interests. Whenever the law requires balancing of interests, there is contention as to how to strike the appropriate balance. Whenever a regulated entity is required to balance its self-interest against interests of others, self-interest might be considered likely to prevail, and particularly where those others (viz., affected individuals) may not fully understand how their interests are being affected, where detection of inappropriate balancing is difficult, and where enforcement resources are stretched.

In many other jurisdictions, the domestic data privacy (data protection) statute or overarching human rights law provides a foundational legal right of privacy directly enforceable by individuals. For example, many decisions of the Court of Justice of the European Union interpreting and applying the GDPR[26] commence as private litigation, often initiated by prominent privacy advocates such as Max Shrems and Johnny Ryan, and turn on construction and application of Article 8 (Right to respect for private and family life) of the European Convention on Human Rights. Article 8 provides:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence,
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. [27]

Without an overarching foundation or guardrail of a legal right to privacy conferred by domestic statute and enforceable by affected individuals, the Australian Privacy Act is more heavily dependent upon transparency to affected individuals as the key control or safeguard of privacy than is the case for legal rights-based privacy statutes in other jurisdictions.

Key requirements of the Australian Privacy Act

The Australian Privacy Act requires each regulated entity to:

- make available a privacy policy that explains generally how the entity deals with personal information about individuals,

Commissioner, December 2020; Mark J Taylor, "Personal Information and Group Data under the Privacy Act 1988", 2020, 94 ALJ 730; Danielle Keats Citron and Daniel J Solove, "Privacy Harms", forthcoming publication in Boston University Law Review, Vol. 102, 2022, available at http://dx.doi.org/10.2139/ssrn.3782222; Ryan Calo, "The Boundaries of Privacy Harm", 86 Indiana Law Journal 1131, 2011; Ryan Calo, Privacy Harm Exceptionalism, 12 Colo. Tech. L.J. 361, 2014

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council on 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[27] See further the extensive caselaw referenced and discussed in European Court of Human Rights, Guide on Article 8 of the Convention, "Right To Respect for Private and Family Life", updated on 31 August 2021, at https://www.echr.coe.int/documents/guide_art_8_eng.pdf

- collect personal information only as is reasonably necessary for one or more of the entity's functions or activities,
- take such steps as are reasonable in the circumstances to notify affected individuals of the purposes for which the APP entity collects personal information (commonly referred to as the purpose limitation, and common across many jurisdictions),
- only use personal information for that notified purpose and related secondary purposes (commonly referred to as the secondary uses limitation, and also common across many jurisdictions), or otherwise only with informed consent of the affected individual,
- collect personal information about an individual only from that individual, unless it is unreasonable or impracticable to do so, or otherwise only with informed consent of the affected individual,
- obtain consent in relation to collection and uses of certain narrower categories of more 'sensitive' personal information.

The legal requirements as to 'reasonably necessary' and stated 'purpose' operate as significant constraints upon APP entities. It is therefore incorrect to characterise the Privacy Act as principally reliant on privacy self-management by users. However, the balance between privacy self-management by users, and self-responsibility and accountability of APP entities, is heavily weighted towards the former.

Entity accountability and multiparty data ecosystems

Over the last decade data privacy reforms across the globe have rebalanced legislated privacy settings towards greater accountability of regulated entities that collect and control personal information in relation to their own acts and practices. Reform of the Australian Privacy Act can be confidently expected to follow this trend.

Many jurisdictions have recognised a distinction between 'data controllers', being entities that collect and control personal information about individuals, and data processors, being entities that process that personal information on behalf of data controllers in circumstances where the control as to subsequent uses and disclosures of that information remains with the data controller. Those jurisdictions typically require the data controller to implement contractual safeguards and take active steps to monitor the activities of those data processors when processing personal information on their behalf. However, those jurisdictions typically do not require data controllers to actively monitor activities of entities to whom they disclose personal information where that disclosure is with the consent of the affected individual and the information then leaves the discloser's effective control.

The Australian Privacy Act does not recognise a controller-processor distinction. Regulatory guidance by the Australian Information Commissioner uses a concept of "effective control" in drawing a distinction between a third party "use" of personal information at the direction of a regulated entity, and provision of personal information to a third party which then is no longer acting under the direction or control of the regulated entity, being a "disclosure".[28] A

[28] See Office of the Australian Information Commissioner (OAIC), Australian Privacy Principles guidelines, July 2019, para 8.8, B.64, https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines

more recent trend in some jurisdictions has been imposition of legal accountability upon entities that curate or otherwise enable multiparty data ecosystems to monitor and control privacy affecting activities of other entities within those multiparty data ecosystems, regardless of whether those other entities are data processors or data controllers in relation to relevant personal information. Various legal theories of responsibility and accountability of entities for acts and practices of others have been invoked, including legal theories analogous to the broad legal concept of "knowingly concerned" (sanction, approve or countenance) as used in Australian Consumer Law.[29] One key issue in reform of Australian data privacy law is how to address responsibility and accountability of entities that curate or otherwise enable multiparty data ecosystems.

The illusion of (transparency and) consent[30]

Critiques of privacy self-management mechanisms, particularly as applied to internet enabled services, focus upon:

- the impracticability of individuals reading and understanding privacy policies and requests for consent, given the volume and complexity of privacy policies and collection notices,
- 'notice and consent fatigue', leading to users simply clicking the 'I agree' button without perusing or thinking about the privacy related terms.[31]

Many criticisms revolve around the problem of expecting affected individuals to properly understand and make a choice about whether to accept an act or practice which affects the individual's privacy. An informed understanding requires willingness of an affected individual to engage with explanations as to the *why* and *how* of collection, use, and sharing of personal

[29] Under the Corporations Act 2001 (section 79), Fair Work Act 2009 (section 550) and ACL (section 2), a person (including a company) will be "involved" in a breach of the respective statutes where that person has aided, abetted, counselled or procured the contravention; or induced, whether by threats or promises or otherwise, the contravention; or been in any way, by act or omission, directly or indirectly, knowingly concerned in, or party to, the contravention; or has conspired with others to effect the contravention. See further Australian Competition and Consumer Commission v Joystick Co Pty Ltd [2017] FCA 397; Yorke v Lucas [1985] HCA 65 [9].

[30] Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", 57 UCLA L. Rev. 1701, 2010;Paul Ohm, "Changing the Rules: General Principles for Data Use and Analysis", in Lane, Julia I., Privacy, big data, and the public good : frameworks for engagement, New York: Cambridge University Press, 2014, pp 96-111;Daniel J Solove, "Privacy Self-Management and the Consent Dilemma", Harvard Law Review 126, 2013, pp 880–903;Daniel Susser, "Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't", Journal of Information Policy, Vol. 9, 2019, pp 37-62

[31] See further Peter Leonard, "Notice, Consent and Accountability: Addressing the Balance Between Privacy Self-Management and Organisational Accountability: A paper for the Office of the Australian Information Commissioner", June 2020, https://www.oaic.gov.au/__data/assets/pdf_file/0012/1371/privacy-harms-paper.pdf.pdf; Future of Privacy Forum (FPF) and Personal Data Protection Commission (PDPC) of Singapore, Event Report: From "Consent-Centric" Frameworks to Responsible Data Practices and Privacy Accountability in Asia Pacific, 28 September 2021, https://fpf.org/blog/event-report-from-consent-centric-frameworks-to-responsible-data-practices-and-privacy-accountability-in-asia-pacific/; Kayleen Manwaring, Katharine Kemp and Rob Nicholls (mis)Informed consent in Australia, 31 March 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3859848; Ian Warren and Dr Monique Mann, Enhancing Consumer Awareness of Privacy and the Internet of Things, ACCAN and Deakin University, August 2021, https://accan.org.au/grants/grants-projects/1611-regulating-the-internet-of-things-to-protect-consumer-privacy; Radha N Pull ter Gunne, "The Illusion of Control", (2020) 48 ABLR 424

information. Explanations provided by service providers are often technically complex. Often the counter-factual – any adverse effect on availability, quality or relevance of an internet service that an affected individual will experience if the individual does not allow data collection and uses as proposed by a service provider – is not clearly stated by the service provider. If an individual cannot understand the counter-factual, is a clear statement as to a proposed data sharing sufficient to demonstrate individual choice to permit a relevant data flow? Individual choice requires options and informed understanding as to the consequences of exercising them.

Options offered to internet users also need to be readily exercisable. If options as to privacy settings are difficult to find and exercise, are they 'real' options? Some internet services offer little practical ability for a user to say *no*, or even to say *no to that, but it might be OK if you did it this other way*.

Doubling down on consent

Some critiques suggest that the legislature should extend the categories of acts and practices for which consent is required, as well as cranking up the requirements for a valid consent. These critiques often cite with approval the EU GDPR concept of 'unambiguous express consent'.[32] When faced with the response that such changes risk increasing the clamour for consent and resultant consent fatigue, some critics say that the impracticability of obtaining heightened consents would create disincentives for organisations from seeking consent, with an outcome of limiting privacy affecting acts and practices of regulated entities.

Those alleged disincentives may be overstated. Jurisdictions such as Korea that had long standing prescriptive requirements for much more granular and frequent requests for consent have not demonstrated any significant difference in privacy affecting acts and practices of regulated entities within Korea, as compared to other, less prescriptive, jurisdictions.

The 'consent problem' under Australian data privacy law is not as acute as in other jurisdictions that have incentivised over-reliance by data controllers upon consent, in turn leading to further erosion of the value of consent.

We should continue to contest whether and when requiring consent is sensible. We should ensure that enhancements in practical options for individuals to control their privacy settings are not compromised by any change in consent requirements. Consent should only be required, and sought, where it can be given thoughtfully, sparingly and with understanding. Consent is only 'real consent' where an individual has a real choice.

[32] Consent is defined in Article 4(11) as: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". See further European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en; UK ICO, "What is valid consent?", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/

Winding back requirements as to consent, to achieve an objective of improving data privacy, may sound both radical and counter-intuitive.

Both consent fatigue and notice noise fatigue are real. Many proposals for reform of data privacy law risk doubling down on both the consent problem and the noise of policies and notices problem, casting the net too widely. We need to make consent meaningful, again.

(Selective) noise reduction

We also need to reduce the level of noise in privacy policies and privacy (collection) notices.[33] Many privacy policies and privacy (collection) notices are long on statement of 'the bleeding obvious' and drown, in an ocean of text, explanation of the unusual, the unexpected or the odd. For many categories of internet services, it is relatively obvious what collections and uses of personal information that are a reasonably necessary incident of provision of that service, or of offsetting the cost of provision of a no-charge or cross-subsidised service. Most consumers will understand the points value-for-data exchange inherent in card loyalty programs, including programs offering special rewards, premium features, discounts and or privileges. Statement of 'the bleeding obvious' should not be permitted to distract attention from the unusual, the unexpected or the odd.

In particular, attention of consumers should be directed towards a full and fair explanation by a collector of personal information as to sharing of that information into multi-party data ecosystems in circumstances where the entity making a disclosure statement is not in continuing control of uses and further disclosures by other entities in that data ecosystem.

Accountability of data collectors depends upon full transparency as to data sharing practices. We need to ensure that each entity in multi-party data ecosystems through which personally identifying information about individuals may pass has appropriate incentives:

- to handle that information responsibly and transparently,
- to not pass on information without applying appropriate controls, and in particular to not to pass on information in a form that might reasonably be anticipated as facilitating misuse of that information by the recipient.

The right and ability of internet users to self-manage privacy settings remains important.

However, each individual should only be expected to self-manage what is realistically manageable by her or him. We should consider how to reduce the clamour of consent requests, and how to reduce the level of noise (length, technical complexity, coverage of unimportant and obvious subject matter) of privacy policies and collection notices. Noise reduction measures might include appropriately targeted exceptions, such as through legitimate interests or legitimate uses or 'compatible data practices'[34], or sector or

[33] See further Peter Leonard, "Notice, Consent and Accountability: Addressing the Balance Between Privacy Self-Management and Organisational Accountability: A paper for the Office of the Australian Information Commissioner", June 2020 and references there cited

[34] See Section 7 (Compatible Data Practice) of the Uniform Personal Data Protection Act as drafted by the U.S. Uniform Law Commission, https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=009e3927-

application specific codes or standards, class exemptions by regulators, trust marks and certification schemes,[35] standardisation of language and use of graphics or other user-friendly transparency measures.

Bringing it together and the role of transparency

Transparency is of course appropriate for data subjects that want to read privacy policies and collection notices. However, no sensible human should be expected to read all that stuff. We need new thinking as to the purposes of privacy policies and collection notices. We need less noise and clutter in our lives. Does it matter if many people don't read privacy policies and collection notices, provided that regulators, civil society organisations and potential litigants are able to do so?

However, any exception for legitimate interests, legitimate uses or 'compatible data practices' should only operate and allow a regulated entity to collect, handle or disclose personal information about individuals without consent if the processing is aligned with the ordinary expectations of affected individuals, having regard to transparent privacy policies and notices, and not harmful to direct interests of data subjects. In particular, permitted primary purposes of collection and handling of personal information about individuals should remain subject to transparency requirements. Laws addressing fair disclosure, in terms readily understood by a reader of not unusual literacy, are a powerful deterrent against excessive or unduly intrusive data privacy practices.

Bridging the accountability gap: 'fair and reasonable' practices and organisational accountability

Contest as to the effectiveness of data privacy law partly arises because many regulated entities have elected to adopt either a 'catch us if you can', or a 'tick-the-box', strategy in addressing their purported compliance with data privacy law.

Many regulated entities consider privacy risk management as another exercise in form over substance, only providing 'transparency' through buried and opaque disclosures of their privacy affecting acts and practices.

Many data protection regulators are under-resourced, so enforcement action must be selective. Regulators have also been required to divert limited resources to address year on year increases in the number and complexity of data breaches[36], and to investigating and

---

eafa-3851-1c02-3a05f5891947&forceDialog=0 and https://fpf.org/blog/uniform-law-commission-finalizes-model-state-privacy-law/

[35] As in Japan, New Zealand and Singapore: Japan's PrivacyMark System is described at https://privacymark.org/; New Zealand's Privacy Trust Mark at https://www.privacy.org.nz/resources-2/applying-for-a-privacy-trust-mark/; and Singapore's Data Protection Trustmark at https://www.imda.gov.sg/programme-listing/data-protection-trustmark-certification. See also Privcore, Privacy Certification Research for the Australian Information Commissioner, June 2020, https://www.oaic.gov.au/__data/assets/pdf_file/0022/1786/privacy-certification-research.pdf.pdf

[36] See Office of the Australian Information Commissioner (OAIC), Notifiable data breaches statistics, at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics

addressing a variety of concerns as to data handling practices of large online platforms and social media networks.[37]

One criticism of the Australian Privacy Act, and data privacy statutes of comparable jurisdictions, is that they do not adequately bridge the gap between ensuring:

- that there is 'transparency': a fair description is created and provided to an affected individual about the purpose and extent of a proposed data collection, use or disclosure or surveillance activity, and
- that this data collection, use or disclosure or surveillance activity is necessary and proportionate to achieve a reasonable outcome, with reasonableness judged by consideration of:
  - the degree of risk and extent of impact upon legitimate expectations of privacy,
  - whether any individual is reasonably likely to suffer a harm that arises from this act or practice,
  - societal interests, including in health and safety of other individuals and in secure, safe and efficient operation of the internet, and
  - the interests of the regulated entity that wants to collect, use or disclose data and insights derived from analysis of personal information about individuals in a properly risk managed way.

Critiques often suggest that privacy self-management mechanisms need to be supplemented, or replaced, by:

- an over-arching legal requirement of fairness or reasonableness,[38]
- demonstrated organisational accountability of the entity that is collecting, handling or disclosing personal information about an affected individual.[39]

Differential treatment of individuals: scoping the role for data privacy law

One major impetus for overhaul of the Australian Privacy Act and comparable statutes in other jurisdictions is increasing concern about use of personal information about individuals for differentiated treatment of those individuals.

Advances in transactor and transaction analytics, shift to online transactions, take-up of non-conventional internet enabled devices such as personal wellness devices and smart speakers, and deployment of and rearchitecting of data platforms, have fuelled ever more sophisticated ability of service providers to use consumer data to single out an individual for differential treatment. If a supplier has reasons to single out a person - to deal, or not deal, or for a more or less favourable offer – this differentiated treatment is often possible without needing to know the identity of the person that is singled out. If a supplier takes care not to know, and

[37] See Future of Privacy Forum and Nymity, Processing Personal Data on the Basis of Legitimate Interests under the GDPR: Practical Cases, CIPL, "How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation", July 2021; Personal Data Protection Commission (Singapore), Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Chapter 12, The Consent Obligation, pp 66-75

[38] See AGD Privacy Review Discussion Paper, pp 82-93

[39] See discussion above under the heading "Entity Accountability and Multiparty Data Ecosystems"

not to be able to work out, who it is that is being singled out, current Australian data privacy law generally doesn't regulate that singling out, or specify permissible reasons for singling out, because there is no relevant use of personally identifying information about individuals.

Differentiated treatment may be benign (positive or neutral) or have negative effects upon an affected individual. Often differentiation enables presentation of content, choices or offers that have been selected for inferred relevance or convenience. Search engines, marketplaces and comparison sites use algorithmic inferences to differentiate between users to promote presentation of particular content or choices inferred more likely to be of interest to a user (whether or not identifiable), often with the positive effect of reducing that user's search time and effort. Regardless of operation of data privacy law, other laws limit the reasons that may motivate a supplier to single someone out for differential treatment.

An increasing variety of topic and sector specific statutory provisions regulate particular reasons for differential treatment, including laws about discrimination, consumer protection, targeting of children, tracking and surveillance, disinformation and misinformation.

One key issue for reform of the Australian Privacy Act is scoping the role for this statute in regulating profiling: specifically, what should be regulated under this statute as a use of data in relation to an individual to single out that individual for differential treatment, and what is better addressed by Australian Consumer Law, financial services laws or other topic-specific and sector-specific laws?[40]

Even for particular applications of profiling in relation to which a policy choice is made that the Privacy Act is the right regulatory tool to address and control a particular act or practice, it may be difficult to structure the right package of new data privacy rules. A change in one area of data privacy law, such as by broadening the definition of personal information, may have substantial knock-on effects in other areas, such as increasing the complexity of technical information that needs to be disclosed, placing further stress upon consumer understanding of privacy policies and notices. Changes to settings within the Privacy Act requires consideration of the effect of a change upon the balancing of interests of regulated entities in conducting their business operations and addressing interests in privacy of affected individuals.

[40] See further Gregory Crawford et al, "Consumer Protection for Online Markets and Large Digital Platforms", Tobin Center for Economic Policy at Yale, Digital Regulation Project Policy Discussion Paper No. 1, 2021; Johann Laux, Sandra Wachter and Brent Mittelstadt, "Neutralizing Online Behavioural Advertising: Algorithmic Targeting with Market Power as an Unfair Commercial Practice", Common Market Law Review Vol. 58(3), 2021, pp 719-750;Kayleen Manwaring, "Will Emerging Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation", Competition and Consumer Law Journal, 2018, Vol 26(2), pp 141-181;Kayleen Manwaring, "Emerging Information Technologies: Challenges for Consumers", Oxford University Commonwealth Law Journal, 2017, Vol. 17(2); Damian Clifford and Jeannie Paterson, "Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law", 2020, 94 ALJ 741; Katherine Kemp, 2020, "Concealed data practices and competition law: why privacy matters", European Competition Journal, pp. 628-672, https://www.tandfonline.com/doi/pdf/10.1080/17441056.2020.1839228; Australian Treasury, Consultation on strengthening protections against unfair contract terms, August 2021, https://treasury.gov.au/consultation/c2021-201582

A key area of significant controversy is how data privacy regulation and regulators should address the most common form of algorithmically enabled differential treatment of internet users, being targeted ('programmatic' or 'personalised') digital advertising.

Targeted digital advertising as a form of profiling

Examples of digital advertising activities include:

- using information volunteered by a known (identified) consumer about their needs, preferences or interests to select and present tailored offers: for example, marketing by loyalty card program partners to card members based upon their membership data and their interactions with other program partners,
- using observations of a consumer's interactions with a website (for example, searching on a travel website for flights to Cairns) to select and present offers tailored to meet a consumer's characteristics, needs, preferences or interests as inferred from those interactions (i.e., snorkelling gear, sunglasses and reef cruises),
- using advertising services based upon entry of search terms (i.e. a search for new kayak Sydney) to deliver advertisements to consumers searching for a related item (for example, new double kayaks, life vests and paddles available in Sydney).

Digital advertising using audience segments enables 'personalisation', in the sense that a group of identified users receive digital ads targeted to address their needs, preferences or interests. However, the digital ad is not tailored to a particular recipient, and a recipient does not need to be personally identified. Advertisers use ad networks and other adtech intermediaries to target ads to users based on characteristics such as their online behaviour, physical location, or demographics. Behavioural targeting shows ads to users based on their online activity, such as past searches or browsing history. Location-based ads target users based on where they live or when they visit a specific location, such as a stadium or shopping centre. Demographic targeting shows ads to users based on specific social categories (brackets) such as gender, income, level of activity or age.

Some adtech intermediaries also allow advertisers to target ads to custom audiences, such as previous customers. Adtech intermediaries collect data about users to create these segments, to enable these personalized ads and to measure their efficacy. 'Personalisation' is typically through creation and use of an audience segment, not individual targeting of individuals within that audience segment: for example, an adtech intermediary may offer to advertisers the ability to target thousands of internet users inferred to be interested in water sports, addressable by the adtech intermediary enabling serving of ads to users that may or may not be identifiable, using technical information such as tracking codes of internet access devices and browsers. Audience segments as used in personalised digital advertising are intended to be fit for purpose on an aggregated basis, but at the cost of some outliers: that is, over-inclusion of some codes for which the 'personalisation' is not right. This 'outlier cost' often arises because an advertising services provider does not know the identity of a user, or specifics of a particular user's browsing of searching activity over time or across devices. In other words, accuracy in targeting is lost through deidentification, inferences and

aggregation. However, there are privacy protective benefits of deidentification, inferences and aggregation, including:

- minimisation of collection and use of identifying details about people using internet services and browsers and devices used to interact with those services;
- minimisation of sharing of data about users of internet browsers and devices: for example, an adtech services provider could offer to serve a digital ad to thousands of users of internet browsers and devices that are inferred to have an interest in outdoor water sports, without the service provider disclosing to the advertiser or the advertiser otherwise knowing the identity of these individual users or any specifics of those users' online activity.

Adtech intermediaries generally do not share personal information about individuals with advertisers. However, some operators of internet sites (publishers) collect and share personal information with adtech intermediaries, or do not monitor or control collection of personal information from their internet sites by adtech intermediaries with whom they work. Some adtech intermediaries obtain personal information from advertisers, or share personal information back with advertisers. In short, there are differing levels of compliance across the digital advertising sector with requirements and restrictions as to necessity, purpose and transparency.

Regulators around the world have expressed concerns:

- that adtech is not configured to minimise use and disclosure of personally identifying information, and
- that internet users lack transparency, understanding and control as to when and how their internet interactions are being tracked for the purpose of targeted advertising,
- that the manner of presentation and content of privacy policies, notices and requests for consent do not adequately address likely user behaviours and capabilities.[41]

Some publishers and digital advertising service providers have responded to these concerns. Responsive measures include improvements in clarity, simplicity and prominence of notices to internet users about ad targeting, new options for users to change tracking settings, and expanding the subject matter categories of digital ads that they do not permit.

Other publishers and ad service providers have been slower to respond. To date, demonstrably reliable and verified implementation of good privacy practices, including privacy by design and default, have not been widely regarded as differentiators for business success and as a result, over-sharing of personal information about individuals has been

[41] See for example UK ICO, "Information Commissioner's Opinion: Data Protection and Privacy Expectations for Online Advertising Proposals", 25 November 2021, https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf; UK Competition and Markets Authority, "CMA Secures Improved Commitments on Google's Privacy Sandbox", 26 November 2021

common. However, this is now changing across multiple jurisdictions, through the combination of:

- consumer organisations and regulators exerting pressure upon both publishers and adtech intermediaries to adopt more privacy protective practices,
- focus of regulators broadening from acts and practices of the global digital platforms, to include scrutiny of activities of other entities within the digital advertising sector, and
- improvements in data architectures and governance that increasingly enable less identifying information to be gathered or shared while still enabling targeted digital advertising.

In particular, adtech intermediaries are re-architecting data handling and investing in new technologies to address over-sharing of personal information, deliver more relevant ads, and prevent ad fraud. Over recent years the adtech sector has been working on transparency and accountability frameworks for sharing of attribute data across multiparty ad data ecosystems.

IAB Tech Lab Rearc is one example of a federated model, where each entity enabled into an ad data ecosystem would commit to transparency requirements, to observe use restrictions, to follow technical standards and assure 'privacy by default' addressable advertising and measurement.

Other proposals include substitution of tracking codes and device codes for what is variously called common ID, stable ID or universal ID. Universal ID proposals claim to provide a means by which the identity of a user, internet device or browser can be protected against being reverse engineered to a form of identification of a user. For example, the Prebid.org User ID Module would enable a publisher to permit any one or more of a variety of proprietary sub-modules ID generators, including the TradeDesk-sponsored Unified ID (UID) 2.0, Verizon Media ConnectID, and TapadID, which in turn would transport or regenerate the common pseudonymous ID across other solutions. This would facilitate cookie-less tracking of interactions by a unique pseudonymised user with publishers that are unrelated with each other, and also across publishers working with a variety of different adtech solution providers.

One way to address perceived intrusiveness would be to move away from creation of audience segment cohorts for targeted ads through direct correlations based upon observation of browsing behaviour of individuals. Google is currently seeking feedback through its Privacy Sandbox initiative on a number of alternative technical implementations of Federated Learning of Cohorts (**FLoC**), whereby a user's browser is associated with a value, alongside thousands of others with a similar browsing history, which is updated over time as the collective cohort of users traverse the internet. That value, and not the user's actual browsing behaviour, is used to target ads.[42]

FLoC is technologically complex. An individual's browser generates inputs to machine learning algorithms that develop a cohort based on thousands of individuals' interactions, analysing URLs of the visited sites, content of pages visited, and other factors. Input features to the

[42] Chetna Bindra, Building a privacy-first future for web advertising, Google blog post, 25 January 2021, https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/

algorithm, including the individual's browsing history, are kept local on the browser and are not uploaded. The user's FLoC is updated over time, so that it continues to have advertising utility, but (when implemented with appropriate controls) not at a frequency and without granularity of analysis that would enable direct correlations with a user's internet activity. Controls could include the ability for a publisher to opt-out of inclusion in the user's list of sites for cohort calculation, individual users to opt-out of inclusion within any cohort, restrictions as to uses of categories of sensitive information in creation of cohorts, and no-go zones, such as browsers used by young children.

FLoC implementations do not of themselves ensure responsible data governance by entities within multiparty ad data ecosystems. However, they would significantly reduce the collection and centralisation of data about an individual's internet activities, which substantially reduces availability of that data to entities within multiparty ad data ecosystems, thereby mitigating the risk of misuse of data about internet activities.

Some consumer advocates argue in favour of new legal restrictions as to profiling that go well beyond existing data privacy laws. These concerns are often framed not in terms of compliance with data privacy law, but in more emotive terms, such as that "surveillance-based advertising" renders consumers "vulnerable to manipulation, discrimination, misinformation and fraud".[43] Some of these proposals do not differentiate between segmentation of audiences for targeting of ads – that is, delivery of purely expressive content to a cohort of internet users with inferred like interests – and differentiation between users for the purpose of determining terms of dealing with an individual in relation to supply of a particular product or service.

UNSW Law Professor Katharine Kemp recently suggested[44] that sharing of targeting data should be unlawful unless a consumer ticks an unticked box next to a plain message, such as: "Please obtain information about my interests, needs, behaviours and/or characteristics from the following data brokers, advertising companies and/or other third-party suppliers", with each entity named. Professor Kemp also suggested that collection should not be exempt from this rule "simply because the companies use a pseudonym or unique identifier, rather than the consumer's given name or contact details, to link data collected by the marketplace with data about the same consumer collected by a third party". Such proposals would effectively preclude targeted advertising using pervasive tracking and data sharing between adtech intermediaries, whether or not using demonstrably effectively anonymisation, unless there had been an affirmative and express consent by a consumer, and then only as between entities named in that consent. Such proposals loop the debate back to the issue of consent

[43] Examples include Norwegian Consumer Council, "Time to Ban Surveillance-Based Advertising: The Case Against Commercial Surveillance Online", June 2021; https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf; Duncan McCann, Will Strong and Phil Jones, The Future of Online Advertising, October 2021

[44] Katherine Kemp, "How One Simple Rule Change Could Curb Online Retailers' Snooping On You", The Conversation, August 17, 2021, https://theconversation.com/how-one-simple-rule-change-could-curb-online-retailers-snooping-on-you-166174

fatigue of consumers, and whether it is reasonable to expect consumers to engage in understanding complex adtech processes.

'Purely expressive' content and 'compatible uses'

Clearly, differentiation in terms of offer involves significant risk of unfair or illegal price discrimination, or even refusal to deal. But does the former – audience segmentation for delivery of purely expressive content to a cohort of internet users with inferred like interests –raise significant consumer protection concerns?

Reflecting this distinction, the US Uniform Law Commission's Uniform Personal Data Protection Act, published as a model law for US State legislatures, draws a distinction between compatible business practices (processing that "is consistent with the ordinary expectations of data subjects or is likely to benefit data subjects substantially"), which do not require a data subject's consent (but are still subject to transparency requirements), and incompatible business practices, for which either consent is required or are described "in a reasonably clear and accessible privacy policy" as a practice "that, unless the data subject withholds consent, will be applied by the controller or an authorized processor to personal data".[45]

The model statute provides that a controller may use personal data, or disclose pseudonymised data to a third-party controller, to deliver targeted advertising and other purely expressive content to a data subject. However, a controller may not use personal data or disclose pseudonymised data to be used to offer terms, including terms relating to price or quality, to a data subject that are different from terms offered to data subjects generally: this is an incompatible data practice that requires consent, unless otherwise excepted.[46]

Another exception addresses loyalty programs that use personal data to offer discounts or rewards: "although the targeted offering of discounts or rewards would constitute decisional treatment, these are accepted and commonly preferred practices among consumers. ...This subsection does not prevent providing special considerations to members of a program if the program's terms of service specify the eligibility requirements for all participants."[47]

Profiling beyond targeted advertising

Some forms of profiling-based differentiation in terms of offer involve significant risk of unfair or illegal price discrimination, or even refusal to deal. But many uses do not. An online supplier may infer the characteristics of a product or service likely to be of interest to an online user and present that user with an offering with those characteristics more quickly, or with greater prominence. 'Noise' from multiplicity of possible options is thereby decreased, with benefit to the consumer.[48]

[45] Section 6(a)(4) (Privacy Policy), Uniform Personal Data Protection Act; see also the commentary by the Future of Privacy Forum at https://fpf.org/blog/uniform-law-commission-finalizes-model-state-privacy-law/
[46] Ibid., Section 7(c) (Compatible Data Practice)
[47] Ibid, Explanatory Note to Section 7(c) (Compatible Data Practice)
[48] Subject to concerns that may arise from 'echo chambers' or other 'tunnelling': for one expression of these concerns applying human rights principles, see Fish, Eran and Gal, Michal, "Echo Chambers and Competition

Or a supplier may use similar data analytics capabilities to infer that an online user is less price sensitive, and elect not to offer that user as attractive a price as may be offered to other online users that are inferred to be more price sensitive.

Or a supplier may classify a user into a cohort of inferred like individuals as an exclusion audience. Consider offer of community-rated insurance products, where an insurer has an incentive to only actively market a product to those sections of the public likely to take up the product not less likely to make a claim under a policy. If a health insurance product can be marketed only to an audience segment that is inferred from their recent purchases to be physically active young people (regardless of their identity, and although that inference may be wrong in a statistically insignificant number of cases), the offer of that health insurance product may be much more profitable than if that same product is offered at that same price through broadcast media such as free-to-air television. Targeting through data inference may fundamentally alter profitability of a product or service.[49]

The Australian Attorney-General's Department's Privacy Act Review Discussion Paper

The AGD's Privacy Act Review Discussion Paper of October 2021[50] follows the AGD's Review of the Privacy Act 1988 (Cth) – Issues paper of October 2020[51] and references many of the approximately 200 submissions[52] made in response to the Issues Paper.

The Discussion Paper consisted of 217 pages of recommendations and rationale for those recommendations and 1,505 footnotes. It presents what might be regarded as a menu card of possible reforms and also poses further questions for submissions by interested parties.

As at the date of writing this paper (12 January 2022), the consultation processes were ongoing.

Many of the reforms discussed in this Discussion Paper might reasonably be characterised as:

- technical, better aligning substantive provision of the Act with guidance and interpretations issued by the Australian Information Commissioner,
- effecting closer alignment of Australian federal data privacy regulation with EU GDPR: for example, changing requirements for valid consent from allowing inferred consent to alignment with the GDPR standard of 'unambiguous express consent'.

The Discussion Paper proposed to continue the focus of Australian data privacy regulation upon transparency to affected individuals, but with proposals for:

Law: Should Algorithmic Choices be Respected?" (March 16, 2020), in Frederic Jenny Liber Amicorum: Standing Up for Convergence and Relevance in Antitrust, Vol. II, 2020, available at SSRN: https://ssrn.com/abstract=3555124

[49] For an interesting analysis of possible regulatory responses to impact of AI and advanced data analytics in the insurance sector, see Zofia Bednarz and Kayleen Manwaring, "Insurance, Artificial Intelligence and Big Data: Can Provisions of Ch 7 of the Corporations Act Help Address Regulatory Challenges Bought About By New Technologies?", 2021, 36 Australian Journal of Corporate Law 216

[50] Available at https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/

[51] https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper

[52] https://www.ag.gov.au/integrity/publications/submissions-received-review-privacy-act-1988-issues-paper

- ratcheting up the requirements as to both extent and comprehensibility of notice, and
- shifting of emphasis upon form of disclosure from privacy policies and associated privacy centre materials and towards more fulsome collection (privacy) notices, presumably with continued coupling with vigorous enforcement by the Australian Competition and Consumer Commission of its consumer protection powers and in particular the misleading and deceptive conduct prohibitions under Australian Consumer Law. This would continue, and increase, the significant regulatory jeopardy for regulated entities in relation to collection and uses of consumer data, because compliance with expanded transparency requirements carries risk that disclosures will be misleading or deceptive by omission or misdescription, as illustrated by the decision of Mr Justice Thawley of the Federal Court of Australia in *Australian Competition and Consumer Commission v Google LLC* (No 2) [2021] FCA 367.

Other reforms canvassed in the Discussion Paper are more far-reaching. If taken together and enacted, there would be a radical shift of Australian federal privacy regulation towards positions that have been long advocated by consumer organisations and privacy advocates.

Proposals include:

- New requirements in relation to secondary uses of personal information, and derived information from personal information, for 'profiling' of users. What is, or is not, 'profiling' is not clearly articulated, but profiling is very broadly described.[53]
- "An unqualified right to object to collection, use and disclosure for direct marketing".
- A broad opt-out right exercisable by affected individuals in relation to uses and disclosures of personal information, not only in relation to targeted online advertising or other forms of direct marketing and potentially including non-identifying 'profiling'.

[53] As already noted, there is contention between Australian privacy laws experts as to the range of circumstances in which derived transactional data or behavioural inferences which may be used for differentiated treatment of non-identified individuals should be regulated as profiling under the Australian Privacy Act, or whether such differentiation should be addressed to the extent considered a consumer protection concern, by Australian Consumer Law. See further Kayleen Manwaring, "Will Emerging Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation", Competition and Consumer Law Journal, 2018, Vol 26, Issue 2, pp 141-181; Kayleen Manwaring, "Emerging Information Technologies: Challenges for Consumers", Oxford University Commonwealth Law Journal, 2017, Vol. 17(2), available at https://ssrn.com/abstract=2958514; For an expansive view as to the role for data privacy law, see Salinger Privacy, The Definition of Personal Information, Research Paper for the Office of the Australian Information Commissioner, 17 February 2020, https://www.oaic.gov.au/__data/assets/pdf_file/0012/1308/definition-of-pi.pdf.pdf; Katharine Kemp, "How One Simple Rule Change Could Curb Online Retailers' Snooping On You", The Conversation, 17 August 2021, https://theconversation.com/how-one-simple-rule-change-could-curb-online-retailers-snooping-on-you-166174; Anna Johnston, "Individuation: Re-Imagining Data Privacy Laws to Protect Against Digital Harms", Brussels Privacy Hub Working Paper Vol 6 No 24 (July 2020), https://brusselsprivacyhub.eu/publications/wp624.html. For international perspectives, see Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), https://ec.europa.eu/newsroom/article29/items/612053; UK ICO, "What Is Automated Individual Decision-Making and Profiling?", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/.

- Changes affecting provision of services directed to users likely to be under 18 years of age, including potential no-go zones as to online targeting of children and uses of geo-location data relating to activities of children.
- A new 'fair and reasonable' test (that cannot be consented out of).
- No-go zones, including powers for the regulator to determine the extent of no-go zones.
- Ability for the regulator to effectively force industry sectors to develop industry codes within tight time frames or be subject to imposition of a mandatory code determined by the regulator, with limited requirements as to consultation by the regulator with affected covered entities. These industry codes would take effect to supplement substantive requirements directly imposed by provisions of the Privacy Act and activate the enforcement and penalty provisions of the Privacy Act, effectively equating force and effect of provisions of industry codes with substantive requirements directly imposed by provisions of the Privacy Act.
- Ability for the regulator to determine what it considers to be high risk processing environments that require enhanced privacy assessments and risk/harm mitigations.

'Minding the gap' in data privacy impact assessments

Data privacy regulation, when properly applied, should lead to a contextual assessment by each regulated entity of risks of privacy harms to individuals that may arise from acts and practices in collection and handling of data relating to persons with whom that entity deals or otherwise interacts.

A key methodology for this contextual assessment is conduct by regulated entities of data privacy impact assessment (**DPIA**).

Conduct of a DPIA is becoming a key feature of responsible and accountable governance and assurance of data privacy of affected individuals, including in circumstances where conduct of a DPIA is not legally mandated.

DPIAs are hard to do well. Often they are not done well. This shortcoming is increasingly problematic because DPIAs are now being repurposed as a mechanism for algorithmic or AI impact assessments, which are of necessity more complex and multifaceted than data privacy risk assessment. Given the complexity, range and relative novelty of risks and possible mitigations that should be evaluated and addressed in a comprehensive algorithmic or AI impact assessment, it is important to ensure that DPIAs are properly adapted and applied to this new purpose.[54]

[54] To date there are relatively few published examples of fully developed tools for AI risk assessment and assurance. Many examples take the form of checklists or questionnaires rather than assurance frameworks. In December 2021 the NSW Department of Customer Service published an AI assurance framework which NSW government agencies will be required to apply from March 2022 to assess all significant projects that use bespoke artificial intelligence systems before deployment: NSW Government, NSW AI Assurance Framework, available at https://www.digital.nsw.gov.au/policy/artificial-intelligence/nsw-ai-assurance-framework. See also Emmanuel Moss and ors, "Assembling Accountability: Algorithmic Impact Assessment for the Public Interest", Data and Society, June 2021, https://datasociety.net/wp-content/uploads/2021/06/Assembling-

APP 1 of the Australian Privacy Act 1988 requires APP entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs and enable them to deal with enquiries or complaints about privacy compliance. In this way, the APPs require 'privacy by design', an approach whereby privacy compliance is designed into projects dealing with personal information right from the start, rather than being bolted on afterwards. Conducting a DPIA may help an entity to ensure privacy compliance and identify better practice. A DPIA is a systematic and documented assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.[55] However, conduct of a DPIA is not currently mandated by the Australian Privacy Act.

The Privacy (Australian Government Agencies – Governance) APP Code 2017[56] (the **Government Agencies Code**) requires Australian Government agencies to conduct a DPIA for all 'high privacy risk projects'. The Code provides that a project may be a high privacy risk project if an agency reasonably considers that the project involves any new or changed ways of handling personal information that are "likely to have a significant impact on the privacy of individuals". Guidance of the Australian Information Commissioner in relation to the Code states:

> An impact on the privacy of individuals will be 'significant' if the consequences of the impact are considerable, taking into account their nature and severity.
>
> The consequences of a privacy impact could be significant for one individual or a group of individuals, for example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft. The consequences of the potential privacy impacts for a group of individuals may vary based on their individual circumstances, so you should consider whether some individuals may be more significantly impacted than others.
>
> Sometimes projects can have a significant collective impact on society, rather than impacting on people individually. These collective impacts are likely to lead to broad public concern, for example, increased surveillance and monitoring activities, or the establishment of sensitive personal information sharing arrangements between the Commonwealth and other entities.

Accountability.pdf; Margot E. Kaminski and Gianclaudio Malgieri, "Algorithmic impact assessments under the GDPR: producing multi-layered explanations", International Data Privacy Law, 2021, Vol. 11, No. 2, p125

[55] See further Federal: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/; NSW: https://www.ipc.nsw.gov.au/guide-privacy-impact-assessments-nsw; Vic: https://ovic.vic.gov.au/privacy/for-agencies/privacy-impact-assessments/; Qld: https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process/undertaking-a-privacy-impact-assessment

[56] https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment/

> There is no definitive threshold to determine when an impact is 'significant' given each project will differ in nature, scope, context and purpose. Accordingly, agencies are advised to screen for factors that may raise a project's risk profile.[57]

Environmental protection laws require entities to undertake and publish environmental impact statements addressing adverse impacts upon humans and the environment of significant development projects. Unlike the requirement to publish environmental impact statements, in most instances regulated entities are not required to publish a DPIA.

In practice, in many cases a comprehensive DPIA is not conducted, because an entity:

- makes a preliminary determination that the project does not carry significant risks of privacy harms to individuals,
- determines that the Australian Privacy Act does not legally require a DPIA to be conducted, or
- does not recognise that it should be considering whether to conduct a DPIA.

In other cases, an entity may conduct a DPIA, but not identify and appropriately mitigate particular adverse effects on individuals as privacy harms, and accordingly leave unmitigated unacceptable residual risks of harms. These residual risks of harms may then be addressed by an entity through *form of disclosure that a collection and use of data that creates those risks of harms will take place* (not also stating what those risks of harms are), rather than addressing *substance of mitigating those risks of harms and appropriately managing residual risks* that continue to arise notwithstanding implementation of appropriate mitigation measures. In this way, legal requirements for 'transparency' as to privacy affecting acts and practices are purportedly met through inclusion of buried and opaque disclosures in privacy policies and collection notices.

Article 35 of the GDPR covers Data Protection Impact Assessments:

> Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.[58]

The European Data Protection Board provides the following examples of circumstances in which a DPIA should be conducted:

- If you're using new technologies
- If you're tracking people's location or behaviour
- If you're systematically monitoring a publicly accessible place on a large scale
- If you're processing personal data related to "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of

[57] https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment/
[58] https://gdpr.eu/article-35-impact-assessment/

genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

- If your data processing is used to make automated decisions about people that could have legal (or similarly significant) effects
- If you're processing children's data
- If the data you're processing could result in physical harm to the data subjects.[59]

Although privacy impact assessments are becoming more common in relation to proposals for new applications and uses of personal information about individuals, there remains considerable disagreement as to:

- the threshold at which a privacy impact assessment should be undertaken (i.e., what is a serious risk of harm to an individual?),
- the nature and range of "privacy harms" that should be assessed,
- the criteria for assessment of risk and harm,
- the level of potential risk of privacy harm and likely (or other) exposure to adverse impact at which a particular process should be assessed as requiring mitigation, and
- the level of residual risk of harm which is permitted to remain after appropriate mitigation.[60]

Unlike processes for environmental assessment, the frameworks and methodologies for making a preliminary assessment of whether to conduct a DPIA, for conduct and documentation of a DPIA, and for assurance of their reliable implementation, are not yet mature. Many DPIAs are conducted as 'check-the-box' exercises in 'assessment-and-disclosure-washing' to ensure that disclosures match form disclosure requirements stated in privacy principles, rather than genuine attempts by entities to ensure necessity and proportionality in data handling practices, and to build privacy-by-design into those practices.

Boards and senior management often see data privacy compliance as an assurance and audit function, rather than an integral and essential enabler of an entity conducting data-driven, or properly data-informed, business or other operations.

There are surprisingly few privacy professionals in some data-driven industry sectors, such as provision of digital advertising services (at least, outside of the global digital platforms and major media publishers) and adtech intermediation, and provision of digital health services. Relatively few regulated entities have developed in-house competencies of privacy professionals that are active in profit-centre lines of business.

[59] Guidelines on Data Protection Impact Assessment (wp248rev.01) adopted by the European Data Protection Board; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236; https://edpb.europa.eu/our-work-tools/our-documents/guideline/data-protection-impact-assessments-high-risk-processing_en

[60] As to the relationship between DPIAs and algorithmic impact assessment, see "Information Accountability Foundation, The Road to Expansive Impact Assessments – Why It Matters", June 2021

Many in-house privacy professionals have limited visibility of, and participation and influence in, ongoing governance and assurance of privacy affecting acts and practices of those entities. Privacy professionals working within entities are often sited within prudential and risk teams, rather than more directly involved in design and specification, and change management, of an entity's data architectures and data handling practices. As a result, significant privacy affecting practices can creep in unassessed in an entity's ways of working and dealing with individuals, even within entities that otherwise properly conduct privacy impact assessment upon initiation of new major projects.

Often privacy risk assessment is:

- episodic, conducted only upon initiation of major new projects, and
- outsourced to the fast-growing information risk practices of the big consultancies, with one result being that privacy risk assessment is often subsumed within, and obscured by, primary focus upon information security risk assessment. Outsourcing may also lead to an entity failing to develop in-house competencies in risk of harms assessment or to embed those competencies in its business-as-usual processes.

The most common failing of DPIAs is that they are point-of-time and often not revisited and revised as a project or product development progresses and pivots, or to take into account how a product or service is deployed and used over time. As agile methodologies for design and development become more commonly used, and product and service lifecycles shorten, the likelihood of misfit between a DPIA and reality increases. For example, identifiability risk changes unpredictably over time. Individual level transaction and transactor data sets relating to humans at any particular point of time and within a particular data environment sit at a point within a spectrum (continuum) of identifiability from identified, to reasonably identifying (i.e., pseudonymised), to effectively or functionally anonymised, to pervasively anonymised. Information may shift, or be shifted, towards ends of the spectrum, depending on factors including:

- specifics of the processing. For example, sensitivity of the variables in the original dataset, techniques used to reduce the identifiability of individuals in the data, and analytical methods or processes used (i.e., use of pattern matching to single out unique transactors),
- the data environments involved. For example, the technical and organisational measures put in place to control access to the data and reduce identifiability risk, and
- an entity's risk management process. For example, how an entity identifies and mitigate reidentification risks in the processing.

A comprehensive DPIA conducted at a point of time should assess identifiability risk having regard to both the nature of the data and the environment in which that data is held and processed. Often focus upon identifiability of data on the face of the data itself distracts attention of decision-makers from specification of controls and safeguards to be applied over the environments in which that data is held and processed. Many DPIAs do not appropriately address and specify the environment in which that data is held and processed, or lead to

implementation of change control within an entity to detect and appropriately address any significant change in the environment in which that data is held and processed. Environment, factors include:

- additional data that may exist (e.g., other databases, personal knowledge, publicly available sources),
- who is involved in the processing, and how they interact,
- the operational governance processes that are in place to control how the information is managed (e.g., who has access to it, for what purposes, and whether unauthorsied accesses or uses will be promptly detected), and
- contractual and other legal considerations that may apply, such as effective gateways that may impact the potential for disclosing information that enables individuals to be identifiable, and prohibitions that have the effect that while information could technically be combined to aid identifiability, doing so is against the law (e.g., professional confidentiality).[61]

Over time, operation of various factors may cause information to shift towards ends of the identifiability spectrum. For example:

- new information may be brought into the data analytics environment, increasing susceptability to mosaic or pattern reidentification,
- new external information may become reasonably available to a person attempting to reidentify individual data, also increasing susceptability to mosaic or pattern reidentification,
- new threat vectors may emerge,
- new technological means to reidentify an individual may become available to threat vectors,
- verification of operation of technical and operational controls and safeguards may beak down, or levels of training or adherence to operational controls may decline, so that processes and practices become more risky.

DPIAs should be a valuable tool for regulated entities to ensure that their acts and practices in handling of data relating to consumers and other citizens does not create significant risks of privacy harms to individuals. Too often, the tool is not used, or is used poorly, or is not brought out again when the tool needs to be used again.

General challenges and guiding principles for the responsible adoption of automated decision-making

Reform of the Privacy Act will not address many concerns as to harms to individuals, or to society, potentially arising from applications of new technologies and advanced data

[61] See Mark Elliot, Elaine Mackey, and Kieron O'Hara (UKAN), "The Anonymisation Decision-Making Framework: European Practitioners' Guide", 2nd edition, 2020, Dr Ian Oppermann and ors (Australian Computer Society), "Sharing Data in Trusted Frameworks", ACS Technical White Paper, December 2021, at https://www.acs.org.au/insightsandpublications/reports-publications/sharing-data-in-trusted-frameworks.html

analytics. Artificial intelligence (**AI**), machine learning (**ML**) and other algorithmic inference engines, collection of non-traditional data (for example, through IoT devices and other smart cities and smart infrastructure applications), also give rise to concerns that should be addressed by responsible innovators.

Concerns include:

- legal and regulatory compliance,
- competent use and adequate human oversight,
- an entity's ability to explain decisions made with AI or other algorithmic automation systems to the individuals affected by them,
- reduction in an entity's ability to be responsive to customer requests for information, assistance, or rectification, and
- social and economic impacts.

Some concerns are specific to advanced inference engines such as ML. Others arise from more basic algorithmically driven differentiation between users/consumers/citizens. For example:

- The performance of AI systems and other algorithmic inference engines crucially depends on the quality of the data used. However, data quality issues can be difficult to identify and address.
- Models developed with ML can have model characteristics that set them apart from more conventional models, including opaqueness, non-intuitiveness, and adaptivity.
- Adoption of AI and automated decision-making by organisations is often accompanied by significant changes in decision making processes within organisations, creating risks of over-reliance (dependency upon AI in making decisions in contexts or scenarios where that AI is not reliable) and opacity as to why decisions are made.
- Adoption of AI and automated decision-making can be accompanied by significant changes in the structure of technology supply chains, including increases in supply chain complexity and the reliance on third-party providers. Focus upon AI outputs risks creating a frame of review that underestimates or ignores how humans using AI may rely upon AI outputs to effect outcomes that are not fair, socially responsible, reasonable, ethical or legal.

The use of AI and automated decision-making can be accompanied by an increased scale of impacts when compared to conventional ways of performing business tasks. When things go wrong, unintended consequences can be very significant, very quickly.

Recent years have seen a rapidly growing literature on AI ethics principles to guide the responsible adoption of AI and automated decision-making, variously described but often reduced to fairness, accountability, transparency, equity and safety/sustainability (**FATES** or **FEATS**).[62]

[62] The AI Ethics Guidelines Global Inventory, a project by AlgorithmWatch, maps frameworks that seek to set out principles of how systems for automated decision-making (ADM) can be developed and implemented ethically.

As noted by Dr Florian Ostmann and Dr Cosmina Dorobantu of the Alan Turing Institute[63], the general challenges that AI poses for responsible innovation, combined with the concrete harms that its use in financial services can cause, make it necessary to ensure and to demonstrate that AI systems are trustworthy and used responsibly.

AI transparency – making information about AI and automated decision-making systems available to relevant stakeholders – is fundamental to both of these needs. Transparency acts as an essential precondition, an enabler, for ensuring that other principles for responsible AI are met. Transparency is therefore a logical first step for explainability[64] and for responsible and accountable deployment of AI and other automated decision-making systems. Governance and assurance frameworks and processes, and feedback and reassessment loops, depend upon transparency.

Information about AI and automated decision-making systems can take different forms and serve different purposes. A holistic approach to AI transparency involves giving due consideration to different types of information, different types of stakeholders, and different reasons for stakeholders' interest in information. Transparency needs include access to reliable information:

- about a system's logic (system transparency),
- about the processes surrounding a system's design, development, and deployment (process transparency),
- about how a system is used and relied upon as a component in a decision-making chain and in different contexts and scenarios for decision making (contextual decision transparency),

by

- personnel in different roles within the organisation using the system (internal operations and oversight transparency), and
- external stakeholders such as regulators (external oversight transparency),
- external stakeholders, such as citizens on whom use of AI or other automated decision-making may cause significant effects, and civil society organisations and regulators, to

The database currently includes 173 guidelines: https://inventory.algorithmwatch.org/. See further Australian Computer Society, 2021, "The Ethics And Risks Of AI Decision-Making", and the reports and other resources listed there (under 'Further reading' at pp 26-29), available at https://www.acs.org.au/insightsandpublications/reports-publications/the-ethics-and-risks-of-ai-decision-making.html; Australian Government, Australia's Artificial Intelligence Ethics Framework, https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-ethics-framework; "Monetary Authority of Singapore, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector", 2018, OECD, OECD Business and Finance Outlook 2021: AI in Business and Finance, OECD Publishing, Paris, https://doi.org/10.1787/ba682899-en

[63] Florian Ostmann and Cosmina Dorobantu, "AI in financial services", The Alan Turing Institute, June 2021, https://doi.org/10.5281/zenodo.4916041

[64] See UK ICO and Alan Turing Institute, Explaining decisions made with AI, https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/; and ongoing Project ExplAIin work at https://www.turing.ac.uk/news/project-explain; for an example of a published 'explainability statement', see Healthily at https://www.livehealthily.com/legal/explainability-statement

enable those stakeholders to understand possible adverse effects such as overly granular profiling or unfair differentiation between individuals, or excessive surveillance (external affected individuals' transparency).

For system and process transparency alike, there are important questions about how information can be obtained, managed, and communicated in ways that are intelligible and meaningful to different types of stakeholders.

Both types of transparency – internal and external – are relevant in ensuring and demonstrating that applicable concerns are addressed effectively.

These concerns may arise:

- regardless of whether the application of AI involves any use of personally identifying information about (identified or identifiable) users, or information about pseudonymised user-specific activities or behaviours,
- regardless of whether creation and use of the cohort involves unlawful discrimination or other infringement upon currently legally recognised human rights.

In other words, compliance with existing data privacy and antidiscrimination laws is a relevant concern, but only one concern.

Application of broader principles of fairness, equity, accountability and transparency in uses and applications of data about individuals – and not just personal data about these individuals – must become an essential feature of processes and practices of data governance and assurance of businesses, government agencies, political parties and not-for-profits.

Changes in the scope and coverage of the Australian Privacy Act are necessary to address some of these concerns. However, data privacy law is not the right instrument to address many concerns as to harms to individuals, or to society, potentially arising from applications of new technologies and advanced data analytics. In addition, until we better articulate those concerns, and good practice to address them, we cannot fully assess whether other new laws are necessary to ensure that the broad range of entities that are now deploying AI, ML and other automated decision making, and collecting non-traditional data.[65]

Before we condemn entities for failing to be ethical or socially responsible, or impose broad regulatory constraints across diverse applications, we need to ensure that entities applying these new technologies and data analytics capabilities understand how they can ensure that they reliably and verifiably evaluate what they should, or should not, be doing. Publication of ethical principles, without more, is simply not good enough: we need to provide clear guiderails for regulated entities. Principles as to ethical, or socially responsible, conduct, will not be consistently and reliably translated into practice unless there is also clear articulation of:

[65] For a recent analysis of design for AI regulation without unduly impeding innovation, see Ada Lovelace Institute, "Regulate to Innovate", November 2021

- what good practice looks like,
- how good practice should be assessed and given effect through methodologies and tools,
- how unacceptable or illegal practices will be detected and prevented, and
- how to achieve the right balance between incentives for good behaviour and sanctions for unacceptable behaviour.

Challenging indeed, but a necessary concomitant of continuing to derive manifest benefits to society from applications of new technologies and advanced data analytics.

A design manifesto for an Australian Privacy Act that is fit for purpose in the 21st century

The following contentions might inform redesign of the Australian Privacy Act.

1. Federal, State and Territory data privacy statutes in Australia, and in many other jurisdictions, are no longer fit for purpose. Regulation focusses upon ensuring that regulated entities provide transparency to individuals, and afford those individuals with (alleged) choice, as to collection, uses and disclosure of personally identifying information about them. Choice is often illusionary. Regulation does address reasonable necessity to effect a stated purpose, but does not squarely address reasonableness or proportionality of acts and practices of regulated entities in collecting, handling and disclosing personal information about individuals.

2. 'Because of the Privacy Act' is enabled as an excuse to impede individual level data linkage for population analytics conducted for societal benefit even if conducted with appropriately isolated and controlled and safeguarded data analytics environments. Risk of privacy harms to individuals should not be discounted, but societal benefit also needs to be accorded due weight. Many claims of social beneficence and appropriate controls by would-be data analytics entities do not pass objective assessment. However, other data analytics projects that implement best practice governance and assurance are impeded, delayed and often rendered impracticable. Ethics review and approval processes are cumbersome, episodic (project orientated, not enabling standing up of continuing controlled data environments) and not sufficiently informed by preceding approval conditions. Too many ethics committees spend too much time in well intentioned 'reinvention of the wheel' that could be avoided if conditions devised for prior analogous reviews were readily available to inform the committee's deliberations.

3. Federal, State and Territory statutes addressing use of surveillance and tracking devices are difficult to interpret and apply in relation to emerging technologies and novel uses of geolocation data, biometrics and pattern analysis to differentiate between persons in how they are dealt with. Some provisions in those statutes are inconsistent, with the effect that it is often impracticable to deploy uniformly across Australia a service that uses surveillance or tracking technology.

4. The interaction between Federal, State and Territory data privacy statutes, health information statutes, and surveillance and tracking devices statutes, is increasingly problematic. Health-related data is tied up in a labyrinthine interaction of Federal, State and Territory regulation and regulators. Many innovative health and IoT (smart utilities and smart infrastructure) applications require interactions of these regulatory schemes to be addressed with multiple agencies, for no manifest benefit in assessment and mitigation of risk of harms to affected individuals or protection of the public interest. For data uses and sharing, there is no 'one-stop (regulatory or regulator) shop', and very limited mutual recognition, across Australian jurisdictions.

5. Because data privacy statutes are focussed upon acts and practices in handling of information in relation to reasonably identifiable individuals, these statutes generally do not address other data and surveillance applications that enable entities to differentiate on their treatment of persons based upon observations or inferences made by those entities as to characteristics, behaviours, interests or attributes of individuals, or small cohorts of individuals, that are not reasonably identifiable.

6. Emerging technologies increasingly enable collection and use of data that facilitates real time and granular differentiation between non-identified individuals, or grouped cohorts of 'like individuals', to enable entities using those technologies to work out whether, how or on what terms to deal with individuals. If individuals are not reasonably identifiable, this collection and use of data is not an act or practice currently regulated under Federal, State or Territory data privacy statutes as a handling of personal information.

7. In many situations non-identifying differential treatment of persons is benign. Differential treatment of unidentifiable persons generally does not cause significant risk of privacy harms to affected individuals and should not be regulated, because entities should be incentivised to ensure that persons remain unidentifiable. In some situations, this differentiation is beneficial to an affected individual, by enabling more efficient provision of content, or offer or delivery of products or services. In any event, consumer protection and antidiscrimination laws address many forms of differentiation between consumers rightly considered unfair or otherwise illegal. Privacy regulation should remain focussed upon risk to individuals of privacy harms. It should not displace appropriate development of broad form consumer protection law, or the making (where there is good policy justification) of topic and sector specific statutory provisions to regulate other non-identifying differential treatment, such as laws addressing particular forms of unlawful discrimination, targeting of children for unhealthy or otherwise inappropriate content or products, excessive surveillance, disinformation and misinformation.

8. In considering reform of Australian data privacy statutes, we need to go back to basics and ask: 'what harms should privacy law address?', or as Professor Julie Cohen put it,

"what is privacy for"?[66] Revised data privacy statutes should afford due weight to ensuring that Australian society derives benefits from applications of advanced data analytics and artificial intelligence, and from socially beneficial data sharing, while also ensuring that regulated entities are accountable for mitigating risk of privacy harms to individual humans and enabling humans to go about their lives without excessive intrusion upon reasonable expectations of seclusion.

9. Protection of data privacy interests of individuals requires an approach that combines 'top-down'(what is privacy?), and bottom-up (what harms are we seeking to avoid or mitigate and manage?). This conclusion does not lead us to a crisp definition of data privacy. Alas, the search for crisp statutory definitions of privacy, and privacy harm, is a search for a chimera. This conclusion explains why almost all data privacy statutes refer to a right of individuals in and to (data) privacy, and to be protected against (data) privacy harms, without telling us much more about what privacy and a privacy harm actually mean.

10. The foundation of most modern data privacy statutes – notice to affected individuals and affirmative consent as to more privacy affecting activities – remains relevant. However, we need new clarity of thinking as to the purposes of privacy policies and privacy (collection) notices, to reduce the information burden upon affected individuals. We all need less clutter in our lives. Most paragraphs in most privacy disclosures are unnecessary noise. Whether it is through legitimate interests, industry standards, class exemptions by regulators, or brave new concepts such as compatible data practices, we need to reduce the level of noise in privacy policies and notices.

11. Citizens should only be expected to self-manage what is realistically manageable by them. Current regulation encourages erosion of the value of consent. We need to make consent great, again. Many proposals for reform of data privacy law risk doubling down on the problem, casting the net of consent too widely. Consent should only be sought where it is reasonable to believe it will be given (or withheld) actively, thoughtfully, sparingly and with understanding.

12. Any exception for legitimate interests, legitimate uses or 'compatible data practices' should only operate and allow a regulated entity to collect, handle or disclose personal information about individuals without consent if the processing is aligned with the ordinary expectations of affected individuals, having regard to transparent privacy policies and notices, and not harmful to direct interests of data subjects. In particular,

[66] Julie E Cohen, "What is Privacy For" Harvard Law Review Vol. 126 (2013) p 1904-1933; see also Lior Jacob Strahilevitz, 'Toward A Positive Theory Of Privacy Law' Harvard Law Review Vol. 126, No. 7 (May 2013), pp. 2010-2042; Austin Sarat, A World without Privacy What Law Can and Should Do?; Cambridge University Press, 2014, particularly Lisa M. Austen, 'Enough About Me" at pp. 131 – 189, DOI: https://doi.org/10.1017/CBO9781139962964.004

permitted primary purposes of collection and handling of personal information about individuals should remain subject to transparency requirements.

13. Some proposals for reform of data privacy laws respond to shortcomings of the notice and consent framework by advocating new measures of 'organisational accountability', including objective fairness or reasonableness of data privacy practices. There is an important role for organisational accountability in data privacy law.

14. One key issue in reform of Australian data privacy law is how to address responsibility and accountability of entities that curate or otherwise enable multiparty data ecosystems that share information about activities and attributes of citizens. Addressing this concern requires measures that combine increased transparency to affected individuals with organisational accountability. Introduction of a 'data controller-data processor' distinction into the Australian Privacy Act might assist in reducing clutter and noise in privacy disclosures and improve understanding of regulated entities as to their responsibilities in management and oversight of data ecosystems that those entities enable or operate. Attention of consumers should be directed towards full and fair explanation by a collector of personal information as to sharing of that information into multi-party data ecosystems, particularly in circumstances where the entity making a disclosure statement is not in continuing control of uses and further disclosures by other entities in that data ecosystem.

15. The right and interests of individual humans to go about their lives without excessive intrusion upon reasonable expectations of seclusion needs the protection of a data privacy regulator that is credibly resourced, empowered and focussed. We should be realistic and ensure that regulated entities have appropriate incentives to be responsible in, and accountable for, their acts and practices in handling of personal information. Regulatory incentives include real likelihood that an empowered and resourced data privacy regulator will take enforcement action and seek sanctions.

16. The data privacy regulator should also be empowered and resourced to issue detailed guidance and to consult with regulated entities as to good data privacy governance, privacy protective processes and data assurance practices.

17. Protection of consumers from unfair contact terms and deceptive trading practices requires a consumer protection regulator of like attributes and qualities. There is significant overlap. Continuing alignment discussions between these regulators will be necessary, but they fulfil different functions. When data privacy is seen as a consumer protection function, we have forgotten what data privacy is for.

18. Currently scoped data privacy laws and consumer protection laws are not the appropriate frameworks to address some of key challenges of new applications of data sharing, advanced data analytics and AI/ML affecting humans and the environment.

Socially beneficial applications need to be accommodated, without creating workarounds of legal protections of consumer rights and expectations of data privacy. As the EU has recognised in proposals for new regulation of AI, addressing adverse impacts upon some groups of citizens of differentiated treatment of citizens enabled through algorithmic individuated effects requires fresh policy thinking and new regulation.

Peter Leonard

12 January 2022