MONASH University

MONASH LAW

CASTAN CENTRE FOR HUMAN RIGHTS LAW

CENTRE FOR COMMERCIAL LAW AND REGULATORY STUDIES.

Attorney-General's Department Review of the Privacy Act 1988

Submission in response to the Discussion Paper

Prepared by

Yee-Fui Ng

Moira Paterson

Marilyn Pittard

Normann Witzleb

On behalf of the Castan Centre for Human Rights Law, Faculty of Law, Monash University and the Centre for Commercial Law and Regulatory Studies, Faculty of Law, Monash University

20 January 2022

I. Introduction

1. The Castan Centre for Human Rights Law at Monash University's Faculty of Law ('Castan Centre') is a world-renowned academic centre using its human rights expertise to create a more just world where human rights are respected and protected, allowing people to pursue their lives in freedom and with dignity. The Castan Centre's mission includes the promotion and protection of human rights, and it is from this perspective that we make this submission.

2. The Centre for Commercial Law and Regulatory Studies at Monash University's Faculty of Law ('CLARS') facilitates innovative research in commercial law, corporate governance and regulation. CLARS includes select academics, postgraduate students, as well as visiting scholars and international research partners. CLARS is particularly focused on issues relating to sustainability; Environmental, Social and Corporate Governance (ESG); and accountability in the commercial world, and actively engages with legal and business communities, policy makers, and regulators.

3. The Castan Centre and CLARS thank the Attorney-General's Department for the opportunity to make a submission in relation to the *Privacy Act Review – Discussion Paper* (October 2021) (the 'Discussion Paper'). Due to time limitations, this submission will focus only on selected issues arising from the exposure draft of the Online Privacy Bill.

4. The authors of this submission are all experienced academic members of the Castan Centre and of CLARS. Their specialisations and relevant experience are as follows:

    - Prof **Yee-Fui Ng** is an Associate Professor and the Deputy Director of the Australian Centre for Justice Innovation at Monash University, and a 2021-22 Fulbright Scholar. Her research centres on AI and public law, as well as on the intersection between public law and politics, focussing on enhancing executive accountability.

    - Prof **Moira Paterson** is an adjunct professor of law at Monash University, specialising in freedom of information and privacy law.

    - Prof **Marilyn Pittard** is Professor of law at Monash University, specialising in labour and employment law, and workplace relations law. She is the immediate past President of the Australian Labour Law Association.

    - Prof **Normann Witzleb** is an adjunct associate professor of law at Monash University, specialising in privacy and data protection law, torts law and comparative law.

5. In addition to this submission, we make the following of our relevant publications available to the Review Team:

- Murray Brown and Normann Witzleb, 'Big Brother At Work: Workplace Surveillance and Employee Privacy in Australia' (2021) 34(3) *Australian Journal of Labour Law* 170
- Yee-Fui Ng, Maria O'Sullivan, Moira Paterson and Normann Witzleb, 'Revitalising Public Law in a Technological Era: Rights, Transparency and Administrative Justice' (2020) 43(3) *University of New South Wales Law Journal* 1041
- Yee-Fui Ng and Maria O'Sullivan, 'Deliberation and Automation: When is a Decision a "Decision"?' (2019) 26(1) *Australian Journal of Administrative Law* 21
- Moira Paterson and Normann Witzleb, 'Voter Privacy in an era of big data: Time to abolish the political exemption in the Australian Privacy Act' in Normann Witzleb, Moira Paterson and Janice Richardson (eds), Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-targeting, Routledge, 2020, 164
- Normann Witzleb, 'Another Push for an Australian Privacy Tort – Context, Evaluation and Prospects' (2020) 94 *Australian Law Journal* 765
- Normann Witzleb and Moira Paterson, 'Micro-targeting in Political Campaigns: Political Promise and Democratic Risk, in Uta Kohl and Jacob Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law*, Cambridge University Press, 2021, 220
- Normann Witzleb, Moira Paterson, Jordan Wilson-Otto, Gabby Tolkin-Rosen and Melanie Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment: Research paper commissioner by Office of the Australian Information Commissioner* by Monash University and elevenM Consulting, December 2020

II. Scope and Application of the Privacy Act

Objects of the Act (chapter 1)

6. Proposal 1.1 is to amend paras (a) and (b) of the objects clause in s 2A to refer to:
   (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.

7. We **do not support the proposed change to para (a)**. In our view, there is no demonstrated need for restricting the objects of the Privacy Act in that way. In fact, a number of the proposals made in the Discussion Paper suggest that the ambit of the Act may in future become wider and go beyond information privacy.

   a) The inappropriate processing of personal information in an era of Big Data and AI raises important downstream issues that affect interests that are associated with, but distinct from, the interest in privacy. For example, the Discussion Paper makes proposals that are designed to address problems arising from profiling and automated decision-making, including the risks of discrimination and undue manipulation. The proposed expression 'privacy of individuals with respect to

their personal information' may lend itself to a narrower conception of the role of the Act that excludes these associated interests.

b) If a statutory privacy tort was enacted (as in options 1 or 2 of Proposal 26), the Privacy Act would also go beyond the protection of individuals with regard to their personal information. In addition to protecting informational privacy, the Act would then also protect physical and other aspect of privacy,

Accordingly, we **submit** that it is preferable **not to amend s2A para (a)**. If it was thought necessary to amend this provision, we suggest that a more inclusive formulation of the Act's objects should be adopted. For example, para (a) could be stated as follows:

> 'to promote the protection of the privacy of individuals, **particularly** with regard to their personal information'.

8. We **recognise the intent of the proposed change to para (b) but we do not support the proposed formulation.** It is correct that data handling by entities in the context of functions and activities undertaken in the public interest raises concerns that need to be balanced against individual privacy. However, we have doubt that it is correct to say that the subjective interests of entities are not relevant unless they are not supported by the public interest. The Privacy Act recognises that the pursuit of subjective interests can provide a justification for data handling in some contexts. For example, the general situations listed in s 16A include 'asserting a legal or equitable claim' (see APPs 3.4(c) and 6.2(c)), which would not seem to constitute a public interest unless a very wide definition of the public interest was adopted. Similarly, data use for the purposes of direct marketing (see APP 7) would not seem to be carried out in the public interest, properly understood. The suggestion in the Discussion Paper that the 'economic wellbeing of the country' is a public interest[1] would cast that term so widely that it becomes largely devoid of content – and, in any event, it may be difficult to demonstrate in a particular case that a commercial data use enhances the 'economic wellbeing of the country'.

9. Accordingly, we **submit that the current wording** of the Act is preferable. It expresses the intent that the interest in privacy and countervailing interests need to be balanced against one another, and at the same time provides sufficient flexibility to allow these countervailing interests to be given the weight they deserve in a particular context. This includes that interests that are subjective to a data processor, but coincide with the public interest, are given more weight than purely subjective interests of a data processor.

Personal information, de-identification and sensitive information (chapter 2)

The definition of personal information

[1] Attorney-General's Department, *Privacy Act Review: Discussion Paper*, October 2021, p 19.

10. Proposals 2.1 – 2.5 are to amend the definition of personal information in the Act by:
    - 2.1 Replacing the word 'about' with 'relates to'.
    - 2.2 Including a non-exhaustive list of the types of information capable of being covered.
    - 2.3 Defining 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly and including a list of relevant factors to support this assessment.
    - 2.4 Amending the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.
    - 2.5 Requiring personal information to be anonymous before it is no longer protected by the Act.

11. We **generally support proposal 2.1** because it would remedy the uncertainty resulting from the decision of the Full Court of the Federal Court in *Privacy Commissioner v Telstra Corporation Limited (Grubb* case)[2] and its potential to narrow the operation of the Act. However, we **submit** that the definition of personal information should go further in terms of protecting information that can be used to single out an individual without knowing who they are, which often features in the context of targeted advertising. What is significant is that it is possible to manipulate an individual based on their known attributes without actually knowing who they are. We also suggest that it would be prudent to state in the Explanatory Memorandum to the Bill that the change from 'about' to 'relates to' is intended to ensure alignment with how that term has been interpreted in the context of the GDPR so that the definition is not read down in similar manner to that taken in the *Grubb* case.

12. We **support the wording suggested for such a definition in the** Salinger Privacy submission**:**
    - **if the individual is a subject of the information, or**
    - **if the information concerns or links to the individual, or**
    - **if the intent or effect of the information's handling will be to learn, evaluate, treat in a certain way, make a decision about, influence the status or behaviour of, or otherwise have an impact upon, the individual.[3]**

13. We also **support proposal 2.2**. In a world of Big Data and ever-increasing digitalisation, it is important that technical information that relates to an individual, or can be used to individuate a person, is also protected as personal information. We **agree** that a non-exhaustive list in the legislation would be helpful to clarify the term 'personal information' and **support the inclusion** of the identified types of information in such a list.

14. We **support the proposal in 2.3** to further clarify when a person is considered to be identifiable. We also **support** specifying a list of relevant factors to assist in making

[2] (2017) 249 FCR 24; [2017] FCAFC 4.
[3] Salinger Privacy, *Submission in response to the Privacy Act Review – Discussion Paper*, October 2021, January 2022, p 4 ('Salinger Privacy submission').

this assessment and that this list includes the factors identified in the Discussion Paper, such as the 'context in which the information is to be held or released, the costs and amount of time required for identification, and available technology'.[4] We **submit** that, in addition to the suggested factors in proposal 2.2, the **list should include 'current data processing practices, both locally and internationally'**.

15. However, we **submit** that the use of the word **'reasonably' to qualify 'identifiable' is problematic**. Given the reform intention to align Australia's definition with that in other jurisdictions and to increase interoperability, we consider that qualifier to be unnecessary and inconsistent with international models. We **agree** with the Salinger Privacy Submission that this would put an undue focus on resources and motivation rather than risk, and fail to offer protection where an individual can 'actually be identified from the data, such as by a highly motivated party willing to go beyond "reasonable" steps'.[5] This is significant in context where there is no shortage of actors with the motivation and wherewithal to reidentify data for malicious purposes. We **suggest a test of identifiability that is based on a potential or risk of identification that is 'more than insignificant or hypothetical'**.

16. Given the ever-increasing power of technologies based on artificial intelligence to generate and infer information, we **share the concern underlying proposal 2.4** to improve the regulation of generated or inferred data about individuals. However, we agree with the Salinger Privacy submission that it is important not only to define 'collection' to clearly cover inferred information, but also to clarify the definition of 'personal information' itself.[6] This would make all APPs applicable to such information, including when inferences are generated through data mining after the point of collection. We accordingly **support** the recommendation that personal information should be defined as:

> information or an opinion that relates to an individual who is identified or 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; and
> c) includes information or opinion which has been created, generated or inferred.

17. We also **support the proposal in 2.5** that personal information needs to be anonymous before it is no longer protected by the Act. This is very important for the reasons outlined by the ACCC in its DPI report,[7] including the increased risk of re-identification due to the amount of data in circulation, facilitated by advances in technology.

18. We **oppose proposal 2.6** for the reintroduction of the Privacy Amendment (Re-identification Offence) Bill 'with appropriate amendments'. There is no

[4] Attorney-General's Department, *Privacy Act Review: Discussion Paper*, above n 1, pp 27–28.
[5] Salinger, above n 3, p 5.
[6] Ibid, p 13.
[7] Australian Competition and Consumer Commission, *Digital Platforms Inquiry Final Report*, June 2019, ch 7.

demonstrated need for such an offence. In fact, the criminalisation of reidentification activities may be harmful if it has the potential to criminalise 'white hat' researchers and cybersecurity specialists. As outlined in para 1.3 of the dissenting report on the Bill by the Legal and Constitutional Affairs Legislation Committee, 'The bill discourages research conducted in the public interest as well as open discussion of issues which may have been identified'.[8] In the absence of further details of what 'appropriate amendments' are planned, we **do not support** this proposal.

The definition of sensitive information

19. The Discussion Paper asks about the benefits and risks of amending the definition of sensitive information or expanding it to include other types of personal information.

20. We reiterate the views expressed in our submission to the Issues Paper that **the definition of sensitive information should be explicitly amended to include information that acts as proxies for sensitive information, because such proxies may be used as a basis for discrimination**.[9] By way of illustration, having a specific app on one's phone may act as a proxy for sexual preference or for a specific health issue. Because information that an individual has installed a specific app is not defined as sensitive data it is possible to collect that information without the individual's consent and to use it to discriminate against them on that basis. In a world of AI and Big Data it is possible to draw more sophisticated inferences based on intricate patterns in data and to use these both as a basis for decision-making in a wide range of issues both in government (for example, in the context of immigration and law enforcement) and private sector (for example, in the context of employment and credit assessment).

Employee records exemption (chapter 5)

21. The Discussion Paper explored various possibilities with respect to the employee record exemption, namely, to:

- *Remove the employee records exemption*
- *Modify the employee records exemption*
- *Enhance employee privacy protections in workplace relations legislation*

and it posed various questions.

This submission addresses the benefits and challenges of employers being covered by the Privacy Act in respect of employee records, and questions about the appropriateness of workplace laws dealing with privacy.

[8] Senate Standing Committee on Legal and Constitutional Affairs, *Report on the Privacy Amendment (Re-identification Offence) Bill 2016*, Dissenting Report of the Australian Labor Party and Australian Greens, [1.3].

[9] Castan Centre for Human Rights Law, *Submission to Attorney-General's Department Review of the Privacy Act 1988 Issues Paper*, p 19.

22. We **strongly support** the first approach in the Discussion Paper, i.e. the **removal of the employee records exemption from the *Privacy Act*** and outline the reasons in paragraphs 23–29 below.

To allay any concerns of employers that the processes of workplace disciplinary investigations might be compromised by the removal of the employee records exemption, we **submit that an addition to Australian Privacy Principle 12.3 could be made** and outline the suggested addition: see paragraphs 30 and 31 below.

We submit that the *Privacy Act* is the appropriate legislation to deal with collection, use and disclosure of employment information: see paragraph 32 and 33 below.

23. *Regulatory challenges and impost:* Removing the employee record exemption entirely will mean that relevant businesses will be required to abide by the same rules about collection, use, and disclosure of employment information as they are in respect of other information collected which is subject to the *Privacy Act*. In this sense there is uniformity of approach to all information, and not a dual system. Removal may impose a slightly higher burden on employers, however this would be compensated for by the resulting regulatory certainty and the elimination of the burden on employers to determine whether a person is truly an 'employee' and whether the information constitutes an 'employment record' directly related to employment. (See further paragraphs 27 and 82 below.)

24. *Best practice guidelines by Fair Work Ombudsman:* The Fair Work Ombudsman (FWO) issues best practice guides for employers on a range of topics, such as gender equity and flexible working arrangements. A best practice guide has also been developed for workplace privacy. The FWO outlines the reasons for adopting these best practice guides:

> *By adopting best practice initiatives, employers and employees can achieve happier, fairer and more productive workplaces.*[10]

The FWO recommends that employers follow the principles in the *Privacy Act* for employees and employee records. The FWO best practice guide for Workplace Privacy states:

> *Best practice employers choose to meet the requirements of the Australian Privacy Principles **even if they aren't required to**. They also apply the principles to employee records **although this isn't required by law**.* (emphasis added)[11]

This advice, significantly, acknowledges and endorses that it is best practice for employers to do *more* than the law requires in respect of privacy, and to abide by the principles under the *Privacy Act*, for reasons that include promoting 'fairer' workplaces.

25. We **submit** that **this best practice should be legislatively enshrined, by removing the exemption for employee records in the Privacy Act**. Not to do so leaves it

[10] See Fair Work Ombudsman, *Best practice guides* <https://www.fairwork.gov.au/tools-and-resources/best-practice-guides>.
[11] See Fair Work Ombudsman, Workplace privacy: *Best Practice Guides,* <https://www.fairwork.gov.au/tools-and-resources/best-practice-guides/workplace-privacy> p 5.

entirely to the inclination of the employer to follow the guidelines, thereby creating uneven applications between businesses, with some choosing to follow best practice and others not. Fairness relating to privacy is then very uneven in workplaces.

Importantly, even where best practice is followed, but without the support of the legislation, employees are deprived of the legal protection and rights they have under the *Privacy Act* and to make complaints to the Privacy Commissioner. It would remain an entirely voluntary scheme for employers and give no remedies to employees, to a large extent making the best practice hollow. While this commendable advice of the FWO in the best practice guide may seek to ameliorate the effect of the current employee records exemption, we **submit** that it is not sufficient to rest on best practice and employer discretion without legislative mandate requiring that best practice to be followed.

26. *Overseas practice and laws:* Privacy and data collection schemes overseas generally do not exempt employment records from the operation of the privacy. Hence to remove the exemption would bring the protection in Australia more into line with overseas practice.

27. *Uncertain scope of the exemption:* Independent contractors engaged by businesses are covered by the *Privacy Act* whereas employees are not, in respect of employee records. Determining who is legally an 'employee', and whose records are therefore exempt from the *Privacy Act*, can be a vexed issue in certain types of work (eg gig workers; platform work; 'consultants') and in certain methods of engagement adopted by businesses, which attempt to avoid the minimum terms and conditions of employment of the *Fair Work Act*, by engaging workers as independent contractors.

Legal issues frequently arise as to whether the legal status of a worker is truly an 'employee' at law or an independent contractor. This may mean that businesses are operating under misconceptions as to true legal status of their workers. This may result in either the business wrongly claiming the employee record exemption for contractors misclassified as employees, or wrongly applying the privacy principles to contractors who at law would be employees whose records strictly speaking do not have to fall under the privacy law. Removing the exemption would avoid these uncertainties of application. Further, there is no compelling rationale for distinguishing between individual contractors and employees in the *Privacy Act* – especially since both provide their personal labour services to the business for reward.

28. *The definition of employment record and the need that it 'directly' relates to employment:* Definitional issues and the application of the current law create uncertainty as to the true boundaries of the employee record exemption, thereby also creating increased regulatory burden of working out the application of the law. The example of surveillance of drivers in employer-provided vehicles has been given.[12] The employment record would include that data collected whilst the employee is at work (and therefore would be exempt from the Act), but would not include information collected when the employee is using the vehicle for private purposes after work hours. These fine distinctions may be lost on many

[12] Murray Brown and Normann Witzleb, 'Big Brother At Work: Workplace Surveillance and Employee Privacy in Australia' (2021) 34 *Australian Journal of Labour Law* 170.

employers and employees and create uncertainties, which removal of the exemption would avoid.

Likewise, there can be ambiguity about what 'directly' related to employment means. Where the employer provides, say, health insurance or membership to a gym to employees as an extra benefit, information collected in respect of these benefits arguably may not be 'directly' related to employment, in which case it is covered by the privacy principles under the *Privacy Act*. A simpler approach, and one less fraught with uncertainty, is to apply the principles to all information collected by an employer about an employee.

Volunteers: Volunteers who provide their labour services voluntarily and without reward to an organisation might have similar information collected about them as businesses collect about employees. There is presently an anomaly as volunteer records would be subject to the privacy principles, but not the employees' records. There is no rationale for treating similar information differently as between employee and volunteer.

29. *Pandemic highlighted issues:* Many businesses in Australia have mandated that their employees, contractors and others (including volunteers) must be vaccinated in order to enter the business premises and continue working. Where that information is collected and forms part of the employment record for employees – as it directly relates to the ability of the worker to continue working for the employer – it is not subject to the data protection of the Act, but exactly the same type of information relating to the independent contractors and volunteers is. This leads to anomalous consequences arising from the workers' categorisation, yet the type of information – their vaccination status – is the same. It means, too, that contractors and volunteers can complain to the Privacy Commissioner but employees cannot. Working from home has increased during the pandemic, blurring the work-home divide. Employees may collect information about employees – eg. from their background in video meetings that are recorded – and ambiguities about the classification of that information may lead to incorrect claims that is it exempt from the *Privacy Act*.

30. *Effect of removing the employee record exemption on employers and management of employment relationship:* Some employers in submissions expressed concern that there would be some difficulties created for employers in managing the employment relationship if the employee record exemption were removed. We **submit** that notions of fairness and the application of the privacy principles to employees, bringing them into line with independent contractors and volunteers, as well as providing remedies for contravention of the privacy principles, compel all employee records to be governed by the *Privacy Act*.

31. However, there may be one situation where in certain circumstances the management of the relationship is affected – that is a disciplinary investigation conducted by the employer or a third party. If records about a disciplinary investigation into the conduct of an employee were subject to the privacy principles before the investigation is complete, this might compromise the on-going investigation. We **submit that an addition to Australian Privacy Principle 12.3 could protect that process until it is completed** (and then all records data would be covered by the Privacy Act). The suggested amendment to 12.3, to allay some employers' concerns, could be to add another exception to the list, along the following lines:

(#) giving access would reveal information generated within the entity in connection with disciplinary action against an employee in such a way as to prejudice the outcome of those proceedings.

More general concerns about managing the employment relationship are not cogent reasons for retaining the employee record exemption. We also **note** that it is significant that the FWO expressed no reservations in the best practice guide about disciplinary investigations or managing the employment relationship.

32. *Interrelationship of privacy legislation and industrial relations/workplace relations legislation:* An original rationale for exempting employment records from the *Privacy Act* was that the workplace relations legislation should deal with employment records. The Explanatory Memorandum to 2000 Bill amending the Privacy Act stated:

> The Government has agreed that the handling of employee records is a matter better dealt with under workplace relations legislation. An act or practice engaged in by a current or former employer of a person in relation to an employee record will be exempt from the operation of the legislation if the act or practice is directly related to the current or former employment relationship.[13]

Since 2000, the *Fair Work Act 2009* (Cth) was enacted and contains employment record keeping requirements with which employers must comply. Part 3-6 Division 3 of the *Fair Work Act* requires keeping of 'employee records' for a period of seven years, with the definition of employee records being the same as that in the *Privacy Act*.14 However, these requirements largely link to compliance aspects of ensuring that employers are paying and providing minimum conditions in conformity with legal obligations. Contrary to the expectation in the explanatory memorandum, the privacy aspects of the employee record were not generally dealt with in the *Fair Work Act*.

33. We acknowledge that the use, collection and disclosure of the employee records could be dealt with in the *Fair Work Act* from a privacy viewpoint, However, it seems that there was no appetite to do so at the time the *Fair Work Act* was enacted in 2009; nor does it seem there is any present appetite to do so. Moreover, the *Privacy Act* is dedicated to issues of collection, handling and use of information (and complaints) so that it should be treated as the primary source of these obligations. Given that there exists a legislative regime in operation under the *Privacy Act*, the employment record exemption could be removed from that Act, thereby allowing the *Privacy Act* to govern employment records. We are conscious that there would be an issue of slightly different coverage of employers in the *Privacy Act* compared to employers covered generally by the *Fair Work Act*, however **we submit that this does not undermine the case to deal with workplace privacy issues in the**

[13] The Parliament of The Commonwealth of Australia, House of Representatives, Privacy Amendment (Private Sector) Bill 2000, Explanatory Memorandum at <https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r1049_ems_aebd4d72-266b-44ca-a5b0-dabb68c2405a/upload_word/30758%5B1%5D.docx;fileType=application%2Fvnd.openxmlformats-officedocument.wordprocessingml.document>.

[14] Section 12 of the Fair Work Act provides that employee record, in relation to an employee, means 'something that is an employee record, in relation to the employee, for the purposes of the *Privacy Act 1988*'.

Privacy Act. Policy makers could later consider expanding the application of privacy principles to all employers covered by the *Fair Work Act* once it is seen how the *Privacy Act* operates in practice in applying to those employers covered by it.

Political exemptions (chapter 6)

34. The Discussion Paper poses two questions in respect of the political exemptions in the Act:

- *What would be the impact, if any, on freedom of political communication and the operation of the electoral and political process in Australia if political parties were brought within the scope of the exemption that currently applies to political representatives and contractors, subcontractors and volunteers of political parties and political representatives?*
- *What would be the benefits and costs of applying some specific APPs to political parties and their affiliates?*

35. We **strongly support removal of the political exemptions**. When the ALRC considered the political exemptions in the Privacy Act and recommended their abolition in 2008,[15] it referred to

> concerns about political parties withholding from voters information they have stored; inaccurate information being stored on databases without giving voters the right to correct the record; political parties failing to inform voters that information is being compiled about them; and representatives of political parties failing to identify themselves appropriately when collecting information.[16]

36. The issues arising from the use of electoral databases have changed considerably with the advent of big data analytics. The exemptions now enable the largely unregulated collection and processing of personal information in a context where there is increased evidence of excessively manipulative political microtargeting practices. Micro-targeting may be of concern for example, where it includes getting voters 'to hold opinions that they would not hold if aware of the best available information and analysis'[17] and where 'it is used to mislead voters or keep them ignorant about matters relevant to their vote. This might occur where a political party describes itself as standing for different issues depending on its analysis of the

[15] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108, 2008, rec. 41-1.
[16] Ibid, [41.13].
[17] Lawrence R Jacobs and Robert Y Shapiro, *Politicians Don't Pander: Political Manipulation and the Loss of Democratic Responsiveness,* University of Chicago Press, 2000, xv, as quoted in Murray Goot, 'Politicians, public policy and poll following: Conceptual difficulties and empirical realities' (2005) 40 *Australian Journal of Political Science* 189, 189.

individual whom it targets'.[18] The rise of online campaigning has the further consequence that political parties are becoming increasingly dependent on data brokers and other digital intermediaries. As evidenced in the inquiries in the UK following the Facebook/Cambridge Analytica scandal,[19] the corporate actors operating in this domain are reluctant to disclose the methods and technologies they use for data-driven personalisation. The exemptions have the effect of removing the requirement to comply with any of the APPs and to prevent the OAIC from exercising oversight of the data practices of political organisations and digital intermediaries.

37. After a wide-ranging investigation into the use of social media platforms for microtargeting by UK political parties and consultations into a draft framework code of practice, the UK Information Commissioner's Office (ICO) also published guidance for the transparent and lawful use of personal data in political campaigns.[20] The exemptions in the Privacy Act stand in the way of achieving greater transparency for digital political campaigning, which in turn has the potential to reduce public confidence in the political process. Witzleb and Paterson have argued elsewhere that –

> there is no longer a good case for the retention in data protection laws of political exemptions, or overly broad provisions permitting data processing in political contexts. The example of the GDPR suggests that subjecting political parties to the general requirements of fair, transparent and lawful processing would go some way towards 'moderating' political micro-targeting in terms of creating a more rigorous and transparent process with regulatory oversight. This would help rebalance the legitimate functions and interests of political actors and digital intermediaries against the interests and fundamental rights of voters, thereby engendering more trust in political communications. Ultimately such protection could increase the transparency of profiling and targeted messaging, and provide some regulatory oversight at the input and process side of these practices.[21]

38. If the political exemptions were abolished, registered political parties would become subject to the Act and the APPs would apply to acts and practices done in connection with an election, a referendum and the participation in another aspect of the political process, as well as the acts of contractors, subcontractors and volunteers of political parties or representatives. The APPs require data handlers to follow fair information

[18] See Moira Paterson and Normann Witzleb, 'Voter Privacy in an era of big data: Time to abolish the political exemption in the Australian Privacy Act' in Normann Witzleb, Moira Paterson and Janice Richardson (eds), *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-targeting*, Routledge, 2020, 164, 172–173.

[19] United Kingdom, House of Commons Digital, Culture, Media and Sport Committee, Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Final Report* (HC 2017–19, 1791); Information Commissioner's Office (UK), *Investigation into the use of data analytics in political campaigns: A report to Parliament* (6 November 2018).

[20] Information Commissioner's Office (UK), *Guidance for use of personal data in political campaigning* (9 March 2021) at <https://ico.org.uk/for-organisations/guidance-for-the-useof-personal-data-in-political-campaigning/>.

[21] Normann Witzleb and Moira Paterson, 'Micro-targeting in Political Campaigns: Political Promise and Democratic Risk, in Uta Kohl and Jacob Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law*, Cambridge University Press, 2021, 220, 230.

practices in relation to the collection, use and security of personal information, and give affected individuals assess and correction rights. Voters who believe that these practices of political actors fell short of the requirements in the APPs would have a right of complaint to the Privacy Commissioner.

39. In our view, **any adverse impact on freedom of political communication** of bringing political parties, and currently exempted political acts and practices, within the scope of the Privacy Act would be limited, justified and proportionate. As Paterson and Witzleb have argued elsewhere, the removal of the exemptions –

> would not curtail the ability of political parties and other actors to communicate with certain sectors of the electorate about matters of politics and government. The effect on the freedom would merely be indirect, and impose some restrictions on current practices. It is important to note that the privacy principles are open-textured and have been adapted to promote a further objective of the Act which is 'to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities'.[22] ….. The Privacy Act does not provide absolute protection for privacy but rather provides for a set of fair information-handling principles which are designed to protect privacy while still enabling the entities which are required to comply with it to carry out their functions and activities. This balance protects the personal autonomy which is necessary for the operation of a democratic system without unreasonably undermining the ability of political parties to communicate with voters. It follows therefore that the Privacy Act already has built in a number of mechanisms to ensure that the restrictions it imposes are reasonably adapted and appropriate, or proportional, to the ends it pursues. In addition, it can be argued that these protections help to create a level playing field between political parties and between political actors, because they impose certain general standards that all organisations need to adhere to in their political communications with voters, regardless of their financial resources or technical expertise.[23]

40. Our analysis brief examination of recent jurisprudence of the High Court suggests that the removal of the exemption for political parties and political acts would be unlikely to be incompatible with the implied freedom of political communication, as currently defined and we **submit** that it is **not strictly necessary to include a savings provision** to ensure the constitutional validity of the required amendments to the Act. Out of abundance of caution, a savings provision, as is currently already in place for other legislation, could be included in the Privacy Act. It could state that the Act does not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication or parliamentary privilege.

41. We **do not support applying only some specific APPs to political parties and their affiliates**. There is a good case for applying all of them given what is at stake. However, if it is decided to take this approach, to which they should be subject extend

[22] *Privacy Act 1988* (Cth) s 2A(b).
[23] Paterson and Witzleb, above n 18, p 183.

beyond APPs 1 and 10. APPs 3, 5 and 6 are important as it is the collection, use and disclosure of personal information that facilitates political micro-targeting, including practices that are excessively manipulative. In addition, APP 12 has an important role to play in ensuring that individuals are aware of the extent of information held about them and providing some potential for understanding the bases on which they may be targeted.

III. Protections

Consent to collection, use and disclosure of personal information (chapter 9)

42. Proposals 9.1 and 9.2 are for:

- *Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.*
- *Consideration of standardised consents in the development of an APP code, such as the OP code, including standardised layouts, wording, icons or consent taxonomies.*

43. We **support Proposal 9.1**. While consent is required only for a limited range of collections, uses and disclosures of personal information, it is nevertheless important and consistent with international best practice for the Act to provide further guidance as to what constitutes valid consent and to make clear that bundled consents are unacceptable. However, we **submit that a qualification should be added** to the effect that:

> consent is considered 'only valid if it is reasonable to expect that individuals to whom an organisation's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure, to which they are consenting.'

This is important to ensure the protection of children and vulnerable individuals, as will be further discussed below under the section on 'children and vulnerable individuals'.

44. We **support Proposal 9.2**. Standardised consents are a promising mechanism for dealing with the issue of consent complexity and information overload. We agree that they are likely to work better if they are context-specific and that incorporating them in codes would be a useful way forward.

45. The Discussion Paper poses the question of whether there are additional circumstances where entities should be required to seek consent. Arguably **there is a case for doing so in relation to the types of practices mooted for inclusion as restricted practices in Proposal 11.1**. However, given the well documented problems with the notice and consent model for privacy protection, including the issue of burdensomeness, we regard it as more important to strengthen the test for use and disclosure with a fair and reasonable requirement, as discussed below.

46. The Discussion Paper also poses the question as to whether entities should be required to refresh or renew an individual's consent on a periodic basis where such consent is obtained for the collection, use or disclosure of sensitive information. We **agree with this idea**. The advice provided by the ICO in its Guide to the UK General Data Protection Regulation (UK GDPR)[24] provides a useful way forward. This suggests that entities need to refresh consents where processing operations or purposes evolve. It also recommends automatic refreshment of consent at appropriate intervals.

> How often it's appropriate to do so will depend on the particular context, including people's expectations, whether you are in regular contact, and how disruptive repeated consent requests would be to the individual. If in doubt, we recommend you consider refreshing consent every two years – but you may be able to justify a longer period, or need to refresh more regularly to ensure good levels of trust and engagement.[25]

Additional protections for collection, use and disclosure (chapter 10)

47. Proposals 10.1 and 10.2 are to amend the Act to include:

- *A requirement that collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances; and*
- *Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances such as:*
  - *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.*

48. We **strongly support proposal 10.1** for the three key reasons canvassed. First, information handling in an Internet context is too prolific and complex to expect individuals to be able to process the information provided in privacy policies and

[24] Information Commissioners Office (UK), Guide to Data Protection: Guide to the General Data Protection Regulation (GDPR), How should we obtain, record and manage consent? at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/>.
[25] Ibid.

collection notices and to make informed choices based on that information. Secondly, there are issues concerning the voluntariness of consent in contexts where failure to provide consent may lead to exclusion from platforms and services. Thirdly, there is the fact that consent plays a relatively limited role except in the case of sensitive information where it is unreasonable to expect individuals to make a once and for all choice in contexts where it is difficult to predict and understand the consequences of future uses of that information. In our view this test provides a useful mechanism for striking an appropriate balance between the interests of individuals, APP entities and the public interest, as well as between flexibility and certainty. It also assists in ensuring the protection of children and vulnerable individuals, as discussed below.

49. We also **support proposal 10.2**. However, we **recommend the inclusion** of the following additional criterion to address the issue of vulnerable individuals as discussed below in the section on children and vulnerable individuals:

> **the collection, use and disclosure information about vulnerable individuals on a large scale**

50. We **strongly favour subsuming the fair and lawful collection requirement in APP 3.5 within an overarching fair and reasonable requirement**. Collection provides the starting point for the processing of personal information; it is not satisfactory to continue to allow APP entities to collect personal information that is not sensitive information simply on the basis that it is 'reasonably necessary' for their functions and activities, irrespective of what those functions and activities are, whether they are known by the individual and whether the intended data use for carrying out these functions and activities is fair and 17easonable.

51. It is our view that **the fair and reasonable test should 'qualify other requirements in the APPs, including whether an individual has consented to the act or practice'**. This is important because individuals may in reality have little choice other than to consent if they wish to use a platform or service. An APP entity should not be able to rely on consent to legitimise collection, used and disclosure that is not reasonably necessary to achieve its functions and activities or where the individual's loss of privacy is not proportionate to the benefits they obtain.

52. We **do not support a blanket exception from the overarching fair and reasonable test for the exceptions in APP 6.2(b)-(e) and APP 3.4**. While it is true that they are grounded in public interest considerations or are already qualified by 'reasonableness' requirements, there are arguably actions that fall within them that would fail to meet the fair and reasonable test proposed in 10.1 and 10.2. We support the view expressed in the Salinger Privacy submission that the test has sufficient flex to allow it to operate in a common sense way in relation to each of these.[26] However, if this view was rejected we would suggest that at least the exceptions in APPs 3.4 (a), 3.4(d), 6.2(b) and 6.2(e) should be subject to the fair and reasonable test.

[26] Salinger, above n 3, p 18.

53. The wording of the exceptions in APP 3.4 (a) and 6.2(b) is currently too wide insofar as it refers to 'authorised'. While it might be impracticable to submit legal requirements to a fair and reasonable test, we would argue that the reference to authorised should be qualified by a fair and reasonable requirement. **We suggest that the wording of these exceptions is changed to:**

    (i) is required by or under an Australian law or a court/tribunal order or

    (ii) is authorised by or under an Australian law or a court /tribunal order and it would be fair and reasonable to collect, use or disclose that information.

Restricted and prohibited practices (chapter 11)

54. Proposals 11.1 and 11.2 set out alternative options for dealing with the issue of restricted practices. Option 1 proposes that APP entities be required to take reasonable steps to identify privacy risks and implement measures to mitigate those risks where they engage in the following practices:

- *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 proposes instead to increase an individual's capacity to self-manage their privacy in relation to specified restricted practices, for example, by 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.

55. We **support the introduction of specified restricted practices**. In a world of Big Data and artificial intelligence there are specific practices involving the collection, use and disclosure of personal information that require additional regulation because of the risk of harm that they pose. We also **support proscription in the case of practices that are so problematic that there can be no public interest in permitting them to take place**.

56. Our **strong preference therefore is for Option 1**. The regulation of restricted practices should involve putting the onus on APP entities to take action to demonstrate their appropriateness, and to mitigate the risks involved, rather providing individuals with additional means of protecting their interests and requiring them to self-manage their privacy. The latter poses an unacceptable burden of individuals and ignores the practical difficulties and time involved in this process.

57. The Discussion Paper asks what acts and practices should be categorised as a restricted and prohibited practice, respectively. We **support the suggested list of factors in Option 1** subject to the addition of some form of clarification via a drafting note that the last listed criterion covers includes practices listed above that that are qualified by the expression 'on a large scale'. This is important because practices such as the collection, use or disclosure of location data can have high privacy risk or risk of harm to individuals even where they do not occur on a large scale.

58. We also **support adding to the list of *restricted* practices**:

- **The collection, use and disclosure information about vulnerable individuals on a large scale.**

The issue of vulnerable individuals is discussed in detail below in the section on children and vulnerable individuals.

59. We recommend that the list of proscribed categories should include:

a) The collection, use or disclosure of personal information for automated processing undertaken for the purpose of unlawful discriminatory treatment
b) The collection, use or disclosure of personal information for profiling that that is shown to cause harm or discrimination.
c) The collection, use or disclosure of personal information for profiling of children for advertising or other commercial purposes except where this is demonstrably in the child's best interest.
d) The collection, use or disclosure of personal information for profiling of individuals who are known or might reasonably be expected to be vulnerable individuals for advertising or other commercial purposes except where this is demonstrably in the individual's best interest.
e) The collection of children's personal information based on 'nudge' techniques which lead or encourage children to provide personal data that is not necessary for the provision of a product or service to them or to turn off privacy protections.
f) The collection of the personal information of individuals who are known or might reasonably be expected to be vulnerable individuals based on 'nudge' techniques which lead or encourage them to provide personal data that is not necessary for the provision of a product or service to them or to turn off privacy protections.

Pro-privacy default settings (chapter 12)

60. Proposal 11.1 is to introduce pro-privacy defaults on a sectoral or other specified basis. It suggests two alternative options:

> ***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.*
>
> The Discussion Paper asks whether pro-privacy default settings should be enabled by default and, if so, which types of personal information handling practices should be disabled by default.

61. We **support Option 1** as it maximises protection for children and vulnerable individuals. At the very minimum, they should be enabled **where the product or service is directed at children or vulnerable individuals. However, we recommend that** that pro-privacy settings should be enabled by default in relation to any collection of personal information that is not required for provision of goods or services to the individual. This offers such individuals additional protection even where a product or service is not specifically directed at them.

Children and vulnerable individuals (chapter 13)

62. This section of our submission draws extensively from *Privacy risks and harms for children and other vulnerable groups in the online environment: Research paper commissioned by the Office of the Australian Information Commissioner* by Monash University and elevenM Consulting, December 2020.[27]

Children

63. Proposals 13.1 is to amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16. Proposal 13.2 is to require APP 5 notices to be clear, current and understandable, in particular for any information addressed specifically to a child.

[27] N Witzleb, M Paterson, J Wilson-Otto, G Tolkin-Rosen and M Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment: Research paper commissioner by Office of the Australian Information Commissioner* by Monash University and elevenM Consulting, December 2020.

64. We **support proposal 13.1**, **but our preference would be for this cut-off not to be applicable where it is both practicable and reasonable for an APP entity to conduct an individualised assessment of capacity**. Individualised assessment of capacity is consistent with the available research on development psychology, which suggests that the age at which children attain maturity may vary significantly between individuals, making the use of bright line approaches based on age for determining capacity problematic.[28]

65. We also **support proposal 13.2 subject to the addition of a requirement** that notices should contain information addressed to children where there this a reasonable likelihood that the information collected includes the personal information of children.

66. The Discussion Paper raises the question whether there are other contexts aside from children's use of social media services that pose privacy risks to children, which would warrant similar privacy protections to those proposed by the OP code. We suggest that the following should be actively considered:

    - Edutech/learning analytics
    - Behavioural advertising activities directed at children
    - Other activities involving the intentional tracking, monitoring, profiling or targeting of children.

67. The Discussion Paper also asks whether the consent of a parent or guardian should be required for all collections of a child's personal information, or only for the existing situations where consent is required under the APPs. **It is our view that parent/guardian consent should be required only for the existing situations where consent is required under the APPs**, subject to the adoption of an over-arching fair and reasonable test for the collection, use and disclosure of personal information as proposed in 10.1.
68. Two further questions asked are whether the proposed assumed age of capacity of 16 years in the OP Bill apply to all APP entities and whether APP entities also be permitted to assess capacity to consent on an individualised basis where appropriate, such as in the healthcare sector. We **recommend that the cut-off should apply across-the-board but as a default only** so that APP entities are not only able but required to conduct individualised assessment where this is both practicable and reasonable. The healthcare context is one where individualised assessment should continue to be the norm.

69. The Discussion Paper raises as a final question whether the proposed assumed age of capacity should determine when children should be able to exercise privacy requests independently of their parents, including access, correction, objection or erasure requests. In our view, **this is not desirable** as the rationale for the assumed age of consent is ensure that children are protected from the privacy-invasive activities of third parties, not to diminish their autonomy vis a vis their parents and guardians.

[28] See ibid, p 82.

70. For purposes of clarity, we summarise below our recommendations in respect of changes to the Act to maximise the protection of children (including changes relating to erasure of personal information as discussed below).

Recommendations

1) **Provide that consent is valid only if it is reasonable to expect that individuals to whom an organisation's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure, to which they are consenting.**

2) **Require that collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances and, as recommended in Proposal 10.2 of the Discussion Paper, include the following criterion within a legislated list of factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances,**

   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.

3) **Require APP entities to take reasonable steps to identify privacy risks and implement measures to mitigate those risks where they engage in the specified practices, including:**

   the collection, use or disclosure of children's personal information on a large scale.

4) **Proscribe APP entities from engaging in specified practices including:**
   - **(i) the collection, use or disclosure of personal information for profiling of children for advertising or other commercial purposes except where this is demonstrably in the child's best interest: and**
   - **(ii) the collection of children's personal information based on 'nudge' techniques which lead or encourage children to provide personal data that is not necessary for the provision of a product or service to them or to turn off privacy protections".**

5) **Require consent of behalf of a child to be provided by a parent or guardian where a child lacks the required capacity to provide consent, with a cut-off age of 16 for a rebuttable presumption with respect to capacity where it is not practicable or reasonable to make an individualised assessment.**

6) **Require APP 5 notices to be clear, current and understandable, in particular for any information addressed specifically to a child, and to contain information addressed to children where this a reasonable likelihood that the information it collects, includes the personal information of children.**

7) **Require APP entities offering a product or service that contains multiple levels of privacy settings, to pre-select those privacy settings to be the most restrictive in respect of personal information handling in specified situations, in relation to any collection of personal information that is not required for provision of goods or services to the individual (or in specified circumstances including where the product or service is directed at children).**

8) **Provide individuals with a right to request erasure of personal information in specified circumstances, including;**

> **where the personal information relates to a child or was collected, inferred or generated while an individual was child and erasure is requested by the individual, or a parent or authorised guardian.**

Vulnerable individuals

72. The Monash University and elevenM Consulting Report contains a detailed discussion of vulnerability and points out that:

> The particular needs of vulnerable people for privacy protection have been recognised at the highest international level. The United Nations (UN) General Assembly[29] and Human Rights Council[30] have called on States 'to further develop or maintain […] preventive measures and remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular adverse effects on women, as well as children and persons in vulnerable situations or marginalized groups'.

It explains the issue of vulnerability in the following terms:

> Vulnerability [...] can arise where an individual faces greater difficulty than others in protecting themselves from harm. This can be the technical or cognitive skill and experience to use digital platforms and other applications safely.
>
> Individuals can also be vulnerable because they have particular characteristics that expose them to greater or different harm than other people. Such harm can arise from being exposed to or targeted with inappropriate products or services, from unlawful discrimination or inappropriate exclusion from a market.

73. The Discussion Paper contains no specific proposals or questions concerning vulnerable individuals, although we acknowledge that the proposed 'fair and reasonable test' in Chapter 10 and the notice requirements in Chapter 8 have the potential to augment their protection. However, we **submit that Act should address more specifically the protection of vulnerable individuals** so as to draw this matter more clearly to the attention of APP entities. We have accordingly made

[29] UN General Assembly (2014), Right to privacy in the digital age, A/RES/71/199.
[30] UN Human Rights Council, Resolution 34/7 (23 March 2017) <https://www.right-docs.org/doc/a-hrc-res-34-7/>.

recommendations in other sections of this report to more specifically enhance their protection.

74. To clarify the operation of our proposed amendments we also **recommend including in the Act definitions of 'vulnerable individual' and 'vulnerability'**. The Monash University and elevenM Consulting Report cautions:

> If a definition is used, it must not be rigid and should be cognisant of the full range of drivers that can contribute to vulnerability. It is simplistic to associate vulnerability with belonging to a particular group. Vulnerability is not a fixed trait with an easily identifiable threshold; it can improve or worsen over time, depending on personal circumstances, as well as external factors. Furthermore, the causes of vulnerability are complex and can intersect with one another.
>
> We accordingly suggest that the definitions should adopt a factor-based approach that relies on a non-exhaustive list of risk factors, modelled on approaches adopted by the eSafety Commissioner, in the Banking Code of Practice and the General Insurance Code of Practice 2020.

75. For purposes of clarity we summarise below our recommendations in respect of changes to the Act to maximise the protection of vulnerable individuals (including changes relating to erasure of personal information as discussed below). More detailed reasoning underlying these recommendations is contained in the Monash University and elevenM Consulting Report.

Recommendations

1. **Include definitions of "vulnerable individual" and "vulnerability" based on a factor-based definition of vulnerability that relies on a non-exhaustive list of risk factors, modelled on approaches adopted by the eSafety Commissioner, in the Banking Code of Practice and the General Insurance Code of Practice 2020.**

2. **Provide that consent is valid only if it is reasonable to expect that individuals to whom an organisation's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure, to which they are consenting.**

3. **Require that collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances and include a legislated list of factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances.**

4. **Require APP entities to take reasonable steps to identify privacy risks and implement measures to mitigate those risks where they engage in specified practices, including:**

the collection, use and disclosure information about vulnerable individuals on a large scale.

5. **Proscribe APP entities from engaging in specified practices including:**
   - **(i) The collection, use or disclosure of personal information for profiling of individuals who are known or might reasonably be expected to be vulnerable individuals for advertising or other commercial purposes except where this is demonstrably in the individual's best interest; and**
   - **(ii) The collection of the personal information of individuals who are known or might reasonably be expected to be vulnerable individuals based on 'nudge' techniques which lead or encourage them to provide personal data that is not necessary for the provision of a product or service to them or to turn off privacy protections.**

6. **Require APP 5 notices to be clear, current and understandable, in particular where this a reasonable likelihood that the information it collects, includes the personal information of vulnerable individuals.**

7. **Require APP entities offering a product or service that contains multiple levels of privacy settings, to pre-select those privacy settings to be the most restrictive in respect of personal information handling in specified situations, in relation to any collection of personal information that is not required for provision of goods or services to the individual (or in specified circumstances including where the product or service is directed at vulnerable individuals).**

8. **Provide individuals with a right to request erasure of personal information in specified circumstances, including where:**
   the personal information relates to a factor relevant to the assessment of vulnerability and may expose that individual to discrimination or harm.

Right to erasure of personal information (chapter 15)

76. Proposal 15.1 is to provide individuals with a right to request erasure of their personal information where one of the following grounds applies, and subject to exceptions:

    - the personal information must be destroyed or de-identified under APP 11.2
    - the personal information is sensitive information
    - an individual has successfully objected to personal information handling through the right to object
    - the personal information has been collected, used or disclosed unlawfully
    - the entity is required by or under an Australian law, or a court/tribunal order, to destroy the information, and
    - the personal information relates to a child and erasure is requested by a child, parent or authorised guardian.

77. We **strongly support the introduction of right to erasure** on the basis that it enables meaningful consent withdrawal or deletion of personal information where it is being used for a different purpose to what was originally agreed. It also provides an important

mechanism for protecting children and vulnerable individuals from potential future discrimination and harms based on information collected, inferred and generated about them.

78. We acknowledge that erasure is a controversial issue, but it is our view that the model proposed strikes an appropriate balance in terms of the competing public interests involved. We note the inclusion of such a right not only in the GDPR but also in the Californian CCPA, as well as several of data protection laws in the Asia-Pacific region suggests that such a right is capable of working in practice.

79. We **recommend**, however, that **the criterion 'the personal information relates to a child and erasure is requested by a child, parent or authorised guardian' should be amended** to include information collected about an individual who is no longer a child while they were a child. In our view, this is important as it is unreasonable to confine the opportunity for deletion to the period when an individual remains a child. An individual may not recall what information was collected about them or its future implications until long after they reach the age of 18. **We recommend the following revised wording:**

> **where the personal information relates to a child or was collected, inferred or generated while an individual was child and erasure is requested by the individual, or a parent or authorised guardian**.

80. We also **recommend broadening the suggested criteria** to ensure better protection for vulnerable individuals. **We recommend the following revised wording:**

> **where the personal information relates to a factor relevant to the assessment of vulnerability and may expose that individual to discrimination or harm.**

Automated decision-making (chapter 17)

71. The Discussion Paper proposes to:

> *17.1 Require privacy policies to include information on whether personal information will be used in ADM which has a legal, or similarly significant effect on people's rights.*

72. The Discussion Paper asks the following Question:

> *Should the concept of a decision with 'legal or similarly significant effect' be supplemented*
> *with a list of non-exhaustive examples that may meet this threshold?*

73. In relation to automated decision-making, the Castan Centre's and CLARS' submission is as follows:

74. Automated decision-making encompasses a wide ranging constellation of technologies which include digital platforms, and the use of some form of artificial intelligence (AI) that can make predictions or decisions using machine or human-based inputs.[31] Artificial intelligence and its use for decision-making ranges from deterministic systems employing relatively simple binary logic,[32] all the way to machine learning systems, which make probabilistic predictions based on complex algorithms that sometimes go beyond what humans can understand.[33]

75. Technological-assisted decision-making has become increasingly ubiquitous in the Australian public sector, for example, in the form of MyGov for tax and social security benefits, or the use of the SmartGate when arriving in Australia. There has been widespread automation in administrative decision-making in Australia for more than a decade, with the Administrative Review Council in 2003 listing the proliferation of automated systems used by a large range of major federal government agencies, including Comcare, the Department of Defence, the Department of Veterans' Affairs, and the Australian Taxation Office.[34] It is likely that this is even more prevalent today.

76. Automated decision-making systems have significant public law implications,[35] including on the protection of individual privacy, particularly in the era of Big Data, widespread surveillance and data sharing between governments. However, Australian law currently does not contain any specific requirements regarding automated decision-making.

77. The European Union's (EU) General Data Protection Regulation (GDPR) states in its Article 22(1):

    The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

    Importantly, the prohibition in Article 22(1) of the GDPR provides 'additional safeguards' specific to circumstances of '*solely* automated decision-making' including profiling. The EU's Article 29 Data Protection Working Party Guidelines on Automated Individual Decision-making and Profiling ('EU Guidelines') define such

[31] Australian Human Rights Commission, *Human Rights and Technology: Final Report*, 2021, 37.
[32] Monika Zalnieriute, Lyria Bennett Moses and George Williams, 'The Rule of Law and Automation of Government Decision-Making' (2019) 82 *Modern Law Review* 425, 432.
[33] Arun Rai, 'Explainable AI: From black box to glass box' (2020) 48 *Journal of the Academy of Marketing Science*, 137, 138.
[34] Administrative Review Council, *Automated Assistance in Administrative Decision Making: Issues Paper* (2003) 11-5.
[35] Yee-Fui Ng et al, 'Revitalising Public Law in a Technological Era: Rights, Transparency and Administrative Justice' (2020) 43 *University of New South Wales Law Journal* 1041; Yee-Fui Ng and Maria O'Sullivan, 'Deliberation and Automation: When Is a Decision a Decision? ' (2019) 26 *Australian Journal of Administrative Law* 21, 27-31.

decisions as those made 'by technological means without human involvement',[36] distinguishing them from instances where a human is *meaningfully* involved in decision-making.

78. EU member states, when supplementing the GDPR in their domestic law, have similarly limited the protections in Article 22(1) to those 'only', 'exclusively', or 'totally' made by automated processing,[37] with the UK emphasising that this is decision-making that 'excludes any human influence on the outcome'.[38] Paul Voigt and Axel Von dem Bussche explain that Article 22(1) therefore only applies when '*no human* has any decision-making power',[39] irrespective of whether they are otherwise involved in the decision-making process.

79. The Discussion Paper uses the concept of 'legal, or similarly significant effect',[40] which originates from Article 22 and has been proposed for adoption in Australia by the AHRC.[41] However, there is a question as to whether to utilise this concept more broadly than the GDPR, where it is limited to decisions 'based solely on automated processing'. For example, the AHRC proposes to apply a cumulative standard to AI decisions, referring to a decision or decision-making process that is materially assisted by the use of an AI technology or technique, ***and*** has a legal, or similarly significant, effect for an individual.[42] From a human rights standpoint this can be considered both positive and negative.

80. As for the positive, by extending the scope of protections beyond decisions made 'solely' by AI systems to include decisions where humans are involved, the AHRC's broader definition envisages regulation that applies in a broader range of circumstances. It would encompass instances such as recruitment decisions where a human is *informed* by an AI system but makes the ultimate decision, whereas they would not have been under a narrow scope such as that in Article 22(1).

> **Example**: An employer chooses a candidate for employment from a pool of applicants that was created using an algorithm that favoured some people over others. This does not appear to be a decision based 'solely on automated

[36] European Union, Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (2018) 17/EN WP251rev.01, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053> ('*EU Guidelines'*), p 8.

[37] Gianclaudio Malgieri, 'Automated Decision-making in the EU Member States: The Right to Explanation and other "Suitable Safeguards" in the National Legislations' (2019) 35 *Computer and Security Review* 1, 18–19.

[38] Information Commissioner's Office (UK), 'What does the GDPR say about automated decision-making and profiling?', *Information Commissioner's Office* (webpage) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-does-the-gdpr-say-about-automated-decision-making-and-profiling/> ('*ICO Guidelines'*).

[39] Paul Voigt and Axel Von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer, 2018), p 181 (emphasis in original).

[40] Attorney-General's Department, above n 1, p 139.

[41] Australian Human Rights Commission, above n 31, p 24.

[42] Ibid.

processing' covered under the GDPR but a decision where a human was informed by AI.

81. Unfortunately, however, the threshold created by Article 22(1) of the GDPR through the terms 'legal' and 'similarly significant effects' is relatively high, as it was only intended to apply in very particular circumstances. The EU Guidelines which explore these terms, for example, do not in general consider online advertising to have a legal or similarly significant effect on individuals.[43]

82. Notwithstanding, the UN Human Rights Council noted in a 2017 Resolution that 'automatic processing of personal data for individual profiling may lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights'.[44] This may include, for example, online targeted advertising which may have significant potential to discriminate, or reflect past prejudice or implicit bias against' protected groups in myriad ways, many of which are not likely to meet the threshold of 'legal' or 'similarly significant'.

> **Example**: Latanya Sweeney of Harvard University in 2013 conducted a study where she investigated search engine advertisements for internet users with names typically associated with African Americans. She found a statistically significant difference in the type of advertisements served to African American and non-African American users, with the former far more likely to see advertisements relating to arrest and criminal records than users with Caucasian sounding names.[45]

83. This raises questions about the appropriateness of borrowing the terms 'legal effects' and 'similarly significant effects':

- Are these terms appropriate in a context which is intended to go beyond decisions based solely on automated processing?; and
- Are the terms too narrow to protect the human rights of the subjects of such a broader range of decisions?

(a) 'Legal' effects

[43] European Union, Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-making and Profiling for the purposes of Regulation 2016/679*, 17/EN WP251rev.01 (2018) 22 <https://ec.europa.eu/newsroom/article29/items/612053> ('*EU Guidelines*').

[44] UN Human Rights Council, *The right to privacy in the digital age*, 7 April 2017, A/HRC/RES/34/7 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/31/PDF/G1708631.pdf?OpenElement>.

[45] Latanya Sweeney, 'Discrimination and Online Ad Delivery' (2013) 50(5) *ACM Queue* 44-54; see also Lillian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" is Probably not the Remedy You are Looking For' (2017) 16 *Duke Law & Technology Review* 46; Katarina Throssell, 'When Algorithms Discriminate: A Framework for the Ethical Use of Algorithmic Decision-Making in the Public Sector', *Department of Premier and Cabinet* (Report, 23 May 2018) 22.

84. The EU Guidelines provide that a decision with 'legal' effects refers to a decision that affects someone's 'legal rights', 'legal status' or 'rights under a contract'. Further, the Guidelines state that 'only serious impactful effects will be covered by Article 22'.[46]

> **Examples** of legal rights affected in this context include the rights under the Charter of Fundamental Rights of the European Union, such as the right to associate with others, the right to vote, and the freedom to take legal action.
>
> **Examples** of decisions that impact upon legal status or contractual agreements in turn include decision impacting on admission into a country, denying citizenship, affecting entitlements to social benefits granted by law, and cancellation of contracts.

85. Voigt and Von dem Bussche emphasise in their 'Practical Guide to the GDPR' that both positive and negative effects for the data subject should be covered by Article 22.[47]

86. The benefit of interpreting 'legal' effects in this way is that 'impacts on legal status can be determined according to the letter of the law', whereas 'similarly significant effect' is a vaguer concept, as discussed below.[48]

87. It should, however, be noted that 'legal rights' in the context of the European Union differs to that in Australia. In particular, the existence of a European Charter of Human Rights establishes binding fundamental rights for EU citizens. With such human rights enshrined in law, automated decisions that impact upon these freedoms would be considered to have a 'legal effect'.

88. Conversely, the absence of such protections in most Australian jurisdictions through a similar human rights instrument limits the utility of protections for subjects impacted by AI decisions with 'legal effect'. The introduction of a federal charter of rights would therefore be an important step to enhancing the protections provided by AI regulation.

'Similarly significant effects'

89. There has been considerable contention around the use of the phrase 'similarly significant effects'.

---

[46] *EU Guidelines*, above n 43, p 21.

[47] Paul Voigt and Axel von dem Bussche, T*he EU General Data Protection Regulation (GDPR): A Practical Guide,* Springer Press, 2018, 182.

[48] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76, 92-93; see also Lee Bygrave, 'Minding the Machine: Art 15 of the EC Data Protection Directive and Automated Profiling' (2000) 7 *Privacy Law and Policy Reporter* 67.

90. The EU Guidelines state that its inclusion indicates that the 'threshold for significance must be similar to that of a decision producing a legal effect'.[49] Therefore, 'similarly significant effects' are understood in the GDPR to mean those in which there is:

- no change to legal rights or obligations; and
- the data subject is still impacted sufficiently so as to require protection.

Academics have raised concerns around the vagueness of the term 'significant' in the context of Article 22 of the GDPR. The EU Guidelines provide limited guidance on the use of the term within the context of the GDPR. They state that 'significant' means 'sufficiently great or important to be worthy of attention'.[50] But this does little to elucidate the meaning of the term as it does not answer the question of what is 'sufficient', or 'important', nor the question of worthy of attention to *whom?*

91. Commentary from the Guidelines appears to indicate an objective standard. The EU specifies that such decisions must:

- Impact upon the circumstance, behaviour or choices of the data subjects;
- Have a prolonged or permanent impact on the data subject; or
- Lead to the exclusion or discrimination of individuals.[51]

92. Sandra Wachter, Brent Mittelstadt and Luciano Floridi, for example, question what perspective should be taken when defining significant effects – should such effects be significant from the subjective perspective of the data subject? Or measured by an external standard?[52] Other commentary in the Guidelines, however, suggests that 'significance' can be subjective in certain circumstances, stating that 'processing that might have little impact on individuals generally may in fact have a significant effect for certain groups of society, such as minority groups or vulnerable adults.'[53] Further, the Guidelines state that children require enhanced protection.[54]

93. As raised by Emily Pehrsson of Stanford University, this continued ambiguity 'could immerse the courts in a slew of litigation and hurt business across the EU by creating unpredictability in Article 22's application'.[55]

94. Examples of decisions that have similarly significant effects provided by the Guidelines include decisions that affect a subject's financial circumstances, health services, employment opportunity or access to education. EU Recital 71 specifically

---

[49] *EU Guidelines*, above n 43, p 21.
[50] Ibid.
[51] Ibid.
[52] Wachter, Mittelstadt and Floridi, above n 48, 98.
[53] EU Guidelines, above n 43, p 22; see also Emily Pehrsson, 'The Meaning of the GDPR Article 22' (2018) 31 *European Law Working Papers* 1, 16 <https://law.stanford.edu/wp-content/uploads/2018/05/pehrsson_eulawwp31.pdf>.
[54] EU Guidelines, above n 43, p 22.
[55] Pehrsson, *The Meaning of the GDPR Article 22,* above n 53.

names instances of online credit eligibility assessments and online employment recruiting as decisions which have 'similarly significant effects'.[56]

95. The inclusion of the word 'similarly' may not be advisable in the Australian context. Firstly, introducing a threshold of significance elevated to a standard akin to a legal right may create barriers to justice for vulnerable individuals not currently protected under existing legislation. As mentioned above for example, the absence of a federal charter of rights limits the grounds upon which subjects impacted by AI-informed decision-making make claim a decision has had 'legal effect'.

96. Further, AI regulation in Australia may benefit from the creation of similar guidelines to those in the EU, which further expand upon examples of AI-informed decision-making that would be considered to have a 'significant' effect. We thus **support**, as asked in the Discussion Question, that the concept of a decision with 'legal or similarly significant effect' should be supplemented with a list of non-exhaustive examples that may meet this threshold.

Decision making

97. The use of the term 'decision making', as opposed to 'decisions', appears to be in line with academic commentary on the subject.

98. This is primarily for two reasons, the first being that there is some contention as to whether AI systems *can* produce legitimate 'decisions'. Gloria Phillips-Wren, for example, contends that AI can only 'attemp[t] to mimic human decision-making in some capacity'.[57] Lillian Edwards and Michael Veale similarly raise that while AI systems can produce outputs as classifications or estimations, they are still 'incapable of synthesising the estimation and relevant uncertainties into a *decision* for action'.[58]

99. Australian courts have adopted a similar view. In the case of *Pintarich,* which concerned AI enabled automated systems used to calculate and claim social services debt for welfare recipients, the Federal Court of Australia found that no 'decision' was made 'unless accompanied by the requisite mental process of an authorised officer'.[59] This means that at least for administrative decisions, a human must be involved for a computed decision to constitute a legal decision.

---

[56] EU GDPR Recital 71, <https://www.privacy-regulation.eu/en/r71.htm>.

[57] Gloria Phillips Wren, 'Intelligent Decision Support Systems', in Gloria Phillips-Wren, Nikhil Ichalkaranje and Lakhmi Jain (eds), *Intelligent Decision Making: An AI-Based Approach*, Springer Press, 2008, 1.

[58] Edwards and Veale, above n 45, 46.

[59] *Pintarich v Deputy Commissioner of Taxation* [2018] FCAFC 79; (2018) 108 ATR 3; discussed in Ng and O'Sullivan, above n 35; see also Kobi Leins, 'What is the Law When AI Makes Decisions?', *University of Melbourne Pursuit* (Blog) <https://pursuit.unimelb.edu.au/articles/what-is-the-law-when-ai-makes-the-decisions>.

100. Secondly, it is also prudent, in the development of regulation, to generate protections for decisions not solely made by AI, but meaningfully assisted or impacted by AI.

Recommendations

- We **support** the proposal to require privacy policies to include information on whether personal information will be used in ADM which has a legal or significant effect on people's rights.

- However, we **recommend that the word 'similarly' be removed** from 'legal or similarly significant effect' as it adds another layer of confusion. There is a risk that 'similarly' could be used to limit rights protection and may lead to lengthy arguments in court about whether or not an effect is similarly significant to a legal effect.

- We **support** the Discussion Question that the concept of a decision with 'legal or similarly significant effect' be supplemented with a list of non-exhaustive examples that may meet this threshold. We recommend that the regulation should be accompanied by clear and accessible guidelines for duty-bearers and rights-holders with concrete examples.

IV. A direct right of action (chapter 25)

101. The Discussion Paper proposes to

25.1 Create a direct right of action with the following design 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.

102. The Discussion Paper asks the following 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?

In relation to this Question, **we make the following submissions. We also comment below** on the need to alleviate the burden on plaintiffs, in particular those in representative actions, to establish that they have suffered loss.

Availability of a direct right of action

- *The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.*

103. We **support** that the action should be available to any individual or group of individuals whose privacy has been interfered with by an APP entity. We agree with the analysis of the ACCC in the Final Report of the Digital Platform Inquiry that a direct right of action would provide consumers with greater control over their personal information, give more direct access to redress than the OAIC complaints process and create additional incentives to APP entities to comply with their obligations under the *Privacy Act* (or 'the Act').[60] It would give a complainant an avenue of redress that is additional to the complaints process involving the Privacy Commissioner, which has in the past often been criticised as lacking teeth.[61]

104. In addition to giving the law greater effectiveness, a greater role for courts in the enforcement of privacy rights as provided by a direct right of action would also give the Act over time more clarity and certainty. This is a particular concern in Australia as the Privacy Act, despite its more than 30 years of operation, has rarely been applied or interpreted by the courts. As a result, many key terms or obligations under the Act continue to be uncertain in their definition or operation. Creating further scope for private enforcement of the Act through legal proceedings would likely generate a greater number of judicial pronouncements on the interpretation of privacy obligations under the Act. These court decisions would not only decide the dispute in question, but also clarify and develop the law for future cases by create binding guidance on applicable data processing standards.

105. A direct right of action would furthermore align the *Privacy Act* with the Consumer Data Right regime in the *Competition and Consumer Act 2010* (Cth), which grants individuals the right to bring an action for damages against another person for breach of the consumer data rules relating to the privacy safeguards or to privacy and confidentiality of CDR data.[62] It would also bring the Australian *Privacy Act* in line with overseas data protection regimes, including those of the European Union,[63] New Zealand,[64] Singapore,[65] China[66], all of which grant direct rights. In the US, the federal

---

[60] Australian Competition and Consumer Commission, above n 7, p 473.
[61] For example, Australian Privacy Foundation, *Submission to Consultation Paper, Guide to Regulatory Action*, Ch. 2 [9], 5 June 2015, <https://privacy.org.au/Papers/OAIC-Reg-150605.pdf>.
[62] *Competition and Consumer Act 2010* (Cth), s 56EY.
[63] *General Data Protection Regulation* (EU), art. 82(1).
[64] *Privacy Act 1993* (NZ), s 88.
[65] *Personal Data Protection Act 2012*, s 48O.
[66] *Personal Information Protection Law*, art. 69.

Fair Credit Reporting Act,[67] the Illinois' *Biometric Information Privacy Act*[68] and now also the California *Consumer Privacy Act of 2018*[69] are among the statutes that allow for private actions in case of alleged violation.[70] A private right of action was also contained in the now lapsed Canadian bill for a new *Consumer Privacy Protection Act.*[71]

106. We **welcome that the Review does not propose to introduce a separate seriousness threshold**. We note that the Office of the Australian Information Commissioner likewise recommended not to limit the right of action to *serious* breaches.[72] Such a limitation would undermine the dual objective of the direct right of action of enhancing compliance with the Privacy Act and providing compensation for a proven interference with privacy. It is unlikely that the direct right of access to the court would be abused significantly by undeserving claimants. The cost associated with bringing an action in court would act as an appropriate disincentive to bringing claims that do not have sufficient prospect of success or that would yield only small amounts of damages. The existing barriers to, and burdens of, court actions can be expected to ensure that matters are unlikely to be brought to the court unless they are sufficiently serious. Depending on its wording, a seriousness requirement might also have the detrimental effect of excluding claims that affected large numbers of persons, but caused only minor loss or damage to each of them.

Jurisdiction of federal courts

- *The action would be heard by the Federal Court or the Federal Circuit Court.*

[67] The FCRA imposes civil liability for wilful or negligent failures to comply with its requirements (15 U.S.C. §§ 1681n, 1681o). Victims of a wilful failure to comply with an FCRA requirement may seek statutory damages of $100 to $1,000 or actual damages (15 U.S.C. § 1681n(a)(1)(A)), including damages for emotional distress; or punitive damages (15 U.S.C. § 1681n(a)(2)) as well as cost and reasonable attorneys' fees. Negligent non-compliance with FCRA requirements entitles to actual damages (15 U.S.C. § 1681o(a)(1)-(2)), including damages for emotional distress, as well as cost and reasonable attorneys' fees.

[68] Under BIPA, successful claimants can recover statutory damages of $1,000 for each negligent violation (and $5,000 for each intention or reckless violation) or actual damages, whichever is greater, as well as reasonable attorneys' fees and costs.

[69] Under s 1798.150(a)(1) of the CCPA, consumers have a private right of action for specified data breaches. If successful, claimants can recover statutory damages between $100 and $750 per incident, or actual damages.

[70] Other statutes allowing individual suits are the progeny the Privacy Act of 1974 (see, eg, 5 U.S.C. § 552a(g)
(1)(D)), the *Right to Financial Privacy Act of 1978* (see, eg, 12 U.S.C. § 3417), the *Cable Communications Policy Act of 1984*, the *Electronic Communications Privacy Act of 1984*, the *Video Privacy Protection Act of 1988* and the *Telephone Consumer Protection Act of 1991*.

[71] Bill C-11 for the introduction of a Consumer Privacy Protection Act, cl 106. The Bill lapsed with the end of the parliamentary term.

[72] Office of the Australian Information Commissioner, *Submission to Privacy Act Review: Issues Paper* (December 2020), rec. 51; Office of the Australian Information Commissioner, *Submission to Privacy Act Review: Discussion Paper* (23 December 2021), [25.7].

107. We **support** that the action should be heard by the Federal Court or Federal Circuit Court, including the suggestion in the Issues Paper that consideration be given to develop a cost-effective 'small claims procedure' for privacy matters.

Assessment for conciliation as a hurdle requirement

- *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.*

108. We **do not support** this requirement. Requiring that a complaint must first undergo conciliation assessment by the OAIC or some other body would create additional procedural steps and complicate the pathway to a remedy. It would, in effect, mean that the right to action was not direct, but merely indirect. Furthermore, many courts, including the Federal Court and the Federal Circuit Court, have existing procedures for mediation for parties who wish to resolve their dispute without going to trial. These existing mechanisms to protect the parties' and the court's resources also lessen the need to create another pre-trial dispute resolution hurdle.

109. In its submission to the Issues Paper, the OAIC has recommended that 'the direct right of action is framed so that individuals are required to make a complaint, or a representative complaint, to the OAIC before applying to the courts'.[73] This was intended to give the OAIC 'national oversight of privacy issues and the ability to identify potential systemic issues in the system that may warrant further regulatory or enforcement action'.[74] However, it is our view that these objectives could be pursued more effectively with other means. For example, the reform legislation could require plaintiffs to inform the OAIC of proceedings brought. Such a requirement would still give the OAIC notice of proceedings and enable it to identify any systemic issues, without requiring an individual who prefers to seek an adjudicated outcome to initiate, and await the OAIC's decision in relation to, a complaints-based process first. This notification requirement should be accompanied by a provision that gives the OAIC standing to participate in the proceedings (see below).

110. Furthermore, despite the OAIC's preference, we note that a requirement to seek an administrative decision first is not always the preferred choice of regulators overseas, as can be seen from the Canadian law reform discussion. As in Australia,[75] the public consultation on Canada's federal privacy law reform identified stakeholder support

[73] Office of the Australian Information Commissioner, *Submission to Privacy Act Review: Issues Paper* (December 2020), rec. 52. See also Office of the Australian Information Commissioner, *Submission to Privacy Act Review: Discussion Paper* (23 December 2021), rec. 100.
[74] Office of the Australian Information Commissioner, *Submission to Privacy Act Review: Issues Paper* (December 2020), [10.17].
[75] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey* (2020), p 67: 78% of the surveyed Australians believe they should have the right to seek compensation in the courts for a breach of privacy.

for an individual's right to seek direct recourse before the Federal Court.[76] The reform Bill C-11 for the introduction of a Consumer Privacy Protection Act ('Bill C-11') contained such a right, although only in a very restricted form. Under cl 106 of Bill C-11, the cause of action would have arisen only if the Office of the Privacy Commissioner of Canada made a finding of a contravention of the Act that can no longer be appealed, or the Tribunal made such a finding. In its submission to Parliament, the Commissioner rightly expressed concern that this was likely to increase its caseload, without improving individuals' access to timely justice.[77] The Bill lapsed with the Canadian federal election, so that a direct right of action, or other improvements of individual redress, remain on the country's legislative agenda for the new government. However, the Commissioner's concerns point to a serious issue: A requirement that the complainant must have exhausted recourse to the Commissioner before a court action becomes available would increase the Commissioner's case load and added delay to the process. It would have also made the direct right an annex to the complaints process, rather than creating an alternative to it. It is welcome that such a restrictive position is not under consideration in Australia.

111. While we **do not support any administrative hurdles to a direct right of action**, we submit that, if any such hurdle was introduced, it should be subject to a strict time bar. For example, it could be provided that a direct right of action becomes available if the complainant has not been informed by the OAIC (or other conciliation body) of the assessment for conciliation within two months after the complaint is made.

112. Another compromise option is that adopted by the Personal Data Protection Act ('PDPA') in Singapore, which also temporarily bars court action but only where the complainant has chosen to make a complaint first. Under the PDPA, the direct right of action is not available if the Personal Data Protection Commission has made a decision under that Act in respect of a contravention, until after the decision has become final. This allows a data subject to decide at the outset whether to make complaint or whether to bring a claim in the courts without any further hurdle. However, in cases where a complaint has been made, the temporary bar avoids a situation in which an existing decision of the Commissioner is bypassed by initiating a court action before the administrative process has taken its course.

OAIC standing as amicus curiae

- *The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court.*

113. We **support** the recommendation to give the OAIC standing to appear as *amicus curiae* to provide expert evidence. There are international models for this approach:

[76] Government of Canada, *Modernization Canada's Privacy Act: What we heard – Report, Justice Canada's online public consultation on Privacy Act modernization* (Fall 2020 to Winter 2021), p 17.
[77] OPC, *Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020* (May 2021), rec. 41.

Under the European regimes, a national data protection authority can likewise intervene or appear as *amicus curiae*, if the claim was filed within its jurisdiction or has the potential to affect its jurisdiction.

Remedies available

- *Remedies available under this right would be any order the court sees fit, including any amount of damages.*

114. Subject to one point addressed below, we also **support** the recommendation that the **court should have the power to make any order the court sees fit, including any amount of damages**. In our view, there is no need to restrict the decision-making power of the court, in particular to impose a cap on damages.

115. While state privacy legislation imposes limits of $100,000,[78] $60,000[79] and $40,000,[80] respectively, on the respective Tribunals' power to award damages, comparable Australian federal legislation providing for a direct right of action does not impose a cap on damages. Notably, section 46PO(4)(d) of *Australian Human Rights Commission Act* 1986 (Cth), which sets out the remedial powers of the Court in unlawful discrimination cases, contains a broad – and unfettered – power to 'make such orders (including a declaration of right) as it thinks fit including an order requiring a respondent to pay to an applicant damages by way of compensation for any loss or damage suffered because of the conduct of the respondent'.[81] While there are undeniably qualitative differences between an interference with privacy and unlawful discrimination, both these wrongs have in common that they affect dignitary interests of the complainants, and therefore primarily cause non-pecuniary losses.[82] It would promote coherence between both statutes, and the areas of human rights protection they regulate, if the statutory powers to award compensation in judicial proceedings were aligned with each other. This would also assist the federal courts that administer these statutes to interpret and apply them in a consistent fashion.

116. The Discussion Paper referred to the concern by some submitters that a statutory cap on damages would help 'to balance the tension between adequately compensating individuals and unduly burdening business'.[83] This, of course, begs the question of whether capped compensation is '***adequate'*** when it leaves plaintiffs who have suffered particularly serious harm partially uncompensated, or whether a

[78] *Information Privacy Act 2009* (Qld) s 178(a)(v); *Privacy and Data Protection Act 2014* (Vic) s 77(1)(a)(iii).
[79] *Information Act* (NT) s 115(4)(b).
[80] *Privacy and Personal Information Protection Act 1998* (NSW) s 55(2)(a); *Health Records and Information Privacy Act 2002* (NSW) s 54(1)(a).
[81] There are also no caps for compensation claims under the *Competition and Consumer Act 2011* (Cth) and the *Corporations Act 2001* (Cth).
[82] Decisions of the AHRC on compensation have been highly influential on the OAIC in exercising its power to determine that a complainant is entitled to compensation under the Privacy Act: For detail, see Normann Witzleb, 'Determinations under the Privacy Act 1988 (Cth) as a privacy remedy' in JNE Varuhas and NA Moreham (eds), *Remedies for Breach of Privacy* (Oxford, Hart Publishing, 2018) pp 377-408.
[83] Attorney-General's Department, above n 1, p 189.

business entity is indeed '*unduly'* burdened if it is required to compensate the harm arising from its encroachments into another's privacy without the benefit of a cap.

117. Apart from that, we **submit** there is **no indication that a cap is needed** to prevent the court from making excessive awards. In the seminal decision in *Hall v A & A Sheiban Pty Ltd*[84] on the award of compensation in unlawful discrimination cases, the Full Court of the Federal Court laid down the principle that awards should be restrained but not minimal.[85] This has led courts to adopt a 'cautious approach' and fix awards at a 'conservative level', as was noted in the 2014 decision of *Richardson v Oracle Corporation Australia Pty Ltd*.[86] In a review of the awards made over the period of 30 years since the enactment of the SDA, Kenny J found that the damages range of between $12,000 and $20,000 had not changed much over the last 15 years, with the consequence that damages over that period had fallen substantially below community expectations. In *Richardson*, the appellant was the victim of sexual harassment over some months, and suffered significant distress, anxiety and psychological injury in the form of a chronic adjustment disorder. At first instance, she was awarded $18,000 as compensation for non-economic loss under section 46PO(4)(d) of the AHRC Act. The Full Court held that this amount, while within the previously accepted range for such cases, was manifestly inadequate as compensation for her loss and damage when judged by prevailing community standards. In light of her analysis, Kenny J held that an award for non-economic loss of $100,000 should be substituted for the award made at trial of $18,000.

118. This landmark decision, and its reasoning, has subsequently been adopted in discrimination cases under other anti-discrimination statutes,[87] including at State level,[88] where tribunals also emphasised that no distinction should be made between the approach to damages taken in a court or a tribunal.[89] While the decision in *Richardson* has significantly reshaped the approach to damages assessments under the SDA and other anti-discrimination statutes, there is no suggestion that it has paved the way to excessive awards. Courts and tribunals are clearly alert to the need for compensation levels to be attuned to community expectations. In light of this responsible and cautious jurisprudence, we submit that a cap on damages is unnecessary to curb compensation awards. Indeed, a cap, if not regularly adjusted, may carry the risk that damages awards over time become unduly depressed and therefore do not perform their statutory objectives.

119. The Discussion Paper Paper adopted the recommendation in the DPI Report that 'aggravated and exemplary damages (in exceptional circumstances) for the financial

---

[84] (1989) 20 FCR 217.
[85] Ibid, 238 (Lockhart J) referring to *Alexander v Home Office* [1988] 2 All ER 118.
[86] Richardson v Oracle Corporation Australia Pty Ltd [2014] FCAFC 82; (2014) 223 FCR 334.
[87] See, eg, the significant decision by Mortimer J in *Wotton v State of Queensland (No 5)* [2016] FCA 1457, [1598]–[1618] (representative proceedings by Palm Island residents concerning unlawful racial discrimination by Queensland police).
[88] *Chalker v Murrays Australia Pty Ltd* [2017] NSWCATAD 112; *Green v State of Queensland, Brooker and Keating* [2017] QCAT 008; Power v Bouvy [2015] TASADT 2; *Collins v Smith (Human Rights)* [2015] VCAT 1029; Kovac *v The Australian Croatian Club Ltd (No. 2) (Discrimination)* [2016] ACAT 4.
[89] *Green v State of Queensland, Brooker and Keating* [2017] QCAT 008; *Collins v Smith (Human Rights)* [2015] VCAT 1029.

and non-financial harm suffered as a result of an infringement of the Act and the APPs'[90] should be awarded. In our view, courts should be available to award aggravated damages, but we **do not support** the power to award **exemplary damages**.

120. Aggravated damages are compensatory, whereas exemplary damages have a punitive function. A court may award aggravated damages where the particular manner in which a wrong has committed added insult, humiliation and the like to the emotional hurt felt by the plaintiff.[91] It is clearly a legitimate objective of a claim under a direct right of action to seek compensation for such harm. However, there is less justification to introduce a power to award exemplary damages in civil proceedings. If the defendant to a claim under a direct right of action has acted in a way that is deserving of punishment, the matter of punishment is more appropriately dealt with by use of the Information Commissioner's enforcement powers.

121. The Commissioner has the power to seek pecuniary penalty orders but does not have the power to determine that a complainant be paid exemplary damages. Based on the wording of section 52(1)(iii) of the Privacy Act, which refers to an entitlement to an 'amount by way of compensation for any loss or damage suffered', the Commissioner has explained repeatedly that the determination power does not extend to punitive awards. In determinations considering the issue, the Commissioner referred to decisions under the (former) section 81 of the *Sex Discrimination Act 1984* (Cth) ('SDA'), the predecessor of s 46PO of the *Australian Human Right Commission Act 1986* (Cth), which has likewise been held not to include a power to grant exemplary damages. In obiter comments in *Hall v A & A Sheiban Pty Ltd,*[92] the Full Federal Court expressed the tentative view that exemplary damages are not available under the SDA because they cannot properly be characterised as damages 'by way of compensation', as they would be awarded in addition to any compensation if the conduct of the respondent was of a particularly outrageous nature.[93] There have been a number of subsequent decisions which have contemplated making or made exemplary awards, but the position continues to be uncertain.[94]

122. Similarly, the possibility of a punitive award under the NSW privacy legislation[95] was left open by the former President of the NSW Administrative Decisions Tribunal. In *RD v Department of Education and Trainin*g,[96] O'Connor DCJ raised the possibility that 'some punitive component' could be 'incorporated into the damages award' if an 'error was not remedied at the first point at which it could reasonably have been

[90] Attorney-General's Department, above n 1, p 189 referring to Australian Competition and Consumer Commission, above n 7, p 473.
[91] *Lamb v Cotogno* [1987] HCA 47; (1987) 164 CLR 1 at 8.
[92] (1989) 20 FCR 217.
[93] Ibid 240-41 per Lockhart J; 282 per French J, referring to the equivalent limitation under (former) s 82 of the Trade Practices Act 1974 (Cth).
[94] The cases (up to 2016) are discussed in *Federal Discrimination Law Online*, a compendium maintained by the Australian Human Rights Commissioner.
[95] See *Privacy and Personal Information Protection Act 1998* (NSW), s 55(2) and *Health Records and Information Privacy Act 2002* (NSW), s 54(1).
[96] *RD v Department of Education and Training* [2005] NSWADT 195.

identified'.[97] In *NZ v Director General, Department of Housing*, O'Connor DCJ reiterated that he did 'not see any difficulty in awarding aggravated or exemplary damages if the case justifies it'.[98] In neither case was an award for punitive damages actually made. In *NK v Northern Sydney Central Coast Area Health Service (No. 2)*, the Tribunal identified a significant number of breaches of privacy obligations by a hospital, in which NK was both a patient and an employee, causing very serious consequences for NK's health and work. Montgomery S held that the respondent's conduct amounted to an 'oppressive disregard of NK's rights and its own privacy duties'.[99] While the availability of exemplary damages was considered, the issue was not determined because the Tribunal decided to award $40,000, the statutory maximum amount of damages available under the NSW legislation. The questions of whether the NSW Acts indeed contain a power to award exemplary damages and whether it could be exercised in the wide circumstances identified by the obiter comments of O'Connor DCJ, therefore must be regarded as unresolved.

123. To avoid similar uncertainty under the Privacy Act, it would be **desirable for the legislation introducing a direct right of action to clarify whether or not exemplary damages are available**. We **advocate** for the reasons above that the legislation should state that **exemplary damages are not available**.

Alleviate the burden to establishing loss

124. The direct right of action is potentially a powerful tool to enhance compliance with privacy principles and to provide redress for persons whose privacy rights have been disregarded. However, it is important that the remedial and procedural mechanisms are adapted to this purpose and do not erect undue barriers to redress. Local and overseas experience has shown that demonstrating loss as a result of a contravention of data protection rules can be a significant obstacle to a successful claim. This is a particular issue in representative proceedings.

125. In the matter of *'WP' and Secretary to the Department of Home Affairs (Privacy)*, the Department unwittingly disclosed personal information of over 9,258 individuals in immigration detention on a publicly available website, including their names, dates of birth, location, periods of detention and the reasons of why they were considered unlawful non-citizens. Following a representative complaint, the Privacy Commissioner determined that the Department's conduct was in breach of the APPs and that class members were to be paid compensation for loss or damage arising from the publication provided they submitted evidence on their feelings of hurt and/or humiliation.

126. While the solicitors for the representative complainant submitted that the assessment of compensation should assume a common element of loss suffered by all class members, which could then be adjusted on the basis of individual submissions, the Commissioner rejected this approach. The Commissioner held:

[97] Ibid, [33].
[98] *NZ v Director General, Department of Housing* [2006] NSWADT 173, [52].
[99] *NK v Northern Sydney Central Coast Area Health Service (No 2)* [2011] NSWADT 81, [60].

> Assessing compensation by having regard to each class member's reaction requires the provision of individualised submissions and/or evidence.[100] Non-economic loss is of an inherently personal nature and does not lend itself to a declaration that class members are entitled to compensation without some evidence from those class members as to their loss. This approach is in keeping with the determination in *'PB' and United Super Pty Ltd as Trustee for Cbus (Privacy)*[101] in which the then Commissioner stated that the onus of establishing loss or damage is on the complainant,[102] and unless an individual member of the class supplies evidence of loss or damage, they are not entitled to a remedy.[103]

127. The Commissioner gave notice of the requirement for class members to make a claim for loss and/or damage, but despite attempts to communicate this notice, only about 1,300 (out of over 9,000) class members provided submissions to the OAIC. The vast majority of the class members were therefore held not to be entitled to compensation.

128. The approach adopted in these proceedings demonstrates that insistence on individual proof of loss has the potential to leave large numbers of complainants without redress despite a demonstrated interference with their privacy.

129. Similar problems have become apparent overseas. In the UK, the recently resolved *Lloyd v Google LLC* litigation[104] tested the potential and limits of data class actions. The claimant, Mr Lloyd, was a consumer advocate who brought a claim on behalf of more than 4 million Apple iPhone users for tracking by Google Inc between 2011 and 2012 in alleged breach of the DPA. As the UK allows class actions only in competition law cases, the claimant brought the action as representative proceedings.

130. In *Lloyd*, the representative claimant did not argue that members of the class suffered emotional harm as a result of the alleged interference with their data rights. Instead, the claimant submitted, with support by the Information Commissioner, that compensation should be awarded for the 'loss of control' of personal data constituted by any non-trivial contravention by a data controller of any of the requirements of the Act. The claim was for a uniform amount of damages to each class member. The Court of Appeal accepted the claimants' argument that, if damages are available without proof of pecuniary loss or distress for the tort of misuse of private information, they should also be so available for an infringement of the *Data Protection Act 1998* (UK). This finding built on the Court's earlier decision in *Gulati v MGN Limited*[105] that, in claims for the tort of misuse of private information, damages could be awarded for the loss or diminution of his right to control the use of that private information, and that claimants were not required to show pecuniary loss or distress. While the Court of Appeal allowed the action to proceed on that basis, the Supreme Court

[100] *BMW Australia Ltd v Brewster* [2019] HCA 45; (2019) 269 CLR 574.
[101] [2018] AICmr 513.
[102] Ibid, [83].
[103] Ibid, [91].
[104] [2019] EWCA Civ 1599; [2020] QB 747.
[105] [2015] EWCA Civ 1291; [2017] QB 149.

unanimously decided to reject this widening of the damage requirement and did not allow the representative claim to proceed.

131. In particular, the Supreme Court held that:

- properly interpreted, the term 'damage' in DPA 1998 s. 13 means material damage, such as financial loss, or mental distress resulting from unlawful data processing. The unlawful processing of personal data in contravention of the Act, i.e. the 'loss of control' over personal data is not of itself a compensable damage; and
- it was necessary, in order to recover compensation under s. 13, to prove what unlawful processing of personal data relating to a given individual was undertaken by Google.

132. While the exact implications of the Supreme Court decision in *Lloyd v Google LLC* are yet to be worked out, it can be predicted that the prospect of class-action like representative proceedings for privacy breaches in the United Kingdom are now dampened.

133. These two cases illustrate that a strict requirement to establish loss on members of a class to demonstrate individual loss affects the capacity of direct rights of action to provide meaningful redress. We therefore **submit** that the direct of action should not require individual proof of actual loss, where members of a class can demonstrate that the contravention of the Act has affected all or a significant number of members in a substantially similar way. We **submit that the Privacy Act should make clear that the interference with the privacy of an individual, as defined in the Privacy Act (s 13), as such constitutes an actionable harm**.

134. In the US, class actions are an established mechanism to address data security breaches or other consumer privacy interferences, especially where they occur at mass scale. Class actions are facilitated through legislative provisions that allow for claims of a statutory amount of damages, irrespective of proof of actual financial or emotional harm. The federal Fair Credit Reporting Act,[106] the Illinois' Biometric Information Privacy Act[107] and now also the California Consumer Privacy Act of 2018 are among the statutes that allow for private actions in case of alleged violation and do not require actual damages in class actions to be established. Under s 1798.150(a)(1) of the CCPA, consumers have a private right of action for specified

[106] The FCRA imposes civil liability for willful or negligent failures to comply with its requirements (15 U.S.C. §§ 1681n, 1681o). Victims of a willful failure to comply with an FCRA requirement may seek statutory damages of $100 to $1,000 or actual damages (15 U.S.C. § 1681n(a)(1)(A)), including damages for emotional distress; or punitive damages (15 U.S.C. § 1681n(a)(2)) as well as cost and reasonable attorneys' fees. Negligent non-compliance with FCRA requirements entitles to actual damages (15 U.S.C. § 1681o(a)(1)-(2)), including damages for emotional distress, as well as cost and reasonable attorneys' fees. However, despite this, the US Supreme Court recently denied standing to claimants who could not show 'concrete harm': *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021). For a critique of this decision, see Daniel J Solove and Danielle Keats Citron, 'Standing and Privacy Harms: A Critique of TransUnion v. Ramirez' (2021) 101 *Boston University Law Review Online* 62.

[107] Under BIPA, successful claimants can recover statutory damages of $1,000 for each negligent violation (and $5,000 for each intention or reckless violation) or actual damages, whichever is greater, as well as reasonable attorneys' fees and costs.

data breaches. If successful, claimants can recover statutory damages between US$100 and US$750 per incident, or actual damages.

135. Given that providing evidence of actual harm can cause difficulty for class action claimants, we **submit** that **consideration should be given to creating similar statutory mechanisms** for the direct right of action under the Australian Privacy Act.

V. A statutory privacy tort (chapter 26)

136. The question of whether a statutory privacy tort should be introduced has been considered many times over the last twenty years or more. Numerous Australian law reform bodies recommended the introduction of a statutory cause of action for invasion of privacy.[108] The most influential, and most detailed, was the report has been published by the Australian Law Reform Commission in 2014 after extensive community consultation.[109] Yet, victims of privacy invasion in Australia still need to rely on a patchwork of general law and statutory provisions that applies to specific aspects of privacy but does not provide comprehensive protection.

137. A statutory right to privacy, actionable in tort law, would not supplant the existing mechanisms, but instead address the current gaps in the protection of privacy interests and provide suitable remedies to victims of privacy invasion, including damages and injunctions. In light of the unanimous support over many years for legislative action by successive law reform and parliamentary inquiries, which all included public consultation processes, it is disappointing that the federal Government continues to hesitate doing so.

138. The Discussion Paper explained that the submissions in favour of establishing a tort for invasions of privacy were 'largely from individual submitters, academics, privacy regulators and experts, and not-for-profit entities focused on cybersecurity, consumer advocacy and digital rights'.[110] Tellingly, opposition to this proposal was 'mostly from media and business stakeholders',[111] which suggests that opposition to this necessary and overdue reform is mainly the product of self-interest, rather than concern for best possible regulation.

139. The Discussion Paper did not make a proposal to introduction of a privacy tort. Instead, it merely proposed that the 'need for a statutory tort for invasions of privacy

[108] For example: New South Wales Law Reform Commission, *Invasion of Privacy* (Report 120, 2009); Victorian Law Reform Commission, *Surveillance in Public Places* (Final Report 18, 2010); Law Reform Committee of the Victorian Parliament, *Report of Inquiry into Sexting* (May 2013), endorsing the recommendation of the VLRC; NSW Legislative Council Standing Committee on Law and Justice, *Remedies for the serious invasion of privacy in New South Wales* (Report no. 57, 2016); South Australian Law Reform Institute, *Too much information: A statutory cause of action for invasion of privacy* (Final Report 4, 2016).
[109] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report 123, 2014).
[110] Attorney-General's Department, above n 1, p 191.
[111] Ibid, p 192.

will continue to be considered following responses to the Discussion Paper'[112] and identified four possible models of further regulation, as follows:

26.1 Option 1: Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.

26.2 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.

26.3 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.

26.4 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.

Preferred Option: Introduce a statutory tort for invasion of privacy

140. This submission **supports option 1** for the introduction of a statutory tort for invasion of privacy. Subject to **one modification**, we recommend the adoption of the tort developed by the ALRC Report 123.

141. The following discussion will set out the reasons why option 1 – **a fully developed statutory privacy tort** – is the preferable way forward and also explain the problems that we have identified with options 2 – 4.

Why a privacy tort is needed

142. One argument commonly put forward against the enactment of a statutory privacy tort is that there is no demonstrated need for it given the existing protections at general and statute law. However, the weight of submissions to Issues Paper suggests that the majority of stakeholders, and the community broadly,[113] have valid concerns about increasing threats to privacy and would prefer a tort to be enacted. The Discussion Paper outlines some of the key areas in which the current law that relies on incidental protection of privacy through other wrongs has shortcomings, including in relation to its uncertain operation and remedies.

143. A second argument relates to the concern that a statutory privacy tort has the potential to stifle media expression. However, on closer consideration this argument also lacks force. The ALRC was at pains to limit the scope of the privacy tort so as to protect media freedom. Indeed, it could be argued that the design of the ALRC cause of action leans more to protecting potential defendants than potential plaintiffs. The restrictive aspects of the tort include the fact that it requires intentional or reckless conduct, and that it introduces a threshold requirement of a *serious*

[112] Ibid.
[113] Office of the Australian Information Commissioner, above n 78.

invasions of privacy. There are several additional mechanisms to ensure that that the defendant's legitimate interests are protected. First, the 'seriousness threshold' operates in addition to the public interest balancing test, a construction which the ALRC acknowledges was intended to 'further ensure the new tort does not unduly burden competing interests such as freedom of speech'.[114] It has been argued that this design feature has the potential to cause 'duplication'[115] and may not be necessary to deter or exclude trivial claims. Second, the ALRC purposefully made it part of the plaintiff's case to demonstrate that the public interest in privacy outweighs the public interest in freedom of expression. This means that it is the plaintiff who carries the ultimate burden of establishing that the interest in privacy should prevail over other public interests. By requiring that the *public* interest in privacy outweigh other public interests, the plaintiff must also establish that her private interest in maintaining her privacy coincides with a corresponding public interest. This has the potential to discount any interest in privacy that does not transcend into the public domain.

144. It cannot be denied that a privacy tort may on occasion limit freedom of speech – to some extent, that is precisely its point. However, the introduction of a statutory privacy tort with finely calibrated defences would ensure that this occurs only where the significance of a person's privacy demonstrably outweighs conflicting public interests, including the interest in free speech. Other torts or equitable causes of action that protect privacy interests only incidentally have not been moulded to respond to the delicate balancing exercise between privacy and other public interests. In their interplay, the features of the ALRC tort ensure that the legitimate interests of others are more than adequately protected. Indeed, as will be explored below, consideration should be given to proposals to widen the scope of protection in some respects.

A well-considered model is available

145. ALRC Report 123 provides a careful analysis of the need for a statutory action to protect privacy. The recommendations of the ALRC were the result of extensive community consultation and took into account comparative research into the law in other jurisdictions. These recommendations have been referred to, and generally been cited with approval, in all subsequent Australian law reform enquiries on the matter.

146. In July 2019, the Australian Competition and Consumer Commission (ACCC) added its voice in support of the introduction of a statutory cause of action for serious invasions of privacy. In the Final Report of its major inquiry into Digital Platforms, the ACCC proposed that the statutory privacy tort should be enacted in the form that had been recommended by the Australian Law Reform Commission (ALRC) in 2014. In December 2019, in the context of its ongoing inquiry into Human Rights and

[114] ALRC, above n 109, [8.15].
[115] David Lindsay, 'A privacy tort for Australia? A critical appreciation of the ALRC report on serious invasions of privacy' (2015) 12 *Privacy Law Bulletin* 8, 10.

Technology, the Australian Human Rights Commission (AHRC) also proposed that this ALRC recommendation be implemented.

147. Although both Commissions made their proposals in different contexts, their respective calls for legislative action respond to the common threat that the rise of modern data-driven technology poses for individual privacy. The AHRC expressed the expectation that a statutory privacy tort could address concerns about the potential misuse of personal information in the context of decision-making informed by artificial intelligence. The ACCC Digital Platforms Inquiry examined the adequacy of Australian regulation of digital platforms in light of their transformative impact on the news media and advertising sector. Data protection and privacy laws were just one aspect of a broad-ranging inquiry that also included competition law, media law and consumer protection law. Given this focus, the ACCC was persuaded that a statutory cause of action would increase the accountability of businesses for their data practices and give consumers greater control over their personal information.

Avoiding divergence within Australia

148. The proposals of the ALRC have also guided law reform recommendations at state level. This includes the report of the South Australian Law Reform Institute,[116] which has led to the introduction of a draft Civil Liability (Serious Invasions of Privacy) Bill 2021. In Queensland, the Crime and Corruption Commission also recommended that the Government consider the introduction of a statutory cause of statutory tort for serious invasion of privacy.[117] It would be undesirable if the civil law on privacy protection was to differ across Australia. However, this outcome may eventuate if the federal government fails to legislate in the area, but state governments decided that statutory law reform is needed to enhance privacy protection.[118] A divergence in tort law on privacy invasion would not only increase the transaction costs for media outlets operating across Australia. It would also create complex conflicts of law issues, which could lead to forum shopping and difficulties in identifying the applicable laws.[119]

The ALRC model allows further fine tuning

149. We submit therefore that the ALRC recommendations for a statutory privacy tort serve as a highly useful model for a statutory tort.

[116] South Australian Law Reform Institute, above n 108.
[117] Crime and Corruption Commission Queensland, *Operation Impala – A report on misuse of confidential information in the Queensland public sector* (February 2020), rec. 17 (p 130).
[118] In NSW, the opposition introduced a Civil Remedies for Serious Invasions of Privacy Bill 2020 into Parliament. The bill lapsed.
[119] For detailed consideration of these issues, Harder and Witzleb, 'The private international law implications of a privacy tort under state or territory legislation' (2016) 21 *Media and Arts Law Review* 121.

150. In formulating the scope of the cause of action, the ALRC has been guided by the concern that the 'Act should provide as much certainty as possible on what may amount to an invasion of privacy'.[120] A statutory cause of action would provide a reliable basis from which the courts could decide individual cases and develop the finer detail of the law.

Option 2: Introduce a minimalist statutory tort

151. A minimalist statutory privacy tort would help overcome the reluctance of Australian courts to recognise a right to privacy. It would create the tort by statute, but then leave its further design and development in the hands of the court. This would be likely to break the current deadlock and ensure that Australia's privacy protection no longer lags behind its counterparts in other common law jurisdictions. This model would be vastly preferable to continuing with the status quo in circumstances where the Australian courts have shown limited appetite for the development of new privacy tort. However, there are several reasons why this approach is overall less desirable than the enactment of a fully fleshed-out statutory tort.

152. Option 2 would leave the development of major aspects of the law in the hands of judges. Our key concerns are that that approach would create more uncertainty and higher costs to litigants, it would take longer for the law to develop and any incremental change to the law on a case-by-case basis is unlikely to reflect community expectations as closely as the proposed statutory tort.

Less democratic legitimacy

153. While tort law has traditionally been the domain of the courts, the more recent trend has been for major reforms to be enacted by statute. Examples of this are the civil liability legislation in all Australian jurisdictions, which deals largely with negligence liability, as well as the uniform defamation statutes to modernise Australian defamation law.

154. Parliamentary enactments in this area ensure that the reform acts have democratic legitimacy and that the form this legislation takes is subject to public scrutiny and political accountability. The enactment of a privacy tort through statute would allow for further public consultation during the legislative process and ensure that the design of the action weighs the conflicting policy positions through parliamentary deliberation.

More uncertainty

[120] Australian Law Reform Commission, above n 109, [5.76].

155. It is true that privacy protections have been developed through the courts in the majority of comparable jurisdictions. This has been the case in the United Kingdom, New Zealand and, although statutory torts exist in some provinces, in parts of Canada. However, in all these jurisdictions, a bill of rights or other human rights legislation has provided a framework for the judicial development of a cause of action to protect privacy. Often, courts have been prompted to recognise a common law right to privacy by considering human rights legislation which guarantees a right to respect for private life alongside other fundamental freedoms, including the right to freedom of expression.

156. In Australia, the absence of a federal human rights instrument has not only stultified the development of a common law right to privacy but also means that the future development of the privacy tort would not be able to draw on such a framework. Moreover, the different fundamental rights context in Australia also means that the more developed jurisprudence in other common law jurisdictions will be of less assistance in formulating this new tort than it would be in other, less rights-sensitive context of torts law.

157. This means that the development of a privacy tort in Australia would be less predictible if only a minimal statutory tort was introduced. There would also be no guarantees that the tort would weigh the conflicting stakeholder concerns as sensitively as the ALRC did in its inquiry into the statutory tort. Ironically, this may not only affect potential privacy claimants, but also potential defendants whose countervailing interests may then be protected to a lesser degree than envisaged by the proposed statutory tort.

158. Furthermore, if a minimalist tort was introduced, it would need to be decided how minimalist such a tort should be. The design of a tort raises a number of potentially contentious issues, including:

    a. Should the tort be available broadly for an invasion of privacy, or – as proposed by the ALRC – only for misuse of private information and intrusion into seclusion?
    b. Should the tort require conduct that is 'highly offensive to a reasonable person' or – as proposed by the ALRC – have a seriousness threshold?
    c. Should the tort have a fault element and, if so, should the fault element be intention and recklessness (as proposed by the ALRC)?
    d. Should the tort be actionable per se (as proposed by the ALRC)?
    e. Should the weight of the countervailing public interest in freedom of speech be considered as a defence or – as proposed by the ALRC – as part of the cause of action?
    f. Which defences should be available?
    g. Which remedies should be available?

Unclear process

159. By definition, a minimalist tort would require Parliament to decide on some of these issues but leave others for future determination in the courts. The Discussion Paper suggests that the Canadian privacy statutes are examples of a minimalist approach. For example, similar to the statutes in some of the other provinces, section 1 of the Privacy Act of British Columbia[121] provides:

(1) It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.
(2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.
(3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.
(4) Without limiting subsections (1) to (3), privacy may be violated by eavesdropping or surveillance, whether or not accomplished by trespass.

Section 2 of the Act then goes on to define 'exceptions' to liability, which amount to defences.

160. While the ALRC tort is more specific than the Canadian tort, it is apparent that much of the scope and shape of the Canadian torts has been defined by Parliament. If option 2 were to emulate the Canadian model, which elements should be determined by Parliament and which would better be left to the Court?

161. Indeed, we **submit** there seems to be little justification to leave any (or all) of these issues in the hands of the courts after many law reform and parliamentary inquiries have poured over these issues intensely and with significant community input – and have reached conclusions which subsequent inquiries into the matter have frequently endorsed.

Parliament must grasp the nettle

162. Government and Parliament would shirk their responsibility if they introduced a tort that is deliberately vague or incomplete. The available options are all on the table and have already been carefully considered many times over. It is difficult to see what advantages might be gained by adopting a minimalist approach unless it was thought than courts were better equipped to decide the arising policy questions than a decade-long law reform process.

163. Furthermore, a tort developed by the common law may lack some desirable features because of the courts' limited power and ability to innovate. For example, while common law torts trigger a limited range of remedies, in particular damages and an

[121] RSBC 1996, Chapter 373.

injunction, the ALRC proposed that the statutory tort should enable plaintiffs to seek a very wide range of remedies, including some innovative remedies that a court may consider to be beyond its powers to introduce, such as an order to publish a correction of false information,[122] or an order that the defendant must apologise.[123] Such features of a privacy tort could only be introduced by statute.

Slower development

164. Common law development of the law allows legal principles to be developed in the context of real-life situations. However, it is also a slow and often not very linear process. In the United Kingdom, the tort of misuse of private information has taken the better part of two decades to develop and reach a level of maturity – despite the UK being a much larger jurisdiction in Australia with a higher case load and despite UK courts being able to derive significant assistance from the jurisprudence of the European Court of Human Rights relation to Article 8 (privacy) of the European Convention on Human Rights in developing the tort. New Zealand, as a significantly smaller jurisdiction, has had only a small number of cases since the tort of misuse of personal information was first recognised by the Court of Appeal in 2005,[124] and very few appellate decisions.

165. As recognised in the Discussion paper, the exact shape of the tort may therefore take many years to develop, which is undesirable.

Access to justice

166. Given the long history of courts avoiding a decision on a common law right to privacy, plaintiffs with a privacy claim tend to be reluctant to argue for the recognition of such a right. Arguments in favour of a common law right of privacy are a risky strategy, leading plaintiffs instead to rely on other avenues of redress where available, or pleading a right to privacy only as an alternative to other claims (as happened in *Giller*). The fact that a common law right to privacy remains a 'high stake' issue has the potential to leave some privacy plaintiffs without redress, in particular if they do not have the strength or financial resources to argue this matter all the way to the High Court.

Option 3: Allow the common law to develop as required and extend application of the Act

167. This option would have the benefit of extending the protection afforded by the Act to certain problematic privacy invasive activities of individuals that are not currently regulated by it, provided they meet the threshold of being highly offensive to an objective reasonable person. However, as pointed out in the Discussion Paper, this

[122] Australian Law Reform Commission, above n 109, rec. 12-10.
[123] Ibid, rec. 12-11.
[124] *Hosking v Runting* [2005] 1 NZLR 1 (CA).

option would continue to leave significant gaps in the protection of privacy interests. We **submit** that it is therefore **less preferable than both Option 1 and Option 2**.

168. In particular, the extension would not apply to activities that fall outside the information handling practices covered in the Act, in particular the 'mere' intrusion into another's private affairs that does not lead to the collection, use or disclosure of personal information.

169. It is also unclear how this measure would sit with any of exemptions that might be retained in the revised Act. For example, would liability arise if an individual acted in a non-business capacity, but the practice fell under the exemptions for political or for journalistic acts? Similarly, there is the potential for incoherent outcomes, if an individual acting in a non-business capacity may incur liability whereas an entity operating an exempt small business would not.

170. Lastly, this measure would require the enactment of suitable defences where defendants engaged in these practices for legitimate reasons (such as in the exercise of their freedom of speech).

171. The wording of this option suggests that the gaps in coverage just outlined would be addressed by allowing the common law to develop as required. However, **in our view, this approach is unsatisfactory**, not only for the reasons outlined above in relation to Option 1 in respect of problems resulting from the absence of a statutory privacy tort in Australia but also for the following reasons.

172. Nearly 20 years have passed since the High Court declared in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*[125] that there are no obstacles to the recognition of a common law right to privacy. The High Court confirmed this position very recently in *Smethurst v Commissioner of Police*.[126] Yet, despite this assurance, no Australian appellate court has to date seen fit to recognise the existence of a privacy tort. In the courts, the law of privacy protection appears to not have moved significantly beyond the 2008 decision of the Victorian Court of Appeal in *Giller v Procopets*.[127] In that case, the defendant sought to humiliate and distress the plaintiff after the breakdown of their long-term relationship by distributing videotapes that showed the couple engaging in sexual intercourse. The plaintiff pleaded three causes of action arising from that conduct: breach of confidence, intentional infliction of emotional distress, and invasion of privacy. However, the Court considered it unnecessary to decide whether such a generalised tort of invasion of privacy should be recognised.[128] It was content to protect the plaintiff's interests on the basis of a claim for breach of confidence and, in doing so, recognised for the first time in Australia that equitable compensation following a breach of

[125] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [2001] HCA 63.
[126] [2020] HCA 14; (2020) 94 ALJR 50, [86]–[87] (Kiefel CJ, Bell J, Keane J); [244] (Edelman J).
[127] *Giller v Procopets* [2008] VSCA 236; (2008) 24 VR 1.
[128] Ibid, [167]–[168] (Ashley JA) and [447]–[452] (Neave JA, Maxwell P agreeing). The claim for emotional distress was denied by majority (Ashley JA and Neave JA, Maxwell P dissenting) because the plaintiff's emotional distress did not reach the threshold of a recognised psychiatric injury.

personal confidence can include an award to compensate for non-pecuniary harm, in particular injury to feelings.[129]

Other causes of action leave gaps

173. Despite this extension of the remedial options, breach of confidence remains only partially suited to the task of responding adequately to privacy invasions. There are difficulties and uncertainties with the scope of the cause of action, the defences and the remedies, all of which could be avoided if a specific privacy tort was recognised or enacted.

174. The essential elements of the equitable cause of action are that the information in question is of a confidential nature, that it was communicated or obtained in circumstances importing an obligation of confidence, and that there was an unauthorised use of the information.[130] One well-known difficulty with the cause of action is that it remains unclear whether an obligation of confidence can arise simply from the *character* of the information, rather than from the *circumstances in which* that information was *obtained*. The equitable obligation arises most clearly when the defendant was entrusted with the information, for example, as the plaintiff's lawyer, physician or spouse. There is also long-standing authority that equitable relief for breach of confidence is also available where a defendant obtained confidential information surreptitiously or improperly – and is therefore bound in conscience not to divulge it.[131] Under the potentially broader formulation of Lord Goff in *Attorney-General v Guardian Newspapers Ltd (No 2*), the quality of the information itself – for example, if it is 'obviously confidential' – can be a sufficient for an obligation of confidence to arise, even in the absence of some confidential relationship between the parties.[132] These expansions of the cause of action, which would be beneficial for the protection of privacy, appear to have been accepted by the Gleeson CJ in *Lenah Game Meats*.[133] Despite the relative dearth of Australian authority on the issue, it is likely that the approach signalled by Lord Goff may prevail,[134] so that claimants can rely on the action for breach of confidence where their private information is disclosed without consent even in circumstances where no prior relationship between the parties exists and where the conduct cannot be classified

[129] The plaintiff was awarded $50,000 damages (including aggravated damages) for mental distress.
[130] *Moorgate Tobacco Co Ltd v Philip Morris Ltd (No 2)* (1984) 156 CLR 414, 438 (Gibbs CJ, Mason, Wilson, Deane and Dawson JJ).
[131] *Lord Ashburton v Pape* [1913] 2 Ch 469, 475. The cases are discussed in detail by Megan Richardson, Marcia Neave and Michael Rivette, 'Invasion of Privacy and Recovery for Distress' in Jason NE Varuhas and Nicole A Moreham (eds), *Remedies for Breach of Privacy* (Oxford: Hart Publishing, 2018), p 165, 166–173.
[132] [1990] 1 AC 109, 281 identifies 'the broad general principle' that 'a duty of confidence arises when confidential information comes to the knowledge of a person (the confidant) in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others'.
[133] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63; (2001) 208 CLR 199, , Gleeson CJ, [36]; see also Gummow and Hayne JJ, [101]; *Wilson v Ferguson* [2015] WASC 15. See further discussion in *Smethurst v Commissioner of Police* [2020] HCA 14; [2020] 94 ALJR 502.
[134] Lord Goff's 'broad principle' (see above n 131) was cited with approval in *Streetscape Projects (Australia) Pty Ltd v City of Sydney* [2013] NSWCA 2; (2013) 85 NSWLR 196, [155] (Barrett JA, Meagher and Ward JJA agreeing).

as ‘surreptitious or improper’ obtaining. However, a statutory tort would mean that the law of confidence no longer needs put to service where the plaintiff complains about a breach of privacy, rather than of confidentiality. A statutory tort would also be likely to enhance the position of plaintiffs in circumstances where the private information has already been published to some extent or by some media. While courts are reluctant to grant injunctive relief for breach of an equitable obligation of confidence after the information has reached the public domain, courts more readily accept in privacy matters that an injunction to prevent further misuse of personal information can still serve a useful purpose even after the information has already reached the public.[135]

175. Even more importantly, while breach of confidence can deal with many instances of unauthorised disclosure of personal information, it is not designed to protect against mere intrusion into the personal sphere, when that invasion is not accompanied by the misuse of personal information. The besetting, surveillance and stalking of persons or the publication of intimate images without consent may in some cases lead to liability under other torts, such as trespass to land or nuisance,[136] or constitute a criminal offence under surveillance legislation[137] or so-called ‘upskirting’ laws in some jurisdictions,[138] but the protection offered by these mechanisms remains ad hoc and is likely to leave some gaps.[139]

176. There also remains uncertainty about the available defences and the availability of compensation for mental distress. For example, there is uncertainty as to whether Australian law recognises a public interest defence that is separate from the traditional iniquity defence, and in what circumstances these defences apply.[140] In *Giller*, it was held that compensation for emotional distress caused by the breach of personal confidence was available both in the exercise of the Court’s inherent jurisdiction to award equitable compensation and, by majority,[141] that it was available

[135] In *PJS v News Group Newspapers Ltd* [2016] UKSC 26; [2016] AC 1081, Lord Mance (with whom Lord Neuberger, Lady Hale and Lord Reed agreed) canvassed the differences in this regard between breach of confidence and the UK tort of misuse of private information ([25]–[34]), highlighting the importance of considering for the latter tort any additional intrusiveness and distress felt by the claimant in the exercise of the discretion to grant or lift an injunction ([35]). Lord Neuberger (with whom Lady Hale, Lord Mance and Lord Reed agreed) held that the widespread publication of the private information in that case in overseas media may have destroyed a claim for an injunction based on confidentiality, but that it did not substantially weaken a claim based on intrusion: [65]. For an Australian discussion, see *Australian Football League v Age Company* Ltd [2006] VSC 308. More generally on futility arguments, see Normann Witzleb, ‘“Equity Does Not Act in Vain”: An Analysis of Futility Arguments in Claims for Injunctions’ (2010) 32 *Sydney Law Review* 503.

[136] But the privacy invasion resulting from the mere overlooking of neighbouring land is not actionable in nuisance: *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479; recently considered and followed in *Fearn v The Board of Trustees of the Tate Gallery* [2020] EWCA Civ 104; [2020] 2 WLR 1081.

[137] *Listening Devices Act 1992* (ACT); *Surveillance Devices Act 2004* (Cth), *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act 2007* (NT); *Invasion of Privacy Act 1971* (Qld); *Surveillance Devices Act 2016* (SA), *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1998; Surveillance Devices Act 1998* (WA).

[138] For example, *Summary Offences Act 1953* (SA), ss 26A–26E; *Summary Offences Act 1966* (Vic), ss 40–41DB.

[139] Australian Law Reform Commission, above n 109, ch 3.

[140] See discussion in *Australian Football League v Age Company* Ltd [2006] VSC 308.

[141] Neave JA, with whom Maxwell JA agreed; Ashley JA dissenting.

under the Victorian version[142] of Lord Cairns' Act.[143] While this decision provided suitable relief to the plaintiff,[144] some commentators continue to doubt that this remedy should be available.[145] The ALRC concluded that the law remains uncertain and recommended, if its primary recommendation for a statutory privacy tort was not accepted, legislation to clarify the courts' powers to award compensation for emotional distress where private information was disclosed in breach of confidence.[146]

The courts are reluctant to recognise a common law right to privacy

177. Without legislative intervention, it is likely that Australian courts would continue to be reluctant to recognise a right to privacy. Australia is now virtually unique among major common law jurisdictions in not recognising a legally enforceable right to privacy. In the majority of comparable jurisdictions, privacy protections have been developed through the common law. However, in these jurisdictions, courts have taken a much more active role in the recognition of privacy wrongs partly because they were prompted to do so by considering human rights guarantees a right to respect for private life alongside other fundamental freedoms, including the right to freedom of expression. In Australia, however, the absence of a federal human rights instrument has stultified the development of a common law right to privacy.

Option 4: States consider legislating that damages for emotional distress are available in equitable breach of confidence

178. We submit that this option is **likewise not satisfactory as a stand-alone option**.

179. As explained above, there is indeed some uncertainty whether damages for emotional distress are available in equitable breach of confidence.

180. However, inviting states and territories to consider legislation that clarifies the law is not a substitute for federal action. First, states and territories may or may not respond to such an invitation, which raises the possibility of conflicting laws within Australia.

181. Second, breach of confidence is – for the reasons identified above – not a suitable substitute for comprehensive privacy protection through a dedicated privacy tort.

---

[142] *Supreme Court Act 1986* (Vic) s 38.
[143] *Chancery Amendment Act 1858*, 21 & 22 Vict, c 27.
[144] Without reliance on Lord Cairns' Act, Mitchell J held in *Wilson v Ferguson* [2015] WASC 15, [82]–[83] that compensation for non-economic loss was available for breach of an equitable obligation of confidence.
[145] John D Heydon, Mark J Leeming and Peter G Turner, *Meagher, Gummow and Lehane's Equity: Doctrines and Remedies*, 5th ed (Chatsworth: LexisNexis Australia, 2015), [24-080], [24-085]; based on an analysis of the legislative history, the reasoning on Lord Cairns' damages in *Giller* is also doubted by Katy Barnett and Michael Bryan, 'Lord Cairns's Act: A case study in the unintended consequences of legislation' (2015) 9 *Journal of Equity* 150, 165. However, the prevailing view in Australia is that equitable compensation can and should provide redress of non-pecuniary harm: see Richardson, Neave and Rivette, above n 131, 165, 166–173 for further discussion.
[146] Australian Law Reform Commission, above n 109, rec. 13-1.

182. This notwithstanding, there would be benefit to states and territories legislating on that issue *alongside* federal legislation introducing a privacy tort.

The fault standard of an Australian privacy tort

183. As discussed above we **strongly favour Option 1**. However, it would be our preference that the statutory tort of privacy **should not be confined to intentional or reckless invasions of privacy.** In our view, limiting liability to intent and recklessness, as the ALRC recommended in Report 123, would set the bar too high.

184. We submit that **negligent invasions of privacy should also be actionable.** In this context, we **note** that the recommendations of the NSW Law Reform Commission and the Victorian Law Reform Commission in favour of a statutory privacy tort did not include the adoption of a fault standard. The NSW Law Reform Commission and the Victorian Law Reform Commission suggested instead that the court would be required to take the degree of fault into account in the overall assessment of whether there was an actionable invasion of privacy.[147] The Victorian Law Reform Commission considered it 'it is unnecessary to expressly exclude negligent acts from the conduct which might fall within the two statutory causes of action. Although it is highly likely that most serious invasions of privacy will involve
intentional conduct, there may be circumstances in which a person's actions were so grossly negligent that civil action ought to be possible'.[148]

185. We **support** these views favouring a more expansive tort, which were formed on the basis of detailed law reform inquiries that included extensive community consultation that 'generally favoured extending liability beyond intentional conduct'.[149] We submit that the limitation to intentional and reckless privacy invasions would leave plaintiffs without redress in some circumstances where they deserve protection. It would create problems of coherence with Privacy Law as well as with wrongs protecting dignitary interests. Finally, we submit that the ALRC did not sufficiently clarify how intention or recklessness would be determined in a particular case.

Bar Too High

186. The case of *Jane Doe v ABC*[150] provides a striking example of why limiting liability to intentional and reckless acts would exclude some deserving cases. In that case, the

[147] New South Wales Law Reform Commission, above n 108; Victorian Law Reform Commission, above n 108.
[148] Victorian Law Reform Commission, ibid, [7.148].
[149] New South Wales Law Reform Commission, above n 108, [5.56].
[150] *Jane Doe v ABC* [2007] VCC 281. Hampel J found nonetheless in favour of the plaintiff because her Honour formulated the cause of action as an 'unjustified, rather than wilful' (at [163]) publication of private facts.

Australian Broadcasting Corporation reported in three radio news broadcasts that the plaintiff's husband had been convicted of raping her. In two of these broadcasts, her estranged husband was identified by name and the offences were described as rapes within marriage. In another broadcast, Jane Doe was additionally identified by name. In all three broadcasts, the journalist and sub-editor breached the *Judicial Proceedings Act 1958* (Vic), which makes it an offence to publish information identifying the victim of a sexual offence. Expert evidence established that the plaintiff was particularly vulnerable at the time of the broadcasts and that the reporting exacerbated her trauma symptoms and delayed her recovery. The defendants were thus guilty of a serious invasion of privacy with grave and long-lasting consequences for the plaintiff. Yet the trial judge, Hampel J, found that the breach of the plaintiff's privacy was the result of the defendants' failure to exercise reasonable care 'rather than [being] wilful'.[151] If the ALRC recommendations were enacted, a person in the position of the plaintiff in *Jane Doe v ABC* would presumably not be able to rely on the statutory cause of action. This would severely curtail the protection for privacy that the law should provide for.

187. Other examples where negligent invasions of privacy can cause significant harm are data breaches. A data breach occurs, according to the definition used by the OAIC,[152] when personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. In the latest Notifiable Data Breaches Report for January-June 2020, the OAIC noted that human error data breaches accounted for 34% of notifications.[153] While data breaches may often also be actionable under the direct right of action under the *Privacy Act*, should it be introduced, there may be circumstances where negligent handling of personal information is not actionable under the *Privacy Act*.

188. As acknowledged by the ALRC Report 123, the *Privacy Act* is subject to a range of broad exemptions, in particular the small business exemption. As a result, the Privacy Commissioner does not generally have jurisdiction over breaches of the *Privacy Act* committed by private sector organisations with an annual turnover of $3 million or less or that fall within one of the exemption, such as those granted to the media, political parties, individuals or in relation to employee records. Although these exemptions are currently under review, they demonstrate that existing remedies leave some real gaps in the protection against negligent data breaches. These should be addressed through a combination of a direct right of action, coupled with the removal of exemptions, and a cause of action against serious invasions of privacy which is based on *fault-based* standard, rather than requiring intention or recklessness.[154]

---

[151] Ibid, [163].

[152] Office of the Australian Information Commissioner, *Data breach notification guide: A guide to handling personal information security breaches* (August 2014) p 2.

[153] Office of the Australian Information Commissioner, Notifiable Data Breaches Report: January–June 2020 <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2020/>.

[154] For an example where a UK government agency committed a negligent data breach and was held liable to pay damages both under the torts of misuse of private information and the *Data Protection Act*

Coherence with Privacy Law

189. A privacy tort is intended to protect the legally recognised interest in privacy, and emotional harm is the typical consequence of an invasion of privacy. It would be incoherent with common law policy to allow recovery for negligently caused emotional distress in trespass and defamation, but not to allow such recovery following a privacy invasion. There is no dignitary wrong in the common law which requires intention or recklessness for recovery of emotional harm.

190. In further support of this argument, the *Australian Privacy Principles* (APPs), which form the basis of regulatory action by the Australian Privacy Commissioner under the *Privacy Act* likewise impose objective obligations that are akin to a negligence standard, such as that conduct must be 'reasonable',[155] 'reasonably necessary',[156] or based on a 'reasonable belief'.[157] There is no sufficient justification to set a much higher bar of intention or recklessness in the context of a private law action. Such subjective fault elements are more appropriate in the context of criminal law rather than private law liability.

191. ALRC Report 123 reasons that '[if] the new tort extended to negligent invasions of privacy, [this might expose] a wide range of people to face liability for invading privacy by common human errors'.[158] However, negligence liability does not lead to liability simply for a human error. Liability arises only for those errors that are the result of a failure to take precautions against a risk of harm that a reasonable person would have taken in the circumstances.[159] Liability for a failure to take reasonable care is pervasive in the law of torts and an expression of the community expectation that everyone should generally conduct their affairs with due regard for the rights and interests of others. Privacy is a core value in Western societies[160] and based on fundamental human interests such as respect for dignity and autonomy.[161] This suggests that privacy should enjoy the same measure of protection as other fundamental interests, such as the property and physical integrity, which are also protected against negligent invasion.

192. The concern that this might extend liability too wide can be countered with the specific restrictions built into the privacy tort. Unlike most other interests protected by torts law, privacy invasions are only actionable if it is found that the defendant's and public interests do not outweigh the privacy interest of the plaintiff. This provides a sufficient protection to defendants against undue encroachment of their rights and

---

1998 (UK), s 13: *Secretary of State for the Home Department v TLU* [2018] 4 WLR 101, [2018] EWCA Civ 2217.

[155] Eg., APP 1, APP 4, APP 5, APP 8, APP 10, APP 11.

[156] Eg., APP 3, APP 6, APP 8, APP 9.

[157] Eg., APP 3, APP 6, APP 8, APP 12.

[158] Australian Law Reform Commission, above n 109, [7.63].

[159] See, e.g., *Civil Liability Act 2002* (NSW), s 5B.

[160] See, eg. Article 17 of the International Covenant on Civil and Political Rights.

[161] *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63; (2001) 208 CLR 199.

liberties. It would be extending these protections too far if negligent invasions of privacy were excluded from the ambit of a privacy tort.

Coherence with Other Wrongs Protecting Dignity

193. ALRC Report 123 points out that 'if actual damage is suffered beyond 'mere' emotional distress, it may well be the case that the plaintiff would have a tort action in negligence'.[162] However, it is doubtful whether a privacy invasion would remain actionable under the tort of negligence if a statutory privacy tort were enacted.

194. In *Sullivan v Moody*,[163] the High Court denied to apply the law of negligence to a case where the 'core of the complaint' was that the plaintiff was 'injured as a result of what he, and others, were told'.[164] It considered that 'the law of defamation … resolves the competing interests of the parties through well-developed principles about privilege and the like. To apply the law of negligence in the present case would resolve that competition on an altogether different basis'.[165] It is likely that the High Court would express similar concerns about legal coherence in the intersection between a statutory privacy tort and negligence law. The proposed privacy tort likewise resolves the conflicting interests of plaintiff and defendant on a basis that is altogether different than the tort of negligence. If conduct did not satisfy the elements of the statutory privacy tort (for example, because it would not be intentional or reckless), it would be unlikely that a plaintiff were allowed to proceed on the basis of negligence. Similar to *Sullivan v Moody*, this would be likely to be seen as an attempt to circumvent the requirements of the statutory tort, which provides its own set of guiding principles, elements, defences and remedies.

Lack of Clarity

195. It is also not sufficiently clear how a standard of intention or recklessness, such as the standard recommended by the ALRC in Report 123, would operate in practice, in particular what elements of the cause of action this standard would relate to.

196. The ALRC Report states in this regard:

> *The ALRC considers that the new tort should only be actionable where the defendant* ***intended to invade*** *the plaintiff's privacy in one of the ways set out in the legislation or was reckless as to that invasion. It should not be actionable where there is merely an intention to do an act that has the consequence of invading a person's privacy*.[166]

---

[162] Australian Law Reform Commission, above n 109, [7.50].

[163] *Sullivan v Moody* [2001] HCA 59; (2001) 207 CLR 562; see also *Tame v New South Wales* [2002] HCA 35; (2002) 211 CLR 317.

[164] *Sullivan v Moody* [2001] HCA 59; (2001) 207 CLR 562, at [54].

[165] Ibid.

[166] Australian Law Reform Commission, above n 109, [7.31].

It explains further that:

> *The requirement does not mean that the defendant needs to intend to commit a legal wrong, or that he or she intends to fulfil the other ingredients for liability (seriousness, lack of public interest justification or defence). This would be too stringent a hurdle for the plaintiff to overcome. It does mean that the defendant needs to have been aware of the facts from which it can be objectively assessed whether or not the plaintiff had a reasonable expectation of privacy and of the facts that an intrusion or disclosure would (or in the case of recklessness, may) occur.*[167]

197. An initial problem with requiring an intention (or recklessness) to intrude upon the plaintiff's seclusion or to misuse the plaintiff's private information is that both terms, 'intrude' and 'misuse', are evaluative and connote wrongfulness. This raises the question of how defendants who felt justified in publishing the plaintiff's private information – because they positively believed to be doing so in the public interest or otherwise under a defence – can be said to have intended an 'intrusion' or 'misuse' or have been reckless in this regard.

198. As the UK case law demonstrates, defendants will frequently argue that they believed that the plaintiff did not have a reasonable expectation of privacy in relation to the information in question,[168] or that publication was justified in light of overriding interests,[169] or – in many cases – both.[170] Proof of awareness of a risk that a privacy invasion may occur (the recklessness standard) could be understood as requiring the plaintiff to disprove that the defendant held a belief in the conduct's lawfulness or that that belief was reasonable. This would be very onerous to demonstrate, because the assessments of whether there was a reasonable expectation of privacy or whether there were overriding public interests in favour of publication are highly fact-specific. It is easy to come to differing assessments in relation to these issues, as the numerous cases in the UK attest to in which courts were divided[171] or in which first instance decisions were reversed on appeal[172].

199. We submit that, if a fault standard of intention or recklessness is introduced, further consideration needs to be given to how intention or recklessness can be established.

Our Recommendations

200. In summary, we submit that setting the bar at intentional and reckless conduct would not provide sufficient protection against privacy invasion. It is necessary to provide

[167] Ibid, [7.35] (citations omitted).
[168] *Murray v Express Newspapers plc* [2008] EWCA Civ 446; [2009] Ch 481.
[169] *AAA v Associated Newspapers Ltd* [2012] EWHC 2103 (QB), [2013] EMLR 2.
[170] *Campbell v MGN Ltd* [2004] 2 AC 457; *McKennitt v Ash* [2006] EWCA Civ 1714; [2008] QB 73; *ETK v News Group Newspapers Ltd* [2011] EWCA Civ 439; [2011] 1 WLR 1827.
[171] *Campbell v MGN Ltd* [2004] UKHL 22; [2004] 2 AC 457.
[172] *Murray v Express Newspapers plc* [2008] EWCA Civ 446; [2009] Ch 481; *ETK v News Group Newspapers Ltd* [2011] EWCA Civ 439; [2011] 1 WLR 1827.

plaintiffs protection also in cases where a negligent invasion of privacy causes serious harm for the plaintiff.

201. The adoption of a fault standard that includes negligence would also better align the statutory cause of action to protect privacy with other wrongs that protect dignitary interests and with the Australian Privacy Principles under the Privacy Act. The interests of defendants are sufficiently protected by other elements of the cause of action, in particular the requirement for balancing privacy with competing interests and the defences.

202. A negligence standard would be closer to the recommendations by the NSW and Victorian Law Reform Commissions under which the court would be required to take the degree of fault into account in the overall assessment of whether there was an actionable invasion of privacy.[173] Such an approach allows actions to be brought where a negligent invasion of privacy has serious consequences and gives the court the flexibility to deny relief where the defendant's invasion of the plaintiff's privacy was merely the result of inadvertence and did not cause particularly harmful consequences.

203. If the limitation to intentional and reckless conduct was retained, its operation would need to be clarified. We submit that it would need to be made clear which elements of the cause of action the defendant needs to have intended or been reckless about. There is some difficulty with requiring the plaintiff to establish that the defendant had the requisite state of mind in relation to the 'reasonable expectation of privacy'. If this was not required, it needs to be made clearer what amounts to an invasion of privacy, in particular if this is a 'conduct' or a 'consequence'. If the latter, it would need to be made clear whether 'intrusion' or 'misuse' requires an understanding of the wrongfulness of the conduct.

[173] New South Wales Law Reform Commission, above n 108; Victorian Law Reform Commission, above n 108.