Privacy Act Review

Discussion Paper, October 2021

Submission to Attorney-General's Department

Professor David Lindsay[1]
Faculty of Law, University of Sydney
Date: 21 January 2022

Introduction

I am grateful to the Attorney-General's Department for the opportunity to make a submission to the Discussion Paper (the DP) on the Privacy Act review. Given the comprehensive scope of the review, this submission does not attempt to address all of the issues raised in the DP. Instead, it aims to provide feedback on selected issues that are important in framing and reforming Australian privacy law so that it is fit for purpose in the context of the considerable challenges arising from contemporary data practices, especially the challenges of contemporary data collection and processing practices at scale.

This submission addresses the following issues:

1. To what extent is there is a need for a new regulatory paradigm for Australian data privacy law?
2. Is there a potential role for a 'risk-based' approach to regulation, especially in determining potentially prohibited or restricted practices?
3. The potential incorporation of the principles of Data Privacy by Default and Design (DPbDD) into Australian law.
4. Is there a right to privacy under Art 17 of the ICCPR?
5. The definition of 'personal information'.
6. Exemptions from the Privacy Act.
7. Notice and Consent.
8. The proposed new 'Fair and Reasonable' Test.
9. Additional protections.
10. The data security principle and 'joined-up regulation'
11. A direct right of action.
12. A statutory tort of privacy.

[1] david.lindsay@uts.edu.au. Research used in this submission was funded by a grant from the Australian Communications Consumer Action Network (ACCAN) for a project entitled: "Regulating to Protect the Security and Privacy in the Internet of Things (IoT)".

1. A New Regulatory Paradigm?

Data privacy laws, such as Australia's *Privacy Act 1988* (Cth) (the 'PA'), can be conceptualised in accordance with generations of laws designed to respond to the challenges of generations of information technologies.[2] As the ACCC made clear in its *Digital Platforms Inquiry* ('DPI') report, Australia's data privacy law has failed to keep pace with the challenges posed by contemporary data collection and processing practices. These technologies and business practices are based upon the collection, analysis and use of data at scale. They also include business practices that use data to profile and target individuals to extract value, sometimes extending to potentially manipulative practices.[3] The PA – which is largely based on a model of soloed processing of data by individual entities and which attempts, in part, to enhance the control of individual data subjects over data practices – is no longer fit for purpose. While the EU GDPR is a more recent attempt to adapt data privacy regulation to apply to contemporary data processing practices, it has also been overtaken by events. The first step in reforming the law so that it is adequately adapted to existing practices is therefore to review the regulatory paradigm. In this, lessons can be learned from regulatory initiatives that attempt to meaningfully grapple with the challenges posed by contemporary data practices.

In April 2021, the European Commission (EC) released its proposal for a Regulation on Artificial Intelligence,[4] which built on experience with measures introduced as part of the GDPR to address 'big data' practices. When taken together, it is possible to see these measures as part of an emerging regulatory paradigm which attempts to address the challenges of regulating near-ubiquitous data collection and processing. The new paradigm moves away from (but does not completely abandon) the regulation of particular practices – such as the collection, storage, use and disclosure of personal information – towards a more holistic approach to regulating complex socio-technical systems, with a focus on regulating technology design.

The emerging new paradigm includes a combination of *ex ante* and *ex post* regulatory measures. *Ex ante* measures include impact assessments, in the form of privacy impact assessments or, as recommended in relation to AI systems by the Australian Human Rights Commission (AHRC) in its report on *Human Rights and Technology,* human rights impact assessments.[5] Such assessments

[2] Graham Greenleaf, *Asian Data Privacy Laws* (OUP, 2014); Graham Greenleaf and Bertil Cottier, 'International and regional commitments in African data privacy laws: A comparative analysis' (2022) 44 *Computer & Security Law Review* 1.
[3] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019).
[4] European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence,* COM(2021) 206 final, 21 April 2021.
[5] Australian Human Rights Commission, *Human Rights and Technology,* Final Report (June 2021).

should be applied to processing systems that present high risks. *Ex ante* regulation also incorporates the important principles of data protection by design and by default (DPbDD), a version of which is enacted in Article 25 of the GDPR. This submission has more to say about DPbDD below.

Ex ante regulatory measures should be designed, as much as possible, to ensure that privacy protection is embodied in the technologies themselves. However, as software-based technologies, such as AI systems and IoT devices, are subject to fundamental change over time, it is important to apply *ex post* regulatory measures. The most important *ex post* measures are ongoing monitoring, and the ability to conduct audits in order to ensure regulatory compliance. Appropriately targeted system auditing is essential to transparency and accountability.[6] Both *ex ante* and *ex post* regulatory measures must be supported by appropriate regulatory powers of investigation and enforcement, including the availability of sanctions.[7]

Given the scale of contemporary data practices, it is unfeasible for all socio-technical systems to be subject to high levels of *ex ante* and *ex post* regulation: regulators have limited resources. The new regulatory paradigm, as embodied in initiatives such as the EC proposal to regulate AI systems and the AHRC report on *Human Rights on Technology,* is to apply a 'risk-based' approach to regulation. Under this approach, regulation – and regulatory resources – are targeted at technologies that pose the greatest risks.[8] For example, the EC's proposed AI Regulation would draw a distinction between AI systems that pose an unacceptable risk, high risk systems, and systems with low or minimal risk. While systems with an unacceptable risk would be prohibited, regulatory measures would target high risk systems, with low risk systems subject to less regulation.

The DP includes proposals that fit within this new regulatory paradigm, but does not address the features of the emerging paradigm in a cohesive manner.

2. 'Risk-based' Regulation

Submissions on the *Issues Paper* proposed that certain collections, uses or disclosures of personal information presented such high risks that they should be more tightly regulated or prohibited

[6] Thomas Pasquier et al, 'Data provenance to audit compliance with privacy policy in the Internet of Things' (2018) 22 *Personal Ubiquitous Computing* 333.
[7] For a similar approach in the context of the regulation of AI systems see: K. Yeung, A. Howes and G. Progebna, 'AI Governance by Human-Rights Centred Design, Deliberation and Oversight: An End to Ethics Washing' in M. Dubber and F. Pasquale (eds), *The Oxford Handbook of AI Ethics* (OUP, 2019).
[8] See, for example, R. Gellert, 'Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative' (2015) 5 *International Data Privacy Law* 3.

entirely.[9] The DP identifies options for dealing with 'high risk' acts and practices, which might include prohibitions (or 'no go zones') or greater protections ('proceed with caution').

The two options identified by the DP are:[10]

Option 1

APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:

- *Direct marketing, including online targeted advertising on a large scale;*
- *The collection, use or disclosure of sensitive information on a large scale;*
- *The collection, use or disclosure of children's personal information on a large scale;*
- *The collection, use or disclosure of location data on a large scale;*
- *The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software;*
- *The sale of personal information on a large scale;*
- *The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale;*
- *The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects; or*
- *Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.*

Option 2

In relation to the specified restricted practices, increase an individual's capacity to self-manage their privacy in relation to that practice.

Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted practices, or by ensuring that explicit notice for restricted practices is mandatory.

[9] DP, p. 94.
[10] DP, pp. 95-6.

The *DP* also sought feedback on whether there is a case for prohibiting certain acts and practices, or 'no go zones'.[11] The acts and practices considered to present risks that might justify prohibitions include: profiling and behavioural advertising knowingly directed at children, the scraping of personal information from online platforms, the tracking and sharing of mental health information other than by the individual's own health service providers, or the use of information about an individual's emotional stress, mental or physical health or financial vulnerability that is shown to cause harm or discrimination.

Given the substantial limitations of the privacy self-management, or 'notice and consent' model, Option 2 is not a feasible approach for effectively regulating high risk acts and practices. Nevertheless, in order to deal with the challenges of regulating contemporary data practices at scale, there is potential in calibrating regulation in accordance with the 'risk' posed by particular acts and practices. Unlike Option 1, however, which merely proposes that APP entities that engage in 'restricted practices' must take 'reasonable steps' to identify and mitigate risks, there is a case for imposing a tiered system of regulation, similar to that in the EC's proposed AI Regulation; for example:

- Acts and practices that present unacceptable risks would be prohibited ('no go' zones);
- Acts and practices that present high risks would be subject to greater levels of *ex ante* and *ex post* regulation ('proceed with caution'), including privacy impact assessments, audits and greater regulatory obligations;
- Acts and practices that present low risks would be subject to less regulation, but would still need to comply with the baseline APPs or a relevant privacy code.

In addition to assisting with focussing regulatory resources, a more highly calibrated or tiered approach to regulation could address issues arising from the removal of the current exceptions in the PA. For example, in considering the case for removing the small business exception, the DP examines the option of retaining the exception, but prescribing further high risk acts and practices.[12] While the flexibly embedded in a principles-based approach, such as the APPs, already arguably embodies a 'risk-based' approach, more expressly recognising this would alleviate potential concerns about the costs of removing the small business exception, while ensuring that high risk acts and practices engaged in by small business do not escape regulation.

[11] DP, p. 96.
[12] DP, pp. 46-7.

Acknowledging the limitations of privacy self-management, in chapter 10 the DP proposes a new 'fair and reasonable' standard, whereby the collection, use or disclosure of personal information would be required to be fair and reasonable 'in the circumstances'.[13] As explained subsequently, there is a good case for implementing a new 'fair and reasonable' test. The test, however, needs to be supplemented by measures for assessing whether acts and practices comply with the standard. A 'risk-based' approach can supplement the proposed new standard by adding certainty to its application. For example, a list of high risk acts and practices could be regarded as presumptively unfair, so that the onus for justifying them shifts to the APP entity.

While there is scope for improving the effectiveness of the PA by more expressly calibrating regulation in accordance with the risks posed by data processing acts and practices, it is important to bear in mind the limitations and problems with applying purely risk-based approaches. For example, risk-based regulation can easily degenerate into crude cost-benefit analysis, which fails to give due consideration to all risks, including unpredictable and systemic risks.[14] In addition, what amounts to a 'risk' necessarily embodies choices about social and political values.[15] Moreover, a purely cost-benefit calculus may be inconsistent with regulation aimed at protecting human rights, such as the right to privacy, which must take into account intangible and difficult to quantify effects of acts and practices. In other words, activities ostensibly categorised as low risk may well result in privacy breaches. The status of privacy as a 'right' under international and Australian law is dealt with later in this submission.

Questions

Based upon the above, this section of the submission addresses a number of questions posed by the DP.

- *Are there further high privacy risk acts and practices that should be prescribed as exceptions to the small business exemption?*[16]

The DP refers to a list of data processing practices that are 'likely to result in high risk' that is maintained by the UK ICO for the purpose of determining whether the practice requires a data

[13] DP, Proposal 10.1, p. 85.
[14] See D. Clifford and J. Ausloos, 'Data Protection and the Role of Fairness' (2018) 37(1) Yearbook of European Law 130.
[15] See, for example, Robert Baldwin & Julia Black, 'Driving priorities in risk-based regulation: What's the problem' (2016) 43(4) *Journal of Law and Society* 565; Maria Eduardo Goncalves, 'The risk-based approach under the new EU data protection regulation: a critical perspective' (2020) 23(2) *Journal of Risk Research* 139.
[16] DP, p. 49.

protection impact assessment.[17] The list is a helpful starting point for determining high risk practices, but requires further work. For example, if a comprehensive risk-based approach were to be applied, a subset of the activities classified as high risk – such as facial recognition (in some contexts) or manipulative data use targeting vulnerable people – might be considered to pose unacceptable risks, and therefore prohibited.

- *Would the introduction of specified restricted and prohibited practices be desirable?*
- *Should restricted practices trigger a requirement for APP entities to implement additional organisational accountability measures, or should individuals be provided with more opportunities to self-manage their privacy in relation to such practices?*
- *What acts and practices should be categorised as a restricted and prohibited practice, respectively?*
- *Should prohibited practices be legislated in the Act, or developed through Commissioner-issued guidelines interpreting what acts and practices do not satisfy the proposed fair and reasonable test, following appropriate public consultation?*[18]

In the context of contemporary data practices that pose considerable risks to individuals and society, it is necessary for some acts and practices to be restricted or prohibited. As explained above, self-management of high risk acts and practices is unlikely to be effective. Moreover, there is a case for greater regulation of high risk acts and practices, which would involve additional accountability measures, such as greater documentation and PIAs.

As envisaged by the DP, prohibited practices may include those specifically targeted at vulnerable groups, such as children. It may be that there is a case for prohibiting some practices pending an assessment of an emerging technology or business practice. For example, considerable resources are being expended on neuro-measurement techniques, which can be used for concerning manipulative purposes. It may be that some practices using these techniques should be prohibited until the implications for individuals and society become clearer. This suggests that, while legislation is needed to prohibit or restrict certain acts and practices, there is a need for flexibility in specifying practices that pose an unacceptable or high risk. This could be achieved by delegated legislation, such as regulations or ministerial determinations.

[17] DP, p. 47.
[18] DP, p. 97.

3. Data Privacy by Default and Design

Although Article 25 of the GDPR purports to incorporate the principles of DPbDD, it is formulated at a high level of generality. There have been disagreements about what the Article means, and difficulties in translating the principles into practice. In practice, it seems to be little more than a catch-all provision, requiring only compliance with other substantive provisions of the GDPR.[19] In addition, even apart from the vague language used in Article 25, there are competing conceptions of 'privacy by design'.[20]

That said, on a proper understanding, 'privacy by design' is one of the most significant regulatory tools for protecting data privacy, as it is aimed at ensuring that privacy is taken into account in all stages of product design and deployment. In other words, the best way to protect data privacy is to address the problem at source.

The DP addresses the principle of 'privacy by design' mainly in chapter 10, which deals with 'Organisational Accountability'. Referring to the Explanatory Memorandum to the 2012 amending bill, the DP explains that APP 1 was intended 'to keep the Privacy Act up-to-date with international trends that promote a 'privacy by design' approach, that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception'.[21] However, a number of submissions to the *Issues Paper* supported a more explicit 'privacy by design' approach in the PA.

APP 1.2 suffers from a similar defect to Article 25 of the GDPR, in that it does no more than impose an obligation to comply with the existing APPs. 'Privacy by design', however, goes beyond mere compliance with existing data privacy principles. It is also broader than merely organisational accountability. It requires privacy to be taken into account at all stages of the process of designing a new product or service, which extends to implementing appropriate organisational arrangements, training and record-keeping; but also requires a comprehensive privacy management program which, where appropriate, would require PIAs by independent third parties.

Privacy by default, which requires that defaults are set to the highest privacy protections, complements the principle of privacy by design. The importance of default settings were explained in a 2018 ENISA report in the following terms:

---

[19] *Ibid.* 167. This also seems to be the interpretation adopted by the European Data Protection Board in its guidelines on Article 25: European Data Protection Board, *Guidelines 4/2019 on Article 25, Data Protection by Design and by Default,* Version 2.0, Adopted on 20 October 2020.

[20] Ari Ezra Waldman, 'Data Protection by Design? A Critique of Article 25 of the GDPR' (2020) 53(1) *Cornell International Law Journal* 147, 149-151.

[21] DP, p. 150.

> When designing IT systems or IT-based services, the default settings, i.e. the properties and functionalities that are in place at the very first employment (of these systems or services) without requiring any activity or choice by the user, are of vital importance, as they constitute the basis upon which the user will initiate his or her interaction. Indeed, the default determines at least the first usage and, if users are not able or willing to change it, it further determines the ongoing use.[22]

Chapter 12 of the DP addresses pro-privacy default settings and identifies the following two options for reform.[23]

Option 1 – Pro-privacy settings enabled by default

Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.

Option 2 – Require easily accessible privacy settings

Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.

Given the limitations of privacy self-management, including the problems of information overload and consent fatigue, Option 2 would be ineffective. While Option 1 is a better reflection of the principle of 'privacy by default', more work is needed in determining how the principle would be applied in practice. In most contexts, the benefits of setting defaults at the most restrictive levels – including greater transparency and accountability for data practices – will likely outweigh the inconvenience faced by users who wish to alter the defaults. On the other hand, where data is necessary for the functioning of a product, altering defaults may impose considerable inconvenience on users. But, where data practices pose high risks – such as near ubiquitous data collection by certain IoT devices installed in the home, there is a good case for data collection to be set to 'off', so that the implications of these practices are more fully brought home to users.

Questions

[22] ENISA, *Recommendations on shaping technology according to GDPR provisions: Exploring the nation of data protection by default,* December 2018, p. 7.
[23] DP, p. 99.

- *Should pro-privacy default settings be enabled by default, or should requirements be limited to ensuring that privacy settings are clear and easy to access?*
- *If pro-privacy default settings are enabled by default, which types of personal information handling practices should be disabled by default?*

As explained above, the principle of 'privacy by default' requires defaults to be set to those that are the most privacy protective. This is a general principle, which supplements the principle of 'privacy by design', and should be applied to all information handling practices. The application of the principle, however, must depend upon context. For example, if data processing is absolutely necessary for the functioning of a product, then requiring settings to be altered would create unnecessary frustration for consumers. However, where data handling practices pose a high risk, there is a good case for settings to be pre-selected to 'off', even if this might mean disabling some product functionality.

Overall, the principles of DPbDD should be codified in the PA; but, to be effective, more work is needed to avoid the problems encountered with Article 25 of the GDPR.

4. Is there a Right to Privacy?

Some submissions to the *Issues Paper* contended that the objects of the Act should expressly recognise the 'right to privacy'. In response, referring to Article 17 of the ICCPR, the DP states that:

> It is not appropriate for the objects to refer to a 'right to privacy' because, despite common parlance, Art 17 does not confer such a right, nor does it amount to absolute protection.[24]

This requires comment. In May 1948, the Australian delegation was responsible for the first proposal for the protection of a right to privacy in the precursor of the ICCPR.[25] Article 17 of the ICCPR states that:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the *right* to the protection of the law against such interference or attacks (emphasis added).

[24] DP, p. 20.
[25] Oliver Diggelmann and Maria Nicole Cleis, 'How the Right to Privacy Became a Human Right' (2014) 14 *Human Rights Law Review* 441, 450.

This is universally regarded as conferring a right to privacy. As CCPR General Comment No. 16, adopted at the thirty-second session of the Human Rights Committee on 8 April 1988, and which expressly refers to Article 17 as a 'right to privacy', puts it:

> Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour and reputation. In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.[26]

The GC explained the application of the Article 17 right to what has become known as 'data protection' or 'information privacy' in the following terms:

> The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[27]

The relationship between Article 17 and the PA was explained by the ALRC in its Report No. 108:

> … the Preamble to the Privacy Act makes clear that the legislation was intended to implement, at least in part, Australia's obligations relating to privacy under the ICCPR.

[26] CCPR General Comment No. 16: Article 17 (Right to Privacy) *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation,* adopted at the thirty-second session of the Human Rights Committee on 8 April 1988, [1].
[27] Ibid, [10].

> The Privacy Act, however, is concerned with information privacy only, and therefore is not a full implementation in domestic law of the meaning of art 17.[28]

While not entirely clear, the comments in the DP could be interpreted as inferring that protecting privacy as a right would confer 'absolute' protection. Rights, and especially rights such as that protected under Article 17, are not absolute – and that is clearly recognised by the qualifications in the wording of Article 17.

The DP makes the following proposal in relation to the objects of the PA:

> Amend the objects in section 2A, to clarify the Act's scope and introduce the concept of public interest, as follows:
> (a) to promote the protection of the privacy of individuals *with regard to their personal information*; and
> (b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities *undertaken in the public interest*.

Recognising a right to privacy in the objects of the Act would be to do no more than implement Australia's obligation to give effect to Article 17 of the ICCPR, in the particular context of information privacy. The DP proposal to introduce a concept of 'public interest' in s. 2A(b) may bear the risk that the interests of those engaged in data processing are regarded as being in the 'public interest' while the protection of privacy is not – when there is clearly a public interest in protecting privacy. Express recognition of a right to privacy in the objects of the PA would also assist with the balancing exercise required to be undertaken in interpreting principles-based legislation such as the PA, as it could import the principle of proportionality. This could, for example, assist in giving substance to the proposed new 'fair and reasonable' test for data processing.[29] Statutory recognition of a right to privacy could therefore be further reinforced by expressly referring to 'proportionality' (rather than 'balancing') in paragraph 2A(b). As was pointed out by Bell J in *Jurecek,*[30] which is referred to in the DP,[31] the *Information Privacy Act 2000* (Vic) was intended 'to give effect in a particular context to the right to privacy stipulated in art 17 of the ICCPR' and 'reasonable proportionality is a central

[28] ALRC, *For Your Information: Australian Privacy Law and Practice,* May 2008, [74.15].
[29] See DP, p. 88; European Data Protection Supervisor, *Assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (December 2019).
[30] *Jurecek v Director, Transport and Safety Victoria* [2016] VSC 285, [69]-[70].
[31] DP, p. 88.

component of that right'. These comments are clearly as applicable to the PA as they are to the Victorian legislation.

5. Personal Information

The majority of submissions to the *Issues Paper* favoured aligning the definition of 'personal information' with the GDPR definition. The DP identifies two main issues with the current definition: uncertainty about whether the definition encompasses, firstly, technical and, secondly, inferred information.[32] To address these deficiencies, the DP recommends including both technical and inferred information, proposing the following revised definition:

> *Personal information means information or an opinion that relates to an identified individual, or an individual who is reasonably identifiable:*
> *a) whether the information or opinion is true or not; and*
> *b) whether the information or opinion is recorded in a material form or not.*
> *An individual is 'reasonably identifiable' if they are capable of being identified, directly or indirectly.*[33]

In addition, the DP proposes the following amendments to support the new definition:

- a non-exhaustive list of the types of information capable of falling within the new definition of personal information
- defining 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly; and including a list of objective factors to assist APP entities to determine when an individual is 'reasonably identifiable'; and
- amending the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

By removing any reference to information being 'about an individual', amending the definition in the way proposed by the DP would address the serious problems arising from the *Telstra* decision,[34] and ensure that the Privacy Act is better equipped to address contemporary data practices. It would also make the Australian Act more consistent with data privacy laws in comparable jurisdictions, including the GDPR.

[32] DP, pp. 21 ff.
[33] DP, p. 26.
[34] *Privacy Commissioner v Telstra Corporation Ltd* (2017) 249 FCR 24.

While the suite of changes to the definition of 'personal information' proposed in the DP would be an improvement, they do not resolve all issues relating to the application of the Act to contemporary data practices. A key problem that arises from attempts to distinguish between personally identifying data and other data is that the combination of mass, indiscriminate collection of data and advances in data analytics mean that almost all data that is collected may potentially both identify and 'relate to' an individual. As Purtova has argued, 'in the age of the Internet of Things, datafication, advanced data analytics and data-driven decision-making, any information relates to a person in the sense of European data protection law'.[35] Moreover, targeting of individuals (or 'individuation') – such as by online profiling and advertising – can cause privacy harms regardless of whether or not an individual is identifiable. The challenges posed by these practices do not mean that an unduly narrow definition should be applied to the concepts of 'personal information' or 'personal data' – which would result in an inadequate level of privacy protection – but that the problem of 'scale' is a difficult problem that requires careful policy consideration.

Two possible solutions to the challenge of ensuring the scalability of data privacy law in the face of contemporary data practices have been canvassed:[36]

1. Retain a broad definition of personal data or personal information, but scale the intensity of data protection obligations to match the risks associated with the data; or
2. Abandon the attempt to distinguish between personal data and 'non-personal' data altogether, and establish a new system of calibrated, scalable data privacy obligations, regardless of whether the information is 'personally identifiable'.

Apparently in recognition of the difficulties arising from attempts to define the scope of data privacy laws by reference to personal identifiability, the privacy safeguards under the Consumer Data Right (CDR) regime are not confined to 'personal information', but apply to 'CDR data', which is specified in instruments that designate a sector as being subject to the regime.[37] The instrument designating the banking sector, for example, specifies information that goes beyond personal information to include information about financial products and uses of products.[38]

---

[35] Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10(1) *Law, Innovation and Technology* 40, 42.

[36] Paul M. Schwartz and Daniel J. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86(6) *New York University Law Review* 1814; Bert-Jaap Koops, 'The trouble with European data protection law' (2014) 4(4) *International Data Privacy Law* 250; Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10(1) *Law, Innovation and Technology* 40.

[37] *Competition and Consumer Protection Act 2010* (Cth) s. 56AI(1).

[38] Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 (Cth).

Despite these problems, there remains a need for data privacy laws to distinguish between regulated and unregulated information (or data). To ensure that the PA properly accommodates contemporary data practices, a broad approach is required in defining the scope of information falling within the Act. The DP proposals for reforming the definition of 'personal information' focus on the risk of identifiability (as embodied in the 'reasonably identifiable' test). The focus of the definition should, however, be on the privacy risks or harms posed by the information or data, which are not necessarily confined to identifiable data. This suggests that, as proposed by Salinger Privacy in its submission to the *Issues Paper,* the definition should extend beyond identifiability to include 'individuation'.[39] To minimise the regulatory imposts by adopting a broad approach to the scope of the Act, consideration should be given to drawing distinctions based upon the risks posed by particular kinds of information or data.[40]

Applying the above approach, the definition proposed in the DP should be modified in a number of ways. First, the definition should apply to identifiable information, regardless of whether or not identification is 'reasonable' and, instead, an approach adopted based on the risks of identifying a person. This approach would ensure that the definition is consistent with the DP's proposal that the Act be amended to require personal information to be 'anonymous', and not merely 'de-identified', before it is no longer protected by the Act.[41] As proposed in the DP, certainty in the application of the definition can be assisted by including a non-exhaustive list of identifiable information. To ensure that 'inferred' or 'generated' information is included in the definition, this should be included in the list. Including inferred or generated information within the definition is necessary as the consequences of the use of this information are effectively indistinguishable from the use of other personal information. Secondly, to ensure that the Act applies to all information of concern, a concept of 'individuation' – meaning information used to separate out a person for individual treatment, regardless of whether it is possible to identify a person from the information – should be added to the definition. If this is considered a step too far, further consideration should be given as to how this form of information, which can have serious effects for individuals, can be regulated. Thirdly, while the DP states that the proposed new definition of 'collection' is intended to encompass inferred and generated information,[42] it should be made clear that the *act* of 'collection' extends to the *acts* of

[39] DP, p. 23.
[40] For a similar approach see Ian Opperman (ed), *Privacy Preserving Data Sharing Frameworks,* Australian Computing Society, 9 August 2019.
[41] DP, p. 31.
[42] DP, p. 28.

inferring and generating personal information. Fourthly, in relation to the definition of 'sensitive information', it is clear that some of the information identified by the DP in its discussion of potential 'no go zones' – such as information that enables targeting of children – poses considerable risks. This indicates a need to ensure consistency between the definition of 'sensitive information' and any potential 'no go' or 'proceed with caution' zones. Moreover, the extent to which the existing categories of 'sensitive information' may be inferred from other information confirms the importance of ensuring that the definition of 'personal information' clearly extends to inferred information.

6. Exemptions from the Act

As a general principle, the PA should apply to data processing that presents risks to the privacy of individuals, regardless of the identity of an entity responsible for the processing. Moreover, as the DP notes, changes in technologies and business practices mean that entities, such as small businesses, are more likely to engage in data processing at scale. There is therefore a good case for removing the current exemptions for small businesses, employee records and registered political parties/political acts and practices. These reforms would be a significant step in bringing Australian law more into line with data privacy laws in comparable jurisdictions and would assist in Australia obtaining an adequacy decision from the European Commission.

In relation to small businesses, the main concern has been the compliance burden imposed by bringing small businesses with the scope of the Act. This can be addressed by providing resources to assist SMEs in ensuring that their practices comply with the Act and, in addition to the flexibility already provided by the APPs, targeting regulation at the practices that pose the most risk. As, after careful consideration, the ALRC concluded in Report No. 108, the exemption for small business is 'neither necessary nor justifiable'.[43]

In relation to the employee records exemption, the main objections to removing the exemption have been compliance costs and potential issues in managing the employment relationship arising from employee access to records. Given the risk posed by employee records, which can include highly sensitive information, such as health information, ALRC Report No. 108 concluded that the exemption should be removed.[44] As the ALRC pointed out, the exceptions to the access and correction principle in the PA are generally sufficient to ensure that employers are not required to

[43] ALRC, *For Your Information: Australian Privacy Law and Practice,* May 2008, [39.139].
[44] *Ibid.* [40.121].

disclose sensitive or confidential information to employees. If, however, the employee records exemption were to be removed APPS 12-13 could be tweaked to alleviate any remaining concerns.

In relation to the exemptions for political parties, as pointed out in submissions to the *Issues Paper,* the Facebook-Cambridge Analytica scandal illustrated the dangers of some of the potentially manipulative data practices engaged in by operatives for political parties. These potential practices are not only a threat to privacy, but to democracy and freedom of expression. The main justification for the exemptions has been that they encourage freedom of political communication and democratic processes. As the ALRC pointed out in Report No. 108, '(c)ompliance with … [the PA] … by those agencies and organisations engaged in the political process will promote – rather than impede – public confidence in the democratic process'.[45] The ongoing development of concerning techniques for exploiting databases on personal information for political purposes since the publication of the ALRC report only serves to reinforce the conclusion that the exemptions should be removed.

7. Notice and Consent

The PA, like other data privacy laws, remains anchored in the general principle of data autonomy or 'privacy self-management': that individuals should be free to consent to the collection, use and disclosure of personal information.[46] In practice, however, the notice and consent model does not work. Confronted with complex privacy policies, people do not generally read notifications of data collection and processing policies. Moreover, people are often willing to 'consent' to data processing practices in return for convenient access to products or services; or consent is illusory, as there is no alternative but to consent in order to acquire a product or service. As the ACCC concluded in the DPI report:

> … privacy self-management tools that rely on consumers to read privacy policies and provide consent may no longer be sufficient, in themselves, to provide consumers with adequate data protection and privacy in a digital economy. The size of the task facing those consumers who want to provide truly informed consent suggests that it may be necessary to shift more of the responsibility for data protection and privacy on to the entities collecting, using, and disclosing personal information.[47]

[45] *Ibid.* [41.57].
[46] See DP, p.80.
[47] *DPI* Report, p. 478.

Similarly, Solove has pointed to the range of problems with the privacy self-management model, which together mean that it 'does not provide people with meaningful control over their data'.[48] First, behavioural science research reveals that individuals often do not make rational choices about the processing of their personal data. Secondly, structural problems inhibit self-management of privacy: so much data is collected about individuals that people suffer from information overload; and it is difficult for individuals to weigh the costs of privacy harms when the costs of each individual privacy harm might be relatively small, but the cumulative societal costs of privacy harms when taken together are significant.[49]

As Solove has further pointed out, the typical response to the failure of privacy self-management is to attempt to improve notice and consent, but this can give rise to dilemmas. First, there is the 'consent dilemma', which refers to how making consent more difficult can potentially mean denying freedom of choice or, as Solove puts it, '(p)rivacy scholars must identify a conception of consent that both protects privacy and avoids paternalism'.[50] Secondly, making notices simpler and easier to understand risks resulting in people not being fully and accurately informed of the consequences of data collection and processing.[51] On the other hand, there are the well-known dilemmas facing consumers of 'notice fatigue' and 'consent fatigue'.

The DP included the following proposals for enhancing the notice and consent provisions in the PA:

- Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.[52]
- Standardised privacy notices could be considered in the development of an APP code … including standardised layouts, wording and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of standardised notices.[53]
- Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable, as soon as possible after collection, unless:
    - the individual has already been made aware of the APP 5 matters; or
    - notification would be *impossible* or would involve *disproportionate effort*.[54]

[48] Daniel J. Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880, 1880.
[49] *Ibid.* 1880-81.
[50] *Ibid.* 1894.
[51] *Ibid.* 1885.
[52] DP, p. 69.
[53] DP, p. 71.
[54] DP, p. 73.

- Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.[55]
- Standardised consents could be considered in the development of an APP code …, including standardised layouts, wording, icons or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consents.[56]

Taken together, the proposed reforms would improve the effectiveness of the 'notice and consent' regime by imposing greater obligations on APP entities to inform users of data practices and obtain consent. Some comment should, however, be made on the relationship between the proposals and the inherent limits of the 'notice and consent' model. The difficult balance to be struck involves providing people with meaningful information and meaningful consent without over-burdening them; and this can be done (even if only in part) by enhancing the regulatory requirements for notice and consent. The DP therefore proposes the increased use of standardised layouts, wording, icons or consent taxonomies. At the same time, given the diverse contexts in which consent may be required, the DP cautions that 'it is likely to be impractical to develop consent templates, icons or phrases across all sectors'.[57]

While it is common for claims to be made that improvements can be made to notifications provided to consumers through systems such as the use of standardised icons, designing and implementing effective systems is complex.[58] Warren, Mann and Harkin have recently found that there are 'mixed views' about the value of certain privacy icons in promoting awareness of privacy issues; and that, while consumers and other stakeholders may find the idea of icons to be appealing, other regulatory reforms may be more effective.[59] That said, properly designed systems aimed at simplifying information provided to consumers can have an effect, but sufficient resources must be expended on consumer comprehension testing to ensure that the systems are robust.

The current Australian law reform process should take advantage of reforms in other comparable jurisdictions. For example, 2021 amendments to the California Consumer Privacy Act clarified the

[55] DP, p. 78.
[56] DP, p. 79.
[57] DP, p. 79.
[58] L. F. Cranor, 'Informing California Privacy Regulations with Evidence from Research', (2021) 63(3) Communications of the ACM 29-32, https://cacm.acm.org/magazines/2021/3/250700-informing-california-privacy-regulations-with-evidence-from-research/fulltext.
[59] Ian Warren, Monique Mann and Diarmaid Harkin, *Enhancing Consumer Awareness of Privacy and the Internet of Things,* August 2021.

definition of 'consent' by identifying actions that would *not* amount to valid consent.[60] Importantly, the amendments provided that 'agreement obtained through the use of dark patterns', essentially meaning a user interface designed to manipulate consumers into an appearance of consent, would not amount to valid consent. Once again, this reform draws attention to the potential use of design elements to influence or manipulate consumers. While the DP's proposed reforms should be welcomed, they may be improved by including a non-exhaustive list of what does not constitute valid consent.

8. The Proposed New 'Fair and Reasonable' Test

In its submission to the *Issues Paper,* the OAIC observed that '(t)he burden of understanding and consenting to complicated practices should not fall on individuals but must be supported by enhanced obligations for APP entities that promote fair and reasonable personal information handling or organisational accountability'.[61] Acknowledging the limitations of the 'notice and consent' model, and that the current APPs confer considerable discretion on APP entities, the DP proposes additional protections to ensure minimum acceptable standards for the processing of personal information. In particular, the DP proposes that:

> A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.[62]

In formulating this proposal, the DP rejected the application of the 'legitimate interest' test under Article 6(1)(f) of the GDPR largely on the basis that the GDPR test incorporates a balancing of rights and interests under the EU rights-based legal regime, which cannot be readily transposed into the Australian legal context. Nevertheless, the test proposed in the DP draws on standards in other data privacy laws, such as Article 5(1) of the GDPR, which provides that:

> Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The 'fair and reasonable' test is obviously a flexible standard and, as such, requires guidance as to how it would apply in practice. To address this, the DP proposed a non-exhaustive list of legislative

[60] See https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB694.
[61] DP, p. 82.
[62] DP, p. 85.

factors to be taken into account in determining whether processing of personal information is fair and reasonable. The factors proposed by the DP are as follows:

- Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances;
- The sensitivity and amount of personal information being collected, used or disclosed;
- Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information;
- Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity;
- Whether the individual's loss of privacy is proportionate to the benefits;
- The transparency of the collection, use or disclosure of the personal information; and
- If the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child.[63]

The introduction of a new 'fair and reasonable' standard for data processing is one of the most significant proposals arising from the DP. While it has considerable potential for improving the protection afforded by the Act, much depends upon how it is formulated and implemented. As referred to previously in this submission, certainty in the application of the proposed new standard could be improved by linking it to a 'risk-based' paradigm. On this approach, certain forms of data processing might be regarded as 'unfair' by definition, and therefore prohibited. Other forms of data processing might be regarded as so risky that they are presumptively unfair, with the onus of justifying the processing shifting to the APP entity. Compliance of other forms of data processing with the new standard would then be left to be assessed by applying the proposed statutory factors.

It is worth noting that some of the proposed statutory factors – such as the sensitivity and amount of personal information being processed; and whether there is a foreseeable risk of unjustified adverse impacts or harms – envisage a form of risk assessment. Especially in the context of complex systems for processing and analysing personal data, the 'foreseeable risk' factor raises the question of whether data processing should be regulated regardless of whether or not the risks are 'foreseeable'. A better way of formulating this factor, which would make it abundantly clear that the test is objective and not subjective, may therefore be as follows:

[63] DP, p. 89.

whether the collection, use or disclosure of personal information poses a risk of adverse impacts or harms to individuals.

The proposed list of statutory factors, as with other elements of the APPs, obviously require a degree of 'balancing'. A balancing exercise such as this can be improved by increased certainty about what is being 'balanced' and how the balancing exercise is to be undertaken. This is better than an open-textured 'shopping list' of unranked factors. One way to enhance the balancing process envisaged by the statutory factors would be to expressly recognise the PA as protecting a right to privacy (or a right to data privacy) in the objects clause. This would, for example, potentially add some rigour to the application of the 'proportionality' principle as one of the legislative factors – which could be re-formulate to read 'whether an infringement of the right to privacy is proportionate to the benefits'. In any case, the reference to 'an individual's loss of privacy' in that factor seems to be too narrowly drawn – and does not fully capture what the PA is designed to protect. In the absence of a reference to a right to privacy, the factor could be reasonably reformulated to 'whether an interference with privacy is proportionate to the benefits'.

9. Additional Protections

In addition to linking the proposed new 'fair and reasonable' test to a tiered risk-based regulatory approach – with some practices prohibited and some presumed to be 'unfair' – the proposed new standard should be linked to the principles of a codified PbDD. The *Issues Paper* sought specific feedback on the following question:

> *How can the personal information of individuals be protected where IoT devices collect personal information from multiple individuals?*[64]

This raises complex issues, as IoT devices installed in the home, such as personal digital assistants, may potentially engage in wide-scale collection of personal information, including information about household members other than the purchaser, and about visitors and guests. Under the proposals raised in the DP, this would presumably be addressed by the proposed new 'fair and reasonable' standard. The proposed new standard would go some way to address problems posed by the potentially unconstrained collection of personal information by domestic IoT devices. For example, in elaborating on the 'reasonable expectations' factor, the DP explained that:

[64] Attorney-General's Department, Privacy Act Review, Issues Paper (October 2020), Question 34, p. 49.

> It is likely that certain kinds of information would attract higher expectations from an objective reasonable individual, for example, sensitive information or IoT smart home data, the handling of which may require a higher standard of privacy protection.[65]

It is generally acknowledged that IoT applications, especially for IoT devices installed in the home, are 'high risk'.[66] Moreover, many purchasers and users of IoT devices installed in the home are ignorant or uncertain of the amounts of data collected by such devices. In this context, it is doubtful whether the 'fair and reasonable' processing principle, unaided, could effectively deal with the issue. However, a more effective approach might be possible if the 'fair and reasonable' standard were to be linked to the principle of 'privacy by default'. For example, the 'fair and reasonable' standard could be supplemented by requiring certain data collection settings by IoT devices installed in the home to be pre-selected to 'off' by default. This would have the effect of ensuring that purchasers of such devices would need to make conscious decisions before enabling data collection and processing that poses substantial risks to privacy. In these circumstances, the benefits of alerting consumers to concerning or risky privacy practices would likely outweigh the inconvenience of requiring consumers to change default settings. The proposed 'fair and reasonable' standard could be linked to the principle of 'privacy by default' by including default settings as a factor to be taken into account in determining whether the standard has been complied with, or by providing that compliance with the principles of PbDD result in a rebuttable presumption that data processing is 'fair and reasonable'.

10. The Data Security Principle and 'Joined-up Regulation'

APP 11 embodies the data security principle, with APP 11.1 requiring APP entities that hold personal information to take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorized access, modification or disclosure. While the DP supports retaining a principles-based and technology neutral security principle, it canvasses proposals for increasing the certainty of the 'reasonable steps' test. In particular, the DP includes the following proposals:

- Amend APP 11.1 to state that 'reasonable steps' includes technical and organisational measures.
- Include a list of factors that indicate what reasonable steps may be required.[67]

[65] DP, p. 86.
[66] See DP, p. 47, citing European Data Protection Board, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020.
[67] DP, p. 146.

The proposals for introducing amendments to increase the certainty of the 'reasonable steps' test are welcome. However, given the fundamental importance of enhancing data security for all, it is important to ensure that security requirements imposed by distinct legal regimes are both coherent and cohesive. Data security is not simply a matter for data privacy laws – and there are a variety of other laws (such as potentially protections under the Australian Consumer Law, as well as the Code of Practice for consumer IoT devices[68]) and technical standards that are relevant. To address the problems of regulatory inconsistency in regulating new technologies, the World Economic Forum (WEF) has recommended applying the concept of 'joined-up regulation'. As the WEF puts it:

> While individual regulations may be designed and administered in a proportionate way, gaps and overlaps with other regulations may lead to worse policy outcomes, while creating unnecessary complexity, cost and delay. The use of common analytical approaches and models for all regulatory impact assessments can support a better understanding of the cumulative impacts of different regulations.[69]

One way to enhance cross-regulatory consistency in relation to the data security principle would be to expressly link APP 11.1 to other relevant data security laws, such as any potential laws arising from the current Home Affairs process aimed at strengthening Australia's cyber security regulations and incentives.[70] In any case, given the centrality of data processing to contemporary business practices, it would be helpful for the final report to give more attention to the challenge of 'joined-up' regulation across regulatory regimes. This challenge is clearly important for a variety of areas relevant to the current inquiry, such as consumer protection/privacy/data security labelling of devices, or the appropriate scope of impact assessments (such as PIAs or human rights impact assessments) for 'high risk' activities.

11. Direct Right of Action

As the DP notes, the majority of submissions to the *Issues Paper* that considered the issue favoured introducing a right of action for individuals to directly enforce the obligations imposed on APP entities under the PA.[71] The availability of a direct right of action would increase incentives for compliance with the Act, assist with the problem of under-resourcing of the regulator (the OAIC) and

[68] Department of Home Affairs, Australian Signals Directorate & ACSC, *Code of Practice: Securing the Internet of Things for Consumers,* 2020.
[69] World Economic Forum (WEF), *Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators* (December 2020), p. 40.
[70] See Australian Government, *Strengthening Australia's cyber security regulations and incentives,* Camberra, 13 July 2021.
[71] DP, p. 186.

create a much-needed body of jurisprudence on the interpretation of the PA. Under the model proposed in the DP, the proposed direct right of action would have the following elements:

- The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.
- The action would be heard by the Federal Court or the Federal Circuit Court.
- The claimant would first need to make a complaint to the OAIC (or FPO) and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman.
- The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application.
- The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.

Question

Is each element of the proposed model fit for purpose? In particular, does the proposed gateway to actions strike the right balance between protecting the court's resources and providing individuals a more direct avenue for seeking judicial consideration and compensation?

As the DP effectively acknowledges, the benefits of introducing a direct right of action overwhelmingly outweigh any potential disadvantages. These benefits would, however, be seriously undermined if the ability of individuals to enforce their rights under the Act were curtailed by unnecessary hurdles. Under the model proposed in the DP, an individual would first need to make a complaint to the OAIC and have it assessed for conciliation before having the possibility of access to a court. This model would effectively negate many of the benefits of establishing a direct right, including the benefit of conserving scarce regulatory/OAIC resources.

A complainant should have the ability to choose between pursuing a complaint before the OAIC and seeking to directly vindicate their rights before a court. Moreover, if a complainant is unsuccessful in a complaint to the OAIC, this should not result in her or him being denied the right to pursue the matter directly before a court. Courts – such as the Federal Court and Federal Circuit Court – have their own established case management systems which are designed to ensure that matters are

quickly and efficiently resolved, and which commonly include considering the suitability of ADR processes. The 'gateway' mechanism proposed in the DP is unnecessary and does not strike the right balance between protecting judicial resources and providing effective recourse for aggrieved individuals. If implemented, it would be more likely to result in unnecessary regulatory expenses and/or deny the ability of aggrieved persons to effectively enforce their rights under the PA. It should be abandoned.

This leaves aside issues relating to effective access to justice by aggrieved complainants. The resources needed to bring actions before the courts are not available to all. But, in our data-centred societies, privacy harms affect everyone. Regulatory laws, such as the PA, are only as effective as their enforcement mechanisms. And, in evaluating enforcement of the PA, it would be helpful for the final report to give more attention to issues relating to access to justice. Ideally, given how important privacy protections are for Australians, public resources would be expended on specialist legal aid to assist with advice on interferences with privacy. At the very least, consideration should be given to the potential for access to a low cost tribunal for resolving privacy complaints falling below a certain monetary threshold.

12. A statutory tort of privacy?

As has been found by a series of public inquiries that have investigated the issue in considerable depth,[72] the introduction of a statutory cause of action to protect privacy would address a long-standing gap in Australian law. While it remains open for the gap to be filled by development of the common law,[73] in reality that is so highly improbable that it may be effectively discounted. If the case for establishing a statutory cause of action for protecting privacy has not, by now, been established to the satisfaction of policy-makers by the conclusions reached by successive public inquiries and the overwhelming majority of academic experts, then there is little point in wasting further time or resources in discussing a reform that seems doomed to remain perpetually within sight, but never quite reached.

Assuming, however, that the current reform process accepts the overwhelming arguments in favour of introducing a statutory cause of action, there are important issues that arise in the design of the cause of action. These issues were canvassed at considerable length during the inquiry leading to

[72] See, for example, ACCC, *Digital Platforms Inquiry,* Final Report, June 2019; Australian Human Rights Commission, *Human Rights and Technology,* Final Report (June 2021); ALRC, *Serious Invasions of Privacy in the Digital Era,* Report 123, 2014; ALRC, *For Your Information: Australian Privacy Law and Practice,* Report 108, 2008; NSW Law Reform Commission, *Invasion of Privacy Report 120*, 2009; Victorian Law Reform Commission *Surveillance in Public Places* Report 18, 2010.

[73] *Australian Broadcasting Corporation v Lenah Game Meats* (2001) 208 CLR 199.

ALRC Report 123. The issues necessarily arise again in connection with the options for reform identified in the DP. The four options identified in the DP are as follows.

Option 1

Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.

Option 2

Introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts.

Option 3

Do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person.

Option 4

In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.

If privacy is to be adequately protected under the general law, Options 3 and 4 are simply not feasible alternatives. In relation to Option 4, the equitable action for breach of confidence does provide recourse for some privacy harms. But, even if the issue of the availability of damages for emotional distress were to be resolved by legislation, then the action does not extend to protect against all privacy harms that would fall within a statutory cause of action. For example, its application to privacy intrusions, as opposed to publications of private facts, is extremely uncertain.

In relation to Option 3, recognition of a private cause of action at common law would require a matter to come before the High Court. There seems little prospect of a suitable dispute making its way to the High Court as, quite apart from the expenses facing an aggrieved plaintiff, defendants with a vested interest in avoiding an unwelcome precedent have incentives to settle. And, even in the unlikely possibility of a suitable dispute coming before the Court, a single decision would likely raise more questions than answers. This process is simply unsuitable for evaluating the complex public policy issues – such as the balance between privacy and freedom of expression - that need to be taken into account in determining the parameters of a cause of action for breach of privacy.

Option 3 does, however, raise the important – and difficult – issue of the current exclusions from the PA for data processing undertaken by individuals in a non-business capacity. Under s 16 of the Act, the APPs do not apply to personal information that is held by an individual for the purposes of personal, family or household affairs. Moreover, under s 7B(1), acts and practices of individuals are exempted if they are engaged in otherwise than in the course of business. Given that technological developments, including the tools made available by digital platforms, have facilitated some privacy intrusions by individuals at scale, these exemptions now require further consideration. The introduction of a private cause of action would at least provide some recourse for those affected by breaches committed by individuals in their personal capacity.

While Australian courts are perfectly capable of determining the scope and application of a minimalist cause of action, the problem with Option 2 is that this would likely take considerable time and resources. And, moreover, a decision from the High Court would be required before the parameters and elements of a cause of action could be authoritatively settled. Given past experience, it seems unlikely that a sufficient threshold of actions would be brought before the courts for important elements of the law to be satisfactorily resolved within a reasonable time frame. Meanwhile, potential litigants and defendants, as well as others, would face significant legal uncertainty.

We are therefore left with Option 1 as the only reasonable and feasible alternative. Unfortunately, this option is phrased in terms that suggest that only model for a statutory cause of action is the statutory tort proposed in ALRC Report 123. The precise design of a statutory cause of action (which need not necessarily be a tort) is a matter on which reasonable minds may disagree. Following release of the ALRC Report, I published an analysis of manner of the detailed recommendation made by the ALRC in an article published in the *Privacy Law Bulletin,*[74] which I refer you to. While generally supportive of the ALRC's proposals, the article suggests some areas where, in my view, there could be scope for improvement and/or refinements to the model proposed by the ALRC. My views on the elements and parameters of a potential cause of action have not substantively changed since the publication of the article. However, in this area the perfect should not be the enemy of the good; and the long-overdue implementation of the ALRC recommendations would be a significant and welcome reform.

[74] David Lindsay, 'A privacy tort for Australia? A critical appreciation of the ALRC report on serious invasions of privacy' (2015) 12 (1&2) *Privacy Law Bulletin* 8.

That said, the precise design of a statutory cause of action does raise some important issues which have not yet received sufficient attention, especially in the context of the digital economy.[75] First, given that plaintiffs may well wish to bring actions against intermediaries, such as digital platforms, further consideration should be given to issues relating to accessorial liability for breach of a statutory cause of action. Secondly, as some defendants, such as digital platforms, will be located outside of Australia, further consideration should be given to private international law considerations, and whether there might be scope for specific rules relating the extra-territorial operation of a cause of action in this context.

[75] See David Lindsay, 'Liability of Platforms under Australian Privacy Law' (2020) 94(10) *Australian Law Journal* 752.