Submission to the Australian Government on the Review of the Privacy Act

Submission by Kimberlee Weatherall[1]
Professor of Law, The University of Sydney Law School
Chief Investigator with the ARC Centre for Automated Decision-Making and Society
29 November 2020

Overview

1. This submission responds to the Issues Paper on the Review of the Privacy Act 1988 (Cth) issued in October 2020.

2. Given the limited time to respond to a very large number of questions about privacy law and principles, on top of too many other consultations in related areas, this submission does not seek to propose specific or detailed legal drafting. There are international precedents for legal text for addressing many of the questions raised in this submission (and the Issues Paper). The details are better debated once the bigger picture policy questions are resolved.

General comment: the presumption should be in favour of reducing legislative exclusions and exceptions, and reinstating a principles-based privacy regime (note that this section has implications for Questions 66-67)

3. My overarching concern with the Issues Paper, and the proposals from the *Digital Platforms Inquiry* that preceded it, is that they reflect an orientation towards tweaking specific rules - and adding more. This will contribute to a privacy regime in Australia that is already too complex and fragmented. *Specialists* already struggle to parse Australian privacy law.

4. A preferable approach would reduce exemptions and exclusions and rely more heavily on the principles-based regulatory form which can adjust and be nuanced 'in the wild' to new kinds of data and new scenarios. It would also strengthen the principles to reduce the need for separate tailored regimes.

5. The 1988 Act was originally designed to cover the Commonwealth public sector, but it has been amended at least 10 times since (5 times in the last 10 years), creating specific rules for certain kinds of data (eg spent convictions; tax file numbers; credit reporting, medicare; the PBS; healthcare identifiers; electronic health records), industries (telecommunications); issues (anti-money laundering; counterterrorism); or to create new systems (eg notifiable data breaches). As a result, the Act is now over 300 pages long.

6. We have also in recent times seen the creation of a new and different privacy regime in relation to the Consumer Data Right, and supplemented with new regulations, and technical standards, as well as guidelines (themselves 180 pages long), as well as *another* new and specific regime for COVIDSafe App data.

7. The proposed new *Data Access and Transparency Bill* - which as presently drafted adds another route for data access (with implications for privacy, albeit via a separate piece of legislation) without actually getting rid of any of the existing systems.

---

[1] The author can be contacted at kimberlee.weatherall@sydney.edu.au. Curriculum vitae and other information is available at https://www.sydney.edu.au/law/about/our-people/academic-staff/kimberlee-weatherall.html

8. And privacy is also governed by other areas of law (such as in relation to the workplace[2]). Separate laws address various kinds of law enforcement, supplemented by non-transparent practices.[3] Then there is an additional layer of State legislation. And of course, this is all before anyone reads any one of the many privacy policies to which they are subject, which are routinely very long and written to require a university degree to make any sense of them.[4]

9. This level of complexity in the law imposes disproportionate compliance costs (which are then used to justify various exclusions, including things like the small business exclusion), and burdens on the public and private sector.

10. And what's worse: all this law *isn't working.* Significant quantitative and qualitative research in Australia illustrates that Australians do not feel in control of data about them.[5] Most people are in no position to understand their rights, let alone pursue them (insofar as they *can* pursue them via means of a complaint, given limits on individual rights of action). They have reason to feel like they have no control, because it is clear that effective surveillance, data collection and use *is* extensive and insufficiently transparent, especially in the private sector but also in the public sector.

11. It also means that Australia's privacy law is not a principles-based regime. It is a set of principles encased in a cocoon of hard rules and confined to only partial application. The principles are inconsistently applied, excluded from important areas, and augmented in others (eg the Consumer Data Right). More fundamentally, this level of complexity is inconsistent with the rule of law,[6] which is *meant* to ensure that people can know the rules that govern them and adjust their behaviour accordingly.

12. The review is an opportunity to bring privacy law to something closer to an actual principles-based regime. Piling on more detailed rules, and exceptions, as foreshadowed in the 68 questions of the Issues Paper, will not solve the overall regulatory problems of an overwhelmed public, an under-resourced regulator, and an environment of non-transparent data collection and use run mad.[7]

---

[2] See eg Charbonneau, Étienne, and Carey Doberstein. "An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector." *Public Administration Review* 80, no. 5 (2020): 780–91. https://doi.org/10.1111/puar.13278.

[3] See eg Moses, Lyria Bennett, and Louis De Koker. "Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by NAtional Security and Law Enforcement Agencies." *Melbourne University Law Review* 41 (2017): 530–70.

[4] See Amos, Ryan, Gunes Acar, Elena Lucherini, Mihir Kshirsagar, Arvind Narayanan, and Jonathan Mayer. "Privacy Policies over Time: Curation and Analysis of a Million-Document Dataset," August 20, 2020. https://arxiv.org/abs/2008.09159v2. This very recent study is based on automated analysis of a dataset of over a million privacy policies from over 130,000 websites. It found that policy length had doubled 2009-2019, and that readability was at the college level.

[5] See, eg, Office of the Australian Information Commissioner. "Australian Community Attitudes to Privacy Survey 2020," 2020. https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf; Biddle, Nicholas, Ben Edwards, Matthew Gray, Michael Hiscox, Steven McEachern, and Kate Sollis. "Data Trust and Data Privacy in the COVID-19 Period." The Australian National University, July 30, 2020. https://csrm.cass.anu.edu.au/research/publications/data-trust-and-data-privacy-covid-19-period; Goggin, Gerard, Ariadne Vromen, Kimberlee Weatherall, Fiona Martin, Webb Adele, Lucy Sunman, and Francesco Bailo. *Digital Rights in Australia*, 2017. https://ses.library.usyd.edu.au/handle/2123/17587.

[6] As Lyria Bennett Moses pointed out in an ACS-hosted Masterclass in April 2020

[7] See similar comments from the Banking Royal Commission: Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, *Final Report Vol 1,* at p16: "'… adding a new layer of regulation will not assist. It will add to what is already a complex regulatory regime. No doubt the financial services industry is itself complicated. That may be said to explain why the regulatory regime is as complicated as it is. But closer attention will show that much of the complication comes from piling exception upon exception, from carving out special rules for special interests. And, in almost every case, these special rules qualify the application of a more general principle to entities or transactions that are not different in any material way from those to which the general rule is applied".

Objectives (question 1)

13. The objectives of the *Privacy Act* need reform.

14. Objective 2A(c) identifies the objective to 'provide the basis for nationally consistent regulation of privacy and the handling of personal information' (s 2A(c)). This object should be reformed because, frankly, it is contradicted by the current state of the law as outlined above. An objects clause should not be merely an articulation of wishful thinking, and it should not be misleading to ordinary people. Of course, if we can reform privacy law sufficiently that the objective is at least partially achieved - which should be the aim, as argued above - the objective may be worth retaining.

15. A second object that could use reform states that the Act aims 'to promote the protection of the privacy of individuals' (2A(a)). There are two things wrong with this objective.

16. First, privacy is a multifaceted concept, and is only partially reflected in this legislation, which is more accurately defined as a data protection law. Rather than assert that the Act seeks to promote the protection of privacy (generally), the objective should be more specific: eg, that the the object is to promote the privacy of individuals *by establishing principles governing the collection, use and disclosure of personal information and to ensure that personal data that is collected and used is of high quality, fit for purpose, and subject to both correction and appropriate security*. This would remove any suggestion that the goal is a more holistic protection of people's privacy rights.[8]

17. Second, this object suggests that privacy is purely an individual problem and an individual right, solved by giving appropriate controls over the use of data to individuals. This is exacerbated by the 2nd object (2A(b)) which states that 'the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities'. This 2nd object implies that the only interests relevant in thinking about privacy are the interests of individuals, and those of the organisations (public or private sector) that collect, use and disclose data.

18. An important part of this whole discussion ought to be articulating **society's collective interests** in the information environment, and in appropriate, transparent and fair collection, use, and disclosure of personal information. There are distinct societal and collective interests in data: sometimes in limiting data collection; sometimes (perhaps most obviously in the COVID context) in allowing it but putting protections around it.[9] There are also collective interests implicated by individual choices about data. For example, my personal interests in not being subjected to microtargeting, hypernudging, or excessive surveillance by private or public sector are affected by individual decision-making. If lots of other people allow unfettered collection and use of data, then that data can be used to make inferences about me.

19. A more appropriate objective, then, would be "to promote the protection of the privacy of individuals and Australians' interests in ensuring an information environment that benefits the Australian people, society and economy generally, where data collection, use and disclosure is appropriate, transparent, and fair, and takes into account the

[8] As a matter of legal/statutory interpretation, it may be that this could be especially important if Australia decided to implement an action for 'serious invasions of privacy'. If that *were* enacted, *and placed in the Privacy Act 1988* (Cth), one result could be the inadvertent confining of what counts as a serious invasion of privacy: for example, if the court decided that the concept of what privacy is depends on what is articulated in the Australian Privacy Principles.

[9] See for example Viljoen, Salome, Democratic Data: A Relational Theory For Data Governance (November 11, 2020). Available at SSRN: https://ssrn.com/abstract=3727562 or http://dx.doi.org/10.2139/ssrn.3727562.

interests of a full range of stakeholders.'' There are no doubt other ways of drafting the objective so as to recognise a societal interest.

Exemptions (questions 7-16)

20. Consistent with a goal of reducing complexity and inconsistency in privacy law, the exemptions for small business, political parties, and employee records should all be reconsidered, and removed.

21. One problem with current exemptions and exceptions to privacy law is that the exclusions directly prevent Australia's privacy law from addressing some of today's most urgent concerns about data collection and use. Following the events around Cambridge Analytica and having watched developments in successive US elections or the advertising antics of certain Australian politicians, there is real concern about the collection and use of data in a political context (through the political parties exemption).[10] The current pandemic has given rise to greater workplace monitoring, and empirical research already strongly suggests that people are profoundly uncomfortable with increasing employee surveillance.[11] The existence of exemptions encourages unchecked, non-transparent, and potentially unfair collection of data: about employees and by political parties.

22. The Act also fails to meet Australian's expectations of who should be covered. According to the most recent OAIC survey, 71% think small Australian businesses should be included, 72% for media organisations, 73% for businesses collecting work-related information about employees and 74% for political parties and political representatives.[12] Many Australians think these organisations are *already* covered by privacy law.[13]

23. A legislative regime which purports to promote the protection of privacy but which fails to address current, urgent concerns and the broadly held expectations of the public will only exacerbate public distrust, resignation and/or cynicism.[14]

24. The **employee records exemption** has long been uncertain in scope. It is becoming more uncertain as firms' capacity to collect and use data increases.[15] To what extent is any given data relating to an employee 'directly related to… a current or former employment relationship between the employer and the individual' (s 7B)? Is data collected via new tools built into Office 365, and used to create visualisations about how 'collaborative' employees are, or how many collaborators they have, or how much 'free time', information 'directly related to … the employment relationship'? Could a firm

[10] See Normann Witzleb and Moira Paterson, 'Micro-targeting and political campaigns: political promise and democratic risk', forthcoming in Uta Kohl and Jacob Eisler (eds), Data-Driven Personalisation in Markets, Politics and Law (forthcoming CUP, 2021), Available at SSRN.

[11] See eg Charbonneau, Étienne, and Carey Doberstein. "An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector." *Public Administration Review* 80, no. 5 (2020): 780–91. https://doi.org/10.1111/puar.13278. The study compares general public attitudes and public sector employee attitudes towards workplace surveillance. The study population is Canadian, not Australian, but similarities between the political and economic cultures of the two countries means that these results are certainly suggestive for Australia.

[12] Office of the Australian Information Commissioner. "Australian Community Attitudes to Privacy Survey 2020," 2020. https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf, 60

[13] Ibid 58.

[14] On resignation/cynicism, see Hoffmann, C. P., Lutz, C., and Ranzini, G. 2016. "Privacy cynicism: A new approach to the privacy paradox," Cyberpsychology: Journal of Psychosocial Research on Cyberspace (10:4).

[15] There have been disputes over the scope of the exception: see eg *'QF' & Others and Spotless Group Limited (Privacy)* [2019] AICmr 20.

argue that such data is relevant to performance and hence to the employment relationship? Perhaps such an argument would be rejected if it ever went to court, but it is probably sufficiently arguable to encourage a significant proportion of firms to believe that such surveillance is both justified and does not implicate privacy law.

25. The **small business exemption** is internationally anomalous. It has become ever more possible for small companies to collect and use significant amounts of personal information. If companies wish personal information to be part of their business, then they should be required to treat it with respect. Many small businesses are already obliged to comply with privacy law as a result of European or New Zealand rules. If there is a concern about compliance costs, that concern should be channelled into reducing the excessive complexity of privacy legislation and law, and turning privacy law back into a genuinely principles-based regime.

26. Excluding **political parties** has more risks for democracy than benefits, as Witzleb and Paterson have recently argued.[16] It has the additional, deleterious effect of subjecting politicians and leaders to a different set of rules than they impose on most others - which is inconsistent with the rule of law.

27. The concerns that gave rise to the exemptions can be dealt with in other ways. The compliance burden on small business can be addressed by reducing legislative complexity, and improving consistency with other generally applicable regimes such as New Zealand law and/or the GDPR, which many small businesses must comply with in any event. Including political parties in privacy law will not prevent communication with constituents, but will impose basic obligations to be transparent; to respect individuals' rights, and to ensure that data is held securely. Including employee records will not prevent the collection and storage of employee data but will require again, more transparency and security.

Privacy notices (questions 20-25)

28. Several brief points may be made about privacy notices.

29. First, there are good reasons to support a layered approach to privacy notices, comprising (a) simple icon-based models; (b) machine-readable versions, and (c) detailed versions. Each layer serves a different purpose:

    a. Simple versions are important for better communicating with users.

    b. Machine readable privacy notices could enable the develop of consumer tools for privacy management.

    c. Detailed versions (legalese) are also important, not because lots of people will read them (they don't), but because the existence of those notices enables both deeper research and analysis of privacy-related practice, *and* enforcement via consumer law. For example, where corporate practice is inconsistent with detailed privacy notices, this can form the basis for an action under consumer law for misleading or deceptive conduct.[17] In this way, detailed notices are a potential additional source of discipline on corporate

[16] Normann Witzleb and Moira Paterson, 'Micro-targeting and political campaigns: political promise and democratic risk', forthcoming in Uta Kohl and Jacob Eisler (eds), Data-Driven Personalisation in Markets, Politics and Law (forthcoming CUP, 2021), Available at SSRN.

[17] This is the basis of an action filed by the Australian Competition and Consumer Commission against Google. See also Hintze, Mike. "In Defense of the Long Privacy Statement" *Maryland Law Review* 76, no. 4 (2017 2016): 1044–84.

behaviour, as *other* laws, other than privacy, can be used to enforce those notices.

30. Finding better ways to communicate the implications of policies is important; it is also very challenging, and importantly, *not new*. Those tasked with designing new systems could benefit from the extensive existing models,[18] empirical research on health stars, and growing research in UX design too large to summarise here.[19] One means for tackling these questions and drawing on this research could be by commissioning an accompanying technical paper by relevant experts (as the Australian Human Rights Commission has recently done in relation to bias and artificial intelligence, or as Data61 did for standards in relation to the consumer data right). Any such paper should draw on a range of expertise: linguistics, HCI, marketing; as well as privacy and privacy law and no doubt others I've not thought of. My own brief review of 2020 literature on related questions as part of preparing this submission suggests that there is an undesirable amount of 'siloing' in the literature, with unconnected writings in law, design, and data science.

Consent and its effectiveness (questions 26-30)

31. Numerous experts have pointed out that consent should not be a 'get out of gaol free' card that enables all kinds of data collection and use. Relying on consent underestimates the impact that *some* people agreeing, or not agreeing, to data collection or use has on both the individual privacy interests of *other* people, and the impact on other *collective* interests:

    a. Sometimes requiring consent prevents socially beneficial activity: sometimes it is too hard to get all the consents needed to undertake some activity, but the benefits of the activity outweigh the dangers: eg, some medical research; some monitoring during public health emergencies;

    b. Sometimes allowing consent to be sufficient will allow for undesirable activity that impacts negatively on the privacy of others: as noted, if a majority are happy to consent to social media privacy terms, this impacts on other individuals in two ways: first, it allows the collection of data from consenting individuals that can be used to make inferences about non-consenting individuals; and second, it increases the pressure on nonconsenting individuals to use the service even if they don't want to (for example, because it is the only way to keep in touch with what is happening in one's community sports club or school year). My decision to have an IOT device in my home, or install cameras on my property, has privacy impacts on my neighbours and visitors. It is entirely legitimate to legislate to limit these activities to protect collective interests.

    c. It is simply unreasonable to impose all the burdens of managing privacy on individuals rather on the organisations that want to collect and use data, which benefit the most from its collection and use, and which are in the best position to be informed about what they will do with data and what the implications of that use are.

[18] Cranor, L. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. Journal on Telecommunications and High Technology Law, 10(2), 273-308.

[19] See, eg, Rossi, A., and M. Palmirani. "Can Visual Design Provide Legal Transparency? The Challenges for Successful Implementation of Icons for Data Protection." *Design Issues* 36, no. 3 (June 2020): 82–96. https://doi.org/10.1162/desi_a_00605.

32. Frankly, people should never be required to consent to outrageous and exploitative practices around data in order to get access to a service - but that is precisely what happens, because Australia is overly reliant on a consent-based regime and has not made the effort to either set more general restraining principles regarding use and disclosure of data (see next heading) or identify red lines, or no-go zones. Doing the former (more general restraining principles) is straightforward today because many international precedents exist. Identifying 'no go zones' will be harder, but ultimately is likely to be more beneficial (and simpler for market actors to understand and implement).

33. As to the form of consent: I repeat the submissions above paras [28]-[30]: that finding simple ways to communicate with consumers is important but challenging; and that an accompanying technical paper drawing on a range of sources of expertise and several large existing literatures may be the best way to identify how to do it.

Regulating use and disclosure

34. Australians deserve better than the current regime which limits collection to certain limited purposes, but does little to limit *how* data is used once the collection is legitimate. There are numerous circumstances where it might be legitimate to collect and use data, but *how* the data is used might be deeply unfair. One might agree, for example, that it is legitimate for one's bank to collect very significant amounts of highly personal data on transactions etc, and even agree that the bank ought to be able to use that data to 'tailor services to me' (and we might consent to that use). But I might then think it unfair if the bank used the data to decide that I 'could afford to pay more' (or wouldn't object to a higher price than my neighbour down the road) – even though that is still 'tailoring services'. Whether or not this is the best example isn't the point: the point is that people care about more than the general purpose for which data is collected.

35. Australians currently receive lesser protection for their privacy risks than citizens in a range of comparable countries, including Europe. Australians would benefit from a privacy regime which:

    a. Imposed restraints on the manner of data collection and use. For example, a number of commentators have noted the general constraints set out in the GDPR, which states that must be:

        i. processed lawfully, fairly and in a transparent manner in relation to the data subject (art 5.1(a)); and

        ii. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation') (Art 5.1(c));

    These restraints are desirable: particularly an obligation to process data **fairly**. Certainly this would give rise to debate about what kinds of data collection and use are 'fair', but there are rich technical and legal literatures on which to draw, and in any event, imposing a requirement as to fairness would have the advantage of giving internal actors within firms a mandate for thinking about the impact of data collection and processing on people - a mandate or requirement that really isn't in the law at the moment at all.

36. Europeans are also entitled to data protection by design and default (art 25) - a salutary position which, if genuinely applied, would place brakes on the 'collection of data for

collections' sake' that occurs at present. Europeans also receive additional protections in the case of automated decision making (art 22) which the Australian Human Rights Commission has been considering, and where perhaps discussion across these reviews would be of most benefit.

37. There would be benefits in identifying no-go zones or basic prohibitions. Here is not the place, or I am not the person, to outline what they should be. Salinger Privacy has identified some worthy of consideration. There are no doubt more. What we actually need is both the identification of immediate no-go zones, *and* - given how dynamic this field is and that the discussion needs to be a broader one among a very wide range of stakeholders not all of whom will be represented in this consultation - a mechanism for having the discussion about where the lines should be drawn on an ongoing basis. The Canadian privacy law identifies one way to do this: by limiting collection, use or disclosure to purposes 'that a reasonable person would consider are appropriate in the circumstances (PIPEDA s 5(3)). This kind of rule could serve the dual purpose of providing a legislative 'hook' for the OAIC to pre-emptively identify uses that 'a reasonable person would not consider appropriate in the circumstances' (and develop appropriate guidelines) and a means for challenging existing activities not yet subject to guidelines from the OAIC through dispute resolution.

38. Prohibitions can benefit firms that want to do the right thing by their customers, and act consistently with known privacy preferences, but which presently are under pressure from other firms. At present, a firm that wants to sell hardware without extensive spying capacities will find it challenging to meet the price point of a firm that looks to data collection and exploitation as part of its business model.