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

Submission to Issues Paper

Prepared by
Assoc. Prof. Normann Witzleb and Prof. Moira Paterson
(with assistance from Andrea Olivares Jones)

On behalf of the Castan Centre for Human Rights Law
Faculty of Law, Monash University

29 November 2020

PART ONE: BACKGROUND

1.1 Introduction

1. The 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 Castan Centre welcomes the Attorney-General's Department *Review of the Privacy Act 1988* and is pleased to contribute to this investigation by way of this submission.

3. We seek to address the following terms of reference:
    a) *The scope and application of the Privacy Act including in relation to:*
        i) *the definition of 'personal information';*
        ii) *current exemptions; and*
        iii) *general permitted situations for the collection, use and disclosure of personal Information.* ***[See Part THREE]***
    b) *Whether the Privacy Act effectively protects personal information and provides a practical and proportionate framework for promoting good privacy practices including in relation to:*
    c) *notification requirements*
    d) *consent requirements including default privacy settings* ***[See Part FOUR]***
    e) *overseas data flows, and*
    f) *erasure of personal information.*
    g) *Whether individuals should have direct rights of action to enforce privacy obligations under the Privacy Act.* ***[See Part FIVE]***
    h) *Whether a statutory tort for serious invasions of privacy should be introduced into Australian law.* ***[See Part SIX]***

1.2 Materials used in this Submission

4) This submission will make use of the following material previously published by the authors, which are also made available as part of this submission:

- 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, & Janice Richardson (eds), *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-targeting* (Abingdon UK, Routledge 2020)164-185

- 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) 377-408

- Normann Witzleb and Julian Wagner, 'When is personal data "about" or "relating to" an individual? A comparison of Australian, Canadian, and EU data protection and privacy laws' (2018) 4(1) *Canadian Journal of Comparative and Contemporary Law 293-329*

- Normann Witzleb, 'Another Push for an Australian Privacy Tort – Context, Evaluation and Prospects' (2020) 94 *Australian Law Journal* 765-782, pre-publication version at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3705881

- 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* (CUP, forthcoming 2021), pre-publication version at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717561

PART TWO: EXECUTIVE SUMMARY OF OUR RCOMMENDATIONS

Question 1: Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?

3.1 Objectives of the Privacy Act

1. We submit that there is a strong argument that s 2A should be reworded to signal more clearly that the main objective of the *Privacy Act* is the promotion and protection of privacy as a human right. We also argue that the structure of the objects clause in the *Freedom of Information Act 1982* (Cth) provides a good model on how to provide better guidance for the interpretation of the *Privacy Act*, in particular the *Australian Privacy Principles*.

2. We submit that s 2A should be redrafted along the following lines:

    (a) The objects of the Act are
        (i) to promote the protection of the privacy of individuals; and
        (ii) to promote responsible and transparent handling of personal information by entities; and
        (iii) to promote the responsible and transparent handling of personal credit information; and
        (iv) to provide a means for individuals to complain about an alleged interference with their privacy.

    (b) The Parliament intends, by these objects,
        (i) to provide the basis for nationally consistent regulation of privacy and the handling of personal information; and
        (ii) to facilitate the free flow of information across national borders consistently with protection of the privacy of individuals; and
        (iii) to implement Australia's international obligation in relation to privacy.

    (c) The Parliament also intends that functions and powers given by this Act are to be performed and exercised, as far as possible, to promote the human right to privacy protection while recognising that other rights and interests may also need to be taken into account.

3.2 Definition of personal information

Question 2: What approaches should be considered to ensure the Act protects an appropriate range of technical information?

3. We submit that, in modernising the definition, close consideration should be given to the definition of 'personal data' in art 4(1) of the EU General Data Protection Regulation ('GDPR').[1] The definition in the *Privacy Act* could be rephrased as:

> *"personal information" means information or an opinion:*
> *(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,*
> ***relating to** an identified individual, or an individual who is reasonably identifiable or **capable of being singled out, directly or indirectly,** in particular **by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to identity of that individual's identity.***

Question 3: Should the definition of personal information be updated to expressly include inferred personal information?

4. We submit that the definition of personal information should make clear that such inferred information is 'personal information'. The revised definition recommended above would achieve this by inclusion of the words 'directly or indirectly' and 'by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to identity of that individual's identity'.

Question 4: Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

5. We recommend that the Act be amended to apply in part to information which is currently non-identifiable but might potentially lead to the identification of individuals if it is considered together with information that might otherwise be available about the information subject. The key principles which should be applicable in those circumstances are the disclosure limitation principle in APP 6 and the security principle in APP 11.

Question 5: Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?

6. We refer to the practice of mining of personal data for attributes that can serve as proxies for the attributes listed in the definition of sensitive information. To clarify that

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, 4.5.2016, 1.

such practices can We submit that the opening words of the definition of 'sensitive information' should be clarified to read as follows:[2]

> *information or an opinion about,* ***or information or opinion that is collected for use as, or used or disclosed as a proxy for,*** *an individual's:* (etc.)

3.3 Employee records exemption

Question 13: Is the personal information of employees adequately protected by the current scope of the employee records exemption

7. We recommend that the exemption should be abolished. It is at odds both Australian community attitudes and with the legal position in comparable jurisdictions.

Question 14: If enhanced protections are required, how should concerns about employees' ability to freely consent to employers' collection of their personal information be addressed?

8. We recommend that enhanced protections are needed where the freedom of an employee to consent may be compromised by actual or perceived economic pressures. Therefore, the Act should limit the ability for entities to collect and process information on the basis of consent in situations where there is an imbalance in the relationship between the entity and the information subject.

Question 15: Should some but not all of the APPs apply to employee records, or certain types of employee records?

9. If it is decided that some additional exclusion is required for employment data, we submit that it would be preferable to include exceptions in respect of APPs 5, 6 and 12 that are narrowly targeted to the specific HR needs of employers.

3.4 Political Parties Exemption

Question 16: Should political acts and practices continue to be exempted from the operation of some or all of the APPs?

10. We submit that the widespread concerns about personalised political communications need to be taken seriously. In our view, the ALRC recommendations to remove the political exemptions to the Privacy Act should be endorsed and implemented. 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.

[2] See *Privacy Act 1988* (Cth) s 6.

11. We argue that removing special exemptions for political parties and political messaging would serve to enhance the privacy of voters without inappropriately undermining the important values inherent in the doctrine of freedom of political communication.

12. Our analysis of the implied freedom of political communication suggests that implementing the ALRC's recommendations would not conflict with the implied freedom of political communication in the Australian Constitution.

4.1 Obtaining consent from Children

Question 33: Should specific requirements be introduced in relation to how entities seek consent from children?

13. We submit that there is a good case for amending the Privacy Act to better protect the personal data of children in the online commercial context.

14. Insights from the US and EU examples make clear that data controllers need to be mindful of children's special vulnerabilities and design their data handling practices accordingly. The ACCC's recommendations either embody, or provide scope for embodying, all of these features other than a right to request deletion of data.

15. The recommendations for immediate amendments to the Privacy Act address the issue of child-friendly notices and also that of younger children lacking the ability to give informed consent. However, insofar as the latter is concerned, the appropriate age limits should be set at after appropriate consultations with children, parents and experts in development studies.

16. The further recommendations for a Code in Recommendation 18 would provide scope for inclusion of key features of the UK's age-appropriate design code, thereby addressing children's desire for increased transparency, accessibility and flexibility in their dealings with online service providers.

17. In addition, we recommend the inclusion in the APPs of a specific right of deletion of data volunteered to an online collector. This would serve as a useful backstop given that the deletion of data goes a long way to resolving the privacy issues associated with its collection.

5.1 Enforcement powers under the Privacy Act and role of the OAIC

Question 53: Is the current enforcement framework for interferences with privacy working effectively?

18. In its 2014 Report on serious invasions of privacy in the digital era, the ALRC recommended that consideration be given to making the complaints process available for alleged breaches of the proposed statutory privacy tort.

19. We submit that this recommendation be implemented.

5.2 Direct Right of Action

Question 56: How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

20. In the Final Report of the Digital Platform Inquiry, the Australian Competition and Consumer Commission ('ACCC') recommends the introduction of a direct right to bring actions and class actions under the Privacy Act.3

21. We submit that this recommendation, which the government supports in principle, should be enacted.

22. We submit that access to the direct act of action should not be curtailed by threshold mechanisms. In our view, there is also no need to put a cap on the amount of damages available.

6.1 Statutory Tort

Question 57: Is a statutory tort for invasion of privacy needed?

23. We submit that, despite the existing protections of privacy at general and statute law, there is an unmet need for a privacy tort. We support the ALRC's proposals for a statutory cause of action, as well as similar calls for law reform made by the ACCC and AHRC.

24. While we broadly favour the enactment of the tort as proposed by the ALRC, we recommend that the tort to intentional and reckless invasions of privacy also extend to include fault-based invasions of privacy. [See below at [29]]

25. We further submit that the general tort of serious invasion of privacy should be complemented by a direct right of action under the Privacy Act [See above]. This would give individuals greater protection and control if their statutory information privacy rights are interfered with.

[3] Australian Competition and Consumer Commission, *Digital Platforms Inquiry*, Final Report (2019), Recommendation 16(e).

Question 58: Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?

26. We submit that the existence of criminal law offences for some serious invasions of privacy resulting from image-based abuse, voyeurism and 'upskirting' does not obviate the need for a statutory privacy tort.

Question 59: What types of invasions of privacy should be covered by a statutory tort?

27. We submit that the ALRC recommendations for a statutory privacy tort serves as a useful starting point for the scope of a statutory tort. We submit that a broad formulation of the cause of action provides redress against all presently recognised forms of privacy infringement.

28. For the sake of clarity, however, we submit that it would be useful to state expressly that 'false light' and 'appropriation' claims are not excluded from the ambit of the new tort. These wrongs should be actionable if the defendant's conduct satisfies the elements of the cause of action. The legislation should clarify that 'private information' includes untrue information if the information would be private if it were true. It should further clarify that an 'appropriation of the plaintiff's name, likeness and other characteristics' may constitute a 'misuse' of personal information.

Question 60: Should a statutory tort of privacy apply only to intentional, reckless invasions of privacy or should it also apply to breaches of privacy as a result of negligence or gross negligence?

29. We submit that the statutory tort of privacy should not be confined to intentional or reckless invasions of privacy, and that negligent invasions of privacy should also be actionable.

PART THREE: SCOPE AND APPLICATION OF THE PRIVACY ACT

3.1 Objectives of the Privacy Act

Question 1: Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?

1. The objects clause of the *Privacy Act 1988* (Cth) ('Privacy Act') is significant because it guides the interpretation of the Act. There are at least two problematic aspects of the current version. The first is that the object stated in s 2A(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', does not signal how this balancing is to occur. In particular, it does not indicate the weight that it is to be attributed to each of these conflicting objectives. Section 2A(b) appears to undercut what should be the key object of the Act, which is stated in 2(a) as to 'promote the privacy of individuals'.[4] The second is that the objects clause has particular significance in a principles-based regulatory regime. A problematic feature of the Australian Privacy Principles ('APPs') is the sufficiency of necessity based on an entity's function or activities as a ground for collection of personal information and consistency with that purpose as a ground for its use and disclosure. The latter is further discussed below in relation to questions about APPs 3 and 6.

2. Insofar as the first problematic aspect is concerned, the objects section should arguably give greater emphasis to privacy protection given the acknowledged status of data protection as a *human right*. Many other legal systems, including Canada, New Zealand and the United Kingdom, give human rights explicit protection through domestic human rights legislation. In Australia, such protection only exists at state and territory level in Victoria, the ACT and now Queensland. Australia, like most countries, is a signatory of the International Covenant on Civil and Political Rights (ICCPR), which in its art. 17 imposes on state parties an obligation to protect everyone against arbitrary or unlawful interference with their privacy, family, home or correspondence. This international obligation is recognised in Art. 2A(h) of the *Privacy Act*. However, given that the ICCPR does not form part of domestic Australian law, it would be helpful for the interpretation of the *Privacy Act* if the human rights status of privacy was recognised more explicitly in the Act. It is an interest that should, in many cases, rank more highly than the 'interest of entities in carrying out their activities and functions', at least where those interests do not themselves enjoy human rights protections. The bare juxtaposition of individual privacy and an entity's interest in carrying out its activities and functions may have made more sense in an era where the processing of information was understood as being separate from, and a fetter on, the underlying business model of commercial entities. However, there is now increasing recognition that privacy protection is, or should be, an integral part of many modern business

[4] *Privacy Act 1988* (Cth) s 2A.

operations, because it drives innovation and adoption of modern applications, rather than impedes it.[5]

3. In these circumstances, there is a strong argument that s 2A(b) should be reworded to signal more clearly that the main objective of the *Privacy Act* is the promotion and protection of privacy as a human right. For example, section 3 of the *Privacy Act 2020* (New Zealand) expresses the purpose of that Act as follows:

> The purpose of this Act is to promote and protect individual privacy by —
> (a) providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognising that other rights and interests may at times also need to be taken into account; and
> (b) giving effect to internationally recognised privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines and the International Covenant on Civil and Political Rights.

A further reason why the objects clause in the *Privacy Act* should be drafted with particular care is that the principles in the APPs are expressed at a high level of generality. This makes it important that their interpretation is appropriately guided. Arguably the objects clause in the *Freedom of Information Act 1982* (Cth) provides a good model on how to provide better guidance. In essence, this contains a short and unqualified statement of the objects of the Act. This is then followed by an explanation of what the Parliament is trying to achieve via those objects and a statement about how the functions and powers of the Act are to be exercised.

4. Using this approach, we accordingly recommend that s 2A should be redrafted along the following lines:

> (a) The objects of the Act are
> (i) to promote the protection of the privacy of individuals; and
> (ii) to promote responsible and transparent handling of personal information by entities; and
> (iii) to promote the responsible and transparent handling of personal credit information; and
> (iv) to provide a means for individuals to complain about an alleged interference with their privacy.
>
> (b) The Parliament intends, by these objects,
> (i) to provide the basis for nationally consistent regulation of privacy and the handling of personal information; and
> (ii) to facilitate the free flow of information across national borders consistently with protection of the privacy of individuals; and

[5] Marc van Lieshout, 'Privacy and Innovation: From Disruption to Opportunities', in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer (2016), 195.

(iii) to implement Australia's international obligation in relation to privacy.

(c) The Parliament also intends that functions and powers given by this Act are to be performed and exercised, as far as possible, to promote the human right to privacy protection while recognising that other rights and interests may also need to be taken into account.

3.2 Definition of 'Personal Information'

Question 2: What approaches should be considered to ensure the Act protects an appropriate range of technical information?

Technical data as 'personal information' in Australia

5. In Telstra Corporation Ltd v Privacy Commissioner, the Administrative Appeals Tribunal ('AAT') ruled that 'an IP address is not information about an individual'.[6] The AAT expressed the view that where IP addresses change regularly over the life of the respective device, they only identify the respective device itself. In its view therefore they are not information 'about' the user of the device, because any connection between the IP address and the user would be 'ephemeral'.[7] As the AAT put it, such IP addresses are 'not about the person but about the means by which data is transmitted from a person's mobile device over the internet', and, therefore, they are not considered to be personal information under Australia's privacy regime.[8]

6. While the Full Court of the Federal Court of Australia upheld the decision of the AAT,[9] the appeal was limited to the interpretation of the definition of 'personal information', and did not extend to its application. It held that the words 'about an individual' had meaning and required consideration before the subsequent issue arose of whether this information identified that individual. The Federal Court declined to consider whether the AAT applied its definition correctly because this was not raised in the appeal. The Office of the Information Commissioner decided not to challenge the Full Court's decision. its updated guidance on the meaning of 'personal information'[10] does not cover the issue of IP addresses.

7. However, a subsequent decision of the AAT specifically adopts the reasoning of the AAT in Telstra. In *Freelancer International Pty Ltd and Australian Information Commissioner*,11 Freelancer operated a website that required user registration and a login by registered users. Freelancer recorded the login IP addresses and associated these IP addresses with particular registrant accounts, including by displaying the IP

[6] *Telstra Corporation Ltd v Privacy Commissioner* [2015] AATA 991, Forgie DP at [113] ('Telstra ATT').
[7] Ibid.
[8] Ibid.
[9] *Privacy Commissioner v Telstra Corporation Limited* (2017) 249 FCR 24; [2017] FCAFC 4.
[10] Office of the Australian Information Commissioner, 'What is personal information?' (May 2017) <https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/ - ftn15>.
[11] *Freelancer International Pty Ltd and Australian Information Commissioner* [2017] AATA 2426.

address used in a session in a Welcome message to the registrant. Nonetheless, the AAT held that, while a user's identity might reasonably be ascertained from the information available to the website operator, the IP address information was 'not "about" an individual. It was information "about" the login itself'.[12] Like the decision of the AAT in Telstra, this decision appears to assume that when information, such as an IP address, is about enabling a communication, it cannot also be about the individual engaged in that communication. This is in contrast to the decision of the Full Court, which did not subscribe to the view that the classification task is binary and stated specifically that information can have more than one subject matter.

8. In summary, while decisions of the AAT, both before and after the decision of the FCAFC in Telstra, suggest that IP addresses of electronic devices do not qualify as 'personal information' and, hence, are not subject to Australian privacy legislation, these decisions are potentially open to challenge. Commentators have called for a broad interpretation of the definition of 'personal information' that promotes the objectives of the Act and is in line with international counterparts.[13]

9. We submit, however, that it would be preferable to put the matter beyond doubt by amending the definition of personal information. We support the recommendation of the ACCC to update and clarify the definition of personal information in relation to technical data, such as IP addresses, that can be used to identify an individual.

Overseas approaches

10. Despite employing similar definitions of 'personal data' or 'personal information' in their respective data protection laws, these terms have been interpreted differently by courts in Australia, Canada and the European Union. Part of these differences may also be due to the fact that the courts in each jurisdiction are hesitant to consider international materials in their decisions.

11. For example, the Canadian definition of personal information resembles the Australian approach. The Canadian *Privacy Act* defines personal information as 'information about an identifiable individual',[14] or, in the equally binding French language version, as 'tout renseignement concernant un individu identifiable'.[15] Nonetheless, its application in practice appears to differ from that adopted in Australia. The Privacy

[12] F*reelancer International Pty Ltd and Australian Information Commissioner* [2017] AATA 2426, Taylor SC at [69].
[13] Joshua Yuvaraj, 'How about me? The scope of personal information under the Australian Privacy Act 1988' (2018) 34(1) Computer and Security Law Review 47; Normann Witzleb and Julian Wagner, 'When is personal data "about" or "relating to" an individual? A comparison of Australian, Canadian, and EU data protection and privacy laws' (2018) 4(1) *Canadian Journal of Comparative and Contemporary Law* 293.
[14] The Canadian *Privacy Act*, s 3 contains further specification for the purposes of this Act, including that the information is 'recorded in any form'. The definition wording, 'information about an identifiable individual that is recorded in any form" is also contained in the *Model Code for the Protection of Personal Information, National Standard of Canada* CAN/CSA-Q830-96 at 1.
[15] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, s 2(1) [*LPRDE*].

Commissioner of Canada has stated that IP addresses not only constitute the technical base for electronic communication but *also provide a potential starting point to unlock additional information about the individual* who used the electronic device which identified itself via the IP address in question. The Canadian Commissioner has accordingly classified IP addresses as being sufficiently linked to the individual using them and, therefore, qualified them as personal information under Canadian law.[16] A similar view was adopted by the Supreme Court of Canada in *R v Spencer*[17] in which the Court held that internet users may have a reasonable expectation of privacy in respect of their internet activities and that a warrantless police request that an ISP provided identifying information about a subscriber of a particular IP address accordingly amounted to an unlawful search and violated the user's privacy rights.[18]

12. Similarly, the EU General Data Protection Regulation ('GDPR') defines 'personal data' as 'any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly …'.[19] Under European Union data protection law, IP addresses normally fall within the scope of personal data. In 2011, the European Court of Justice ('ECJ') ruled in *Scarlet Extended* in relation to the definition in Article 2(a) of the (former) *Data Protection Directive*[20] that IP addresses may allow the precise identification of the persons using the addresses and, therefore, qualify as personal data.[21] This ruling adopted the opinion delivered by the European Advocate General's opinion that an IP address 'may be classified as personal data inasmuch as it may allow a person to be identified by reference to an identification number or any other information specific to him'.[22] However, the decision in *Scarlet Extended* related to the introduction of a system for filtering electronic communications by the ISPs and, therefore, by entities which not only had access to IP addresses but – being the provider – also to the necessary data to link the IP addresses with specific users of the service. The ECJ later expanded this coverage to IP addresses held by entities other than the ISPs in the *Breyer* case.[23]

---

[16] Office of the Privacy Commissioner of Canada, *Metadata and Privacy: A Technical and Legal Overview*, (October 2014), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/>; Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2001-25 (20 November 2001), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2001/pipeda-2001-025/>. See also Eloïse Gratton, 'Personalization, Analytics, and Sponsored Services: The Challenges of Applying PIPEDA to Online Tracking and Profiling Activities' (2010) 8(2) *Canadian Journal of Law & Technology* 299, 300-05.

[17] *R v Spencer*, 2014 SCC 43.

[18] *Canadian Charter of Rights and Freedoms*, s 8.

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, 4.5.2016, art. 4(1).

[20] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23.11.1995.

[21] *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs* SCRL (SABAM) (European Court of Justice, C70/10, 24 November 2011), ECLI:EU:C:2011:771, at para 51.

[22] EC, *Opinion of Advocate General Cruz Villalón delivered on 14 April 2011*, ECLI:EU:C:2011:255 at paras 74-78.

[23] *Patrick Breyer v Bundesrepublik Deutschland* (European Court of Justice, C-582/14, 19 October 2016), ECLI:EU:C:2016:77.

13. In that case, the ECJ stated that the notion of 'personal data' does not necessarily require that the data on its own allow the data subject to be identified or that the controller of the data must be able to identify the data subject without the help of a third party.[24] Instead, the ECJ ruled that it is sufficient if the data controller in question 'has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority' and other private entities.[25] This criterion is fulfilled if the data controller 'has the *legal means* which enable it to identify the data subject with additional data'[26] held by third parties, as long as this does not require 'a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant'.[27] The ECJ then applied this test to dynamic IP addresses stored by a private website operator and came to the conclusion that such addresses allow the identification of the respective device connecting to the internet under the IP address in question because website operators may gain the necessary additional data from the competent authority or the respective ISP. The ECJ finally concluded that under these circumstances, dynamic IP addresses constitute personal data within the meaning of Article 2(a) of the *Data Protection Directive*.[28]

14. As the above illustrates, the scope of application of the respective data protection legislation does not coincide. This has the potential to create friction between these jurisdictions by forming an obstacle to the free flow of personal data as most countries only allow the export of personal data to third jurisdictions if an adequate level of protection is guaranteed. If one country establishes a narrower term of personal data than other countries, thereby constraining the scope of its data protection legislation, the export of such data into this country can become problematic. The lack of uniformity has been demonstrated by the example of IP addresses, which are treated differently in each of the three jurisdictions.

Our recommendation

15. We submit that, against the background of increasingly global data flows, the time has come to adopt a comparative approach to defining the key terms of data protection laws wherever possible.

16. We submit that, in modernising the definition, close consideration should be given to the definition of 'personal data' in art 4(1) of the EU General Data Protection Regulation ('GDPR').[29] The definition in the *Privacy Act* could be rephrased as:

[24] *Ibid* at paras 41 *et seq.*
[25] *Ibid* at para 48.
[26] *Ibid* at para 49 [emphasis added].
[27] *Ibid* at para 46.
[28] *Ibid* at para 49.
[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, 4.5.2016, 1.

"personal information" means information or an opinion:

(c) whether the information or opinion is true or not; and

(d) whether the information or opinion is recorded in a material form or not,

relating to** an identified individual, or an individual who is reasonably identifiable or **capable of being singled out, directly or indirectly,** in particular **by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to identity of that individual's identity.

9. A revision in alignment with the definition in the GDPR would have four key features:

(a) It would replace the word 'about' with the expression 'relates to'. While such a change would draw on the influential definition of personal data in s 4(1) of the GDPR, it would de-couple the Australian definition from the position in the APEC Privacy Framework,[30] the New Zealand *Privacy Act 2020*[31] and in Canadian privacy legislation,[32] all of which use the word 'about'. In EU jurisprudence, the requirement that the information must 'relate to' an individual has been interpreted as meaning that 'it is "linked to a particular person" by reason of its content, purpose or effect'.[33]

While the different wording could justify a different interpretation, there is no compelling reason that the word 'about' should be read as requiring a closer connection of the information with a particular person than the expression 'relates to'. Indeed, the Article 29 Working Party (a former advisory body established under the EU Data Protection Directives), in providing guidance as to how the words 'relating to' should be interpreted, stated that '[i]n general terms, information can be considered to 'relate' to an individual when it is about that individual'.[34] This interpretation suggests that the terms 'relating to' and 'about' are virtually synonymous, so that there is nothing inherent in the different words that dictates a particular interpretation. We submit therefore that use of the word 'relates to' would create greater alignment with the highly influential data regime under the GDPR, but that the advantages of doing so would have to be weighed against the loss of alignment with the regional APEC Framework, as well as the common law jurisdictions of New Zealand and Canada. Either way, we are not suggesting that this choice of terminology is determinative of the issue of whether technical data should fall within the definition of personal information. The more important aspects of the definition are the following.

[30] APEC Privacy Framework (2015), [9].
[31] *Privacy Act 2020* (NZ), s 7.
[32] *Privacy Act*, RSC 1985, c P-21, s 3; *Personal Information Protection and Electronic Documents Act*, RSC 2000, c 5, s 2(1).
[33] P*eter Nowak v Data Protection Commissioner* (European Court of Justice, C-434/16, 20 December 2017), ECLI:EU:C:2017:994 [35].
[34] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, Working Paper 136 (2007), p 9.

(b) The inclusion of the expression 'directly or indirectly' is important as it makes clear that the issue of identifiability needs to be considered in the broader context of what other data is available. For example, in the case of the GDPR, it has been interpreted in the case of dynamic IP addresses as requiring an assessment of whether there is a reasonable likelihood of linkage with other databases that will result in identification.[35]

(c) The suggested revision includes reference to 'capable of being singled out' to address the issue identified by Borgesius[36] where an entity can reach and affect a person, for example, in the context of behavioural targeting, direct marketing, without knowing or needing to know their name or physical identity.

(d) The suggested revision includes the phrase 'by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to identity of that individual's identity' (which is again taken from the GDPR, art 4(1)) is suggested to make abundantly clear that it covers technical and other identifiers. This change is desirable because it would make the definition consistent with the expectations of individuals, including consumers of online services. In the 2020 Australian Community Attitudes to Privacy Survey (which the Australian Office of the Information Commissioner commissioned) 53% of respondents stated that they are uncomfortable with a business combining data about their customers (for example, loyalty card transaction history) with other data (for example, IP address, type of browser used) to better profile their customers.

Question 3: Should the definition of personal information be updated to expressly include inferred personal information?

17. The application of analytical techniques to information that does not initially qualify as personal information to link it to an identifiable/reasonably identifiable individual amounts to a new acquisition of personal data. We submit that the definition of personal information should make clear that such inferred information is 'personal information'. The revised definition recommended above would achieve this by inclusion of the words 'directly or indirectly' and by inclusion of the phrase 'by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to identity of that individual's identity'.

18. The same argument applies where personal information is transformed into sensitive information by specifically linking characteristics that fall within the definition of 'sensitive information' to an identifiable/reasonably identifiable individual.

---

[35] See P*atrick Breyer v Bundesrepublik Deutschland* (European Court of Justice, C-582/14, 19 October 2016), ECLI:EU:C:2016:779 [49].

[36] Frederik J Zuiderveen Borgesius, 'Singling Out People without Knowing Their Names: Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation' (2016) 32 *Computer Law & Security Review* 256.

Question 4: Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

19. Most debate surrounding the definition of personal information is related to the issue of when a person is 'identified' or 'reasonably identifiable'.[37] These discussions have become more important in light of significant recent advances in re-identification technologies.[38]

20. While de-identified information falls outside data protection laws, it has become contentious when information is sufficiently de-identified in the sense that, even with the use of re-identification technologies, individuals are no longer 'reasonably identifiable'.[39]

21. We recommend that the Act be amended to apply in part to information which is currently non-identifiable but might potentially lead to the identification of individuals if it is considered together with information that might otherwise be available about the information subject. The key principles which should be applicable in those circumstances are the disclosure limitation principle in APP 6 and the security principle in APP 11.

Question 5: Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?

Proxies for sensitive personal information

22. There is a further issue that should be dealt with by clarification of the definition. This relates the mining of personal data for attributes that can serve as proxies for the attributes listed in the definition of sensitive information. That is a significant issue given having regard to the proliferation of the algorithmic decision-making and the potential for proxies to be used as a basis for discrimination.

23. We submit therefore that this would be best handled by modifying the opening words of the definition of 'sensitive information' to read as follows:[40]

> *information or an opinion about,* ***or information or opinion that is collected for use as, or used or disclosed as a proxy for,*** *an individual's …* (etc.)

---

[37] See e.g. Anne SY Cheung, 'Re-personalizing personal data in the cloud' in Anne SY Cheung & Rolf H Weber, (eds), *Privacy and Legal Issues in Cloud Computing* (Cheltenham: Edward Elgar Publishing, 2015) 69, 69.
[38] Jane Henriksen-Bulmer & Sheridan Jeary, 'Re-identification attacks – A systematic literature review' (2016) 36(6) *International Journal of Information Management* 1184.
[39] Council of Europe, Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, (2014) 0829/14/EN, WP216; Information and Privacy Commissioner, Ontario, Canada, *Big Data and Innovation, Setting the Record Straight: De-identification Does Work*, by Ann Cavoukian & Daniel Castro (Toronto: IPC, ITIF, 16 June 2014).
[40] See *Privacy Act 1988* (Cth) s 6.

3.3 Employee Records Exemption

Question 13: Is the personal information of employees adequately protected by the current scope of the employee records exemption?

24. The existing position is that the privacy of employees, as opposed to prospective employees, receives no protection insofar as the data relates to their employment relationship. This is the case in relation even to highly sensitive data, including health data in most states, and other categories of personal data that qualify as 'sensitive data'. What is especially significant is that the exception is not restricted to employers' collection and use of this information, or employees' rights to access and request the amendment of their information, but also in respect of other significant obligations, including the obligation to keep it secure and to ensure that it is accurate and suitable for use.

25. This is now more problematic than ever given that technological developments have accelerated the trend towards more extensive collection of personal information, including detailed profiling and other information that is likely to cause significant harm if not handled properly. We submit that the employee records exemption should be abolished.

26. We accordingly recommend that the exemption should be abolished. It is at odds both Australian community attitudes[41] and with the legal position in comparable jurisdictions. For example, the New Zealand *Privacy Act* and the Canadian *Personal Information Protection and Electronic Documents Act* do not contain any equivalent exception for employee data. The EU General Data Protection Regulation likewise does not provide any employee record exception and, in the case of the UK, the Information Commissioner's Office ('ICO') has published both an employment practices code[42] and a guide in respect of it.[43] Significantly also, guidance document concerning to the GDPR's obligations for controllers to prepare data protection impact statements where processing is 'likely to result in a high risk to the rights and freedoms of natural persons' identifies employees as an example of individuals whose vulnerability may require additional privacy safeguards due to an imbalance in the relationship between employers and employees.[44]

[41] Office of the Australian Information Commissioner and Lonergan, *Australian Community Attitudes to Privacy Survey 2020* (September 2020) p 60.
[42] ICO, 'The employment practices code', <https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf>.
[43] ICO, 'Quick guide to the employment practices code', <https://ico.org.uk/media/for-organisations/documents/1128/quick_guide_to_the_employment_practices_code.pdf>.
[44] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, p 8.

Question 14: If enhanced protections are required, how should concerns about employees' ability to freely consent to employers' collection of their personal information be addressed?

27. In most cases, there is a power imbalance between employers and employees. This is demonstrated not only in cases such as *Lee v Superior Wood Pty Ltd,*[45] where the validity of consent in the face of disciplinary processes was in question. The European Data Protection Board suggests in its Guidance on Consent that given the 'dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal'.[46] However, where an employee does not need to anticipate adverse consequences from withholding consent, it can be assumed that a consent if provided was freely given. This may, for example, be the case where an employee is asked whether or not they consent to have their photographs taken while at a social function at work and to have these photographs published in workplace newsletter.

28. We therefore submit that enhanced protections are needed where the freedom of an employee to consent may be compromised by actual or perceived economic pressures. Therefore, the Act should limit the ability for entities to collect and process information on the basis of consent in situations where there is an imbalance in the relationship between the entity and the information subject. It should be required that the data handling would be based on a different justification, such as the protection of the employer's legitimate interests. Ideally this alternative legal basis would require a balancing of the competing interests of employers and employees and be supplemented by detailed guidance by the Office of the Australian Information Commissioner ('OAIC'). This protection could be supplemented by a requirement in such situations to prepare privacy impact assessments in circumstances where the data subject is particularly vulnerable because of the power imbalance between employer and employee.

Question 15: Should some but not all of the APPs apply to employee records, or certain types of employee records?

29. If it is decided that some additional exclusion is required for employment data, we submit that it would be preferable to include exceptions in respect of APPs 5, 6 and 12 that are narrowly targeted to the specific HR needs of employers.

[45] [2019] FWCFB 2946; 286 IR 368.
[46] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1, Adopted on 4 May 2020, [21].

3.4 Political Parties Exemption

Question 16: Should political acts and practices continue to be exempted from the operation of some or all of the APPs?

The rise of political micro targeting

30. When the exemption for political parties and practices was introduced, it was justified by reference to the importance of the freedom of political communication to Australia's democratic process. In the Second Reading Speech, it was posited that the exemption was 'designed to encourage that freedom and enhance the operation of the electoral and political process in Australia'.[47] In light of the newly emerging practices of data-driven political campaigning however, it must now be doubted whether this rationale continues to stack up.

31. The issues arising from the use of electoral databases have changed considerably with the advent of big data analytics. [48] Political parties, movements and candidates increasingly rely on personalised communication informed by sophisticated profiling techniques to target potential voters. Social media platforms are central to such data-driven campaigning because they are the medium for such communications as well as the custodians of the data that enables profiling. Profile-based communication with voters exploits vast troves of personal data held by social media platforms to infer individuals' political views and crafts messages to which targeted persons are expected to be particularly receptive.

32. Political micro-targeting, which involves 'the use of data and analytics to craft and convey a tailored message to a subgroup or individual members of the electorate',[49] has generated a number of privacy concerns. Big data analytics can deduce such receptiveness to particular political messaging from often mundane, non-sensitive personal data.

33. Micro-targeted political communications are significantly different from those that existed prior to the big data analytics revolution. In contrast to conventional political broadcasts in mass media, campaign speeches and strategic door-knocking, modern political communications are 'much more precise, and "knowing"' about their recipients.[50] Harnessing the power of artificial intelligence, they can be designed,

[47] Australian Commonwealth House of Representatives, Parliamentary Debates (12 April 2000) 15749 (D Williams, Attorney-General), 15753.
[48] 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* (Abingdon UK, Routledge 2020)164; see also 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* (CUP, forthcoming, 2021), pre-publication version at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717561>.
[49] Balázs Bodó, Natali Helberger and Claes H de Vreese, 'Political micro-targeting: A Manchurian candidate or just a dark horse?' (2017) 6(4) *Internet Policy Review*, doi: 10.14763/2017.4.776.
[50] Bethany. Shiner, 'Political Campaign Methods and the Need for Fundamental Reform' [2019] *Public Law* 362, 365.

based on the profiling of individual traits, to maximise the emotional and psychological impact on their recipients. Significantly, those individual traits are not necessarily concerned with political leanings per se, but might include anxieties, concerns or vulnerabilities into which a particular political message can tap. Such subtle personalised communications also make it infinitely harder to identify the manipulation and guard against it.

The data handling practices of political parties

34. The data-driven personalisation of political campaigning has therefore created new threats to the privacy of personal information, and to the democratic process as a whole. Political micro-targeting has received its most detailed examination in the US (in the context of the Obama[51] and Trump[52] elections) and in the UK (in the context of the 2016 Brexit referendum[53]). In the US for example, now defunct company *Cambridge Analytica* used a methodology that combined psychometric scores with individual Facebook profiles to build up demographic and psychological profiles, which could then be used for micro-targeting. Official inquiries in the aftermath of the *Cambridge Analytica* scandal[54] have highlighted the wide-scale manipulation and deception of voters by domestic and foreign actors, consisting of 'intentionally and covertly influencing [voters'] decision-making, by targeting and exploiting their decision-making vulnerabilities'.[55] This type of political messaging is a far cry from the liberal assumptions underlying democratic processes that have a rational and well-informed citizenry freely deliberate on past governing records and alternative political manifestos.[56]

[51] See e.g. Lynda Lee Kaid, Juliana Fernandes and David Painter, 'Effects of Political Advertising in the 2008 Presidential Campaign' (2011) 55(4) *American Behavioral Scientist* 437; Bruce Bimber, 'Digital Media in the Obama Campaigns of 2008 and 2012: Adaptation to the Personalized Political Communication Environment' (2014) 11 *Journal of Information Technology & Politics* 130.
[52] Nathaniel Persily, 'The 2016 U.S. Election: Can Democracy Survive the Internet? (2017) 28 *Journal of Democracy* 63; Samuel C Woolley and Douglas R Guilbeault, 'Computational Propaganda in the United States of America: Manufacturing Consensus Online' (2017) Working Paper No. 2017.5, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-USA.pdf>; Roberto J González, 'Hacking the citizenry? Personality profiling, "big data" and the election of Donald Trump' (2017) 33 *Anthropology Today* 9.
[53] Carole Cadwalladr, 'The great British Brexit robbery: How our democracy was hijacked', *The Guardian* (online, 7 May 2017) <www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy>; Marco Bastos and Dan Mercea, 'The public accountability of social platforms: lessons from a study on bots and trolls in the Brexit campaign' *Philosophical Transactions of the Royal Society A* (4 June 2018) <https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2018.0003>.
[54] See, for example, Information Commissioner's Office (UK), *Democracy disrupted? Personal information and political influence* (11 July 2018) <https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf>; Information Commissioner's Office (UK), Investigation into the use of data analytics in political campaigns: A report to Parliament (6 November 2018) pp 5–6 <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>.
[55] Daniel Susser, Beate Roessler and Helen F Nissenbaum, 'Technology, Autonomy, and Manipulation' (2019) 8(2) *Internet Policy Review*, DOI: 10.14763/2019.2.1410.
[56] See, eg, Bernard R Berelson, Paul F Lazarsfeld and William N McPhee, *Voting: A Study of Opinion Formation in a Presidential Campaign* (University of Chicago Press, 1954) 308.

35. A number of high profile enquiries in the UK have since identified significant shortcomings in the data handling practices of political parties and other political actors.[57] The UK Electoral Commission has reported on the 2019 General Election that voters' trust in election campaigns has been undermined because it 'is too often unclear who is behind digital election campaign material', and identified 'significant public concerns about the transparency of digital election campaigns risk overshadowing their benefit'.[58] The UK Information Commissioner's Office recently released an audit that concludes that political parties need to improve their compliance with data protection laws, including their transparency and accountability, and announced that it will update its guidance on political campaigning.[59]

A lack of regulatory oversight

36. Just like their overseas counterparts, Australian political parties are becoming increasingly reliant on using modern technologies to interact with potential voters. However, given the Australian *Privacy Act* does not apply to registered political parties[60] or that many political acts and practices are exempt,[61] the actual data-handling practices engaged in by Australian parties and political organisations remain shrouded in secrecy. Indeed, most Australians are unaware that political parties are able to collect and use the personal information of voters largely without regulatory oversight. This explains why, in the 2020 Community Attitudes to Privacy Survey, 52% of respondents assumed wrongly that Australia's privacy laws apply also to political parties.[62]

37. The exemptions mean that privacy-invasive practices will often not come to light because they cannot be investigated and that there is no obligation on political parties and campaigners to reveal the extent of their use of personal data.

The data obligations of political parties in the EU and the UK

38. The EU's General Data Protection Regulation ('GDPR') – as complemented by the ePrivacy Directive[63] – does not exempt political communications from its regime.[64]

---

[57] Information Commissioner's Office (UK), *Investigation into the use of data analytics in political campaigns: A report to Parliament* (6 November 2018) <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>; Electoral Commission (UK), *Digital campaigning: Increasing transparency for voters* (June 2018).
[58] The Electoral Commission (UK), *UK Parliamentary General Election 2019*, p 2 <http://www.electoralcommission.org.uk/sites/default/files/2020-04/UKPGE election report 2020.pdf>
[59] Information Commissioner's Office (UK), *Audits of data protection compliance by UK political parties: Summary report* (November 2020) <https://ico.org.uk/media/action-weve-taken/2618567/audits-of-data-protection-compliance-by-uk-political-parties-summary-report.pdf>.
[60] *Privacy Act 1988* (Cth), s 6C.
[61] *Privacy Act 1988* (Cth), s 7C.
[62] Office of the Australian Information Commissioner and Lonergan, *Australian Community Attitudes to Privacy Survey 2020* (September 2020) p 58.
[63] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, 37
[64] There are also countries that completely prohibit data capture by political parties, such as Japan. See eg, Bennett and Oduro-Marfo C. J. Bennett and S. Oduro-Marfo, *Privacy, Voter Surveillance and*

Indeed as part of the requirement for lawfully collecting and using data, it stipulates 'explicit consent' as a precondition for collecting and using any data that reveals a political opinion.[65] In the absence of explicit consent by the data subject, processing of sensitive data is permissible only to the extent that it can be justified on specific grounds,[66] which are narrower than in the case of non-sensitive data. These restrictions can also apply to micro data points that are mundane and non-sensitive by themselves, but are processed in order to generate insight about political leanings.

39. The restrictions in the GDPR concerning sensitive data do not apply to communications by a political party with its members, or with others who have regular contact with it.[67] As a consequence, those activities are subject to the lesser restrictions applicable to personal data more generally.[68] These lesser restrictions permit processing on the basis of consent, where processing is necessary for the performance of a task carried out in the public interest, or where it is necessary for the purposes of the 'legitimate interests' of the controller or a third party (except where those interests are 'overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data').[69] This results in a regime in which the lawfulness of data processing generally, consent aside, requires a balancing of the competing rights and interests involved.

40. It is also important to note that the GDPR allows for some derogations by Member States, of which the UK has availed itself. The *Data Protection Act 2018* (UK) gives politicians and political parties important additional leeway because it provides that data processing that is necessary for 'an activity that supports or promotes democratic engagement'[70] is to be regarded as processing of personal data 'that is necessary for the performance of a task carried out in the public interest'.[71] Data processing for democratic engagement, which includes communicating with electors and interested parties, opinion gathering, campaigning activities, activities to increase voter turnout and fundraising,[72] is thereby lawful under the GDPR, provided it is necessary[73] and the task is laid down in domestic law, such as in electoral laws.[74]

Democratic Engagement: Challenges for Data Protection Authorities (ICO and University of Victoria, BC, Canada, 2019) 37–39. <https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf>.

[65] These are specified in GDPR, art. 9(1).

[66] GDPR, art. 6

[67] GDPR, art. 9(2)(d).

[68] GDPR, art. 6(1).

[69] GDPR, art. 6(1)(f).

[70] GDPR, art. 6(1)(e) and (f).

[71] *Data Protection Act 2018* (UK), s. 8(e), taking advantage of the derogation provision in the GDPR, art. 6(2).

[72] *Data Protection Act 2018* (UK), Explanatory Notes, para 86.

[73] The 'very wide' democratic engagement provision has been criticised by the ICO in the legislative process: Information Commissioner's Office (UK), Data Protection Bill, House of Commons Public Bill Committee: Information Commissioner's further written evidence (19 March 2018) <https://ico.org.uk/media/about-the-ico/documents/2258462/data-protection-bill-public-bill-committee-ico-further-evidence.pdf>.

[74] See GDPR, art. 6(3) and Information Commissioner's Office, *Guidance on political campaigning: Draft framework code for consultation* <https://ico.org.uk/media/about-the-

41. Notably, the GDPR appears implicitly to recognise the structural weakness of consent as a legitimising device for data processing, by setting up an overarching framework of 'background' duties on data controllers which are independent of user consent. These include the principles of 'privacy by default' and 'privacy by design'.[75]

42. A further background duty is the obligation to carry out 'Data Privacy Impact Assessments' (DPIAs) for highly invasive activities, measured either by the scale of processing activity of 'sensitive data' or their effect on individuals,[76] with the view to identifying and minimising risks. DPIAs are a mechanism that allows a data controller to systematically and comprehensively analyse their processing with a view to identifying and minimising data protection risks. Whilst these duties apply to political parties that employ micro-targeting in their campaigns,[77] they neither hinder such messaging nor necessarily prevent its manipulative variations. However, they do impose a more rigorous process of establishing practices that pay sufficient regard to the fairness and transparency of the data processing and its anticipated purposes.

43. In addition, art 22 GDPR contains a right not to be subject to automated decision making, 'including profiling, which produces legal effects' concerning the data subject or similarly significant effects. That right is, however, subject to a number of exceptions, including where the profiling is authorised by a law to which the controller is subject and lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

44. Benefits of data protection laws also arise in the case of data breaches. Many jurisdictions now mandate data controllers to notify individuals about the loss or unauthorised access of personal information. These laws would also apply to political parties, which – as we know also from Australia[78] – have been the target of malicious hacks, including by foreign actors.

The ALRC proposal to abolish the political exemptions

45. When the Australian Law Reform Commission ('ALRC') conducted its review of the *Privacy Act* in 2008, it noted that electoral databases might contain a range of personal information about voters, including 'policy preferences and party identification as well

ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf> 37.

[75] Ibid.

[76] GDPR, arts. 33–36. European Commission, *Commission guidance on the application of Union data protection law in the electoral context* (September 2018), COM(2018) 638 final <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf> 8.

[77] Information Commissioner's Office (UK), *Investigation into the use of data analytics in political campaigns: A report to Parliament*.

[78] Michelle Grattan, '"State actor" makes cyber attack on Australian political parties', *The Conversation* (18 February 2019), <https://theconversation.com/state-actor-makes-cyber-attack-on-australian-political-parties-111993>.

as such matters as the individual's occupation, membership of community organisations, and so on'.[79] The ALRC 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.[80]

46. It concluded:

> [P]olitical parties and those engaging in political acts and practices should be subject to the Privacy Act – provided that the legislation can accommodate adequately the constitutional doctrines of implied freedom of political communication and parliamentary privilege.[81]

47. The ALRC report accordingly recommended to remove both the exemption for registered political parties and the exemption for political acts and practices.[82] The ALRC also recommended amending the Act 'to provide that [it] does not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication or parliamentary privilege'.[83]

48. This recommendation was based on a model provision issued by the Office of Parliamentary Counsel.[84] Provisions of this type exist in other Australian statutes[85] and are designed to ensure that the Acts can be read down to ensure their constitutional validity. The ALRC commented that this enabled the constitutional validity of specific acts and practices to be 'determined on a case-by-case basis by the relevant court or tribunal',[86] thereby allowing for a more fine-tuned approach to invalidity than a blanket exemption.

Our recommendations

49. As we have argued elsewhere in more detail,[87] the unprecedented use of micro-targeted messaging in political communications in their manifold variations – ranging

---

[79] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* ALRC Report 108 (2008) [41.13].
[80] Ibid.
[81] Ibid [41.16].
[82] Ibid Rec 41-1.
[83] Ibid Rec 41.2.
[84] The current version of this model provision is contained in: Parliament of the Commonwealth of Australia, Parliamentary Counsel, Drafting Direction, No. 3.1 Constitutional law issues (October 2012) 6.
[85] See e.g. the identical provisions in: *Spam Act 2003* (Cth) s 44; *Do Not Call Register Act* 2006 (Cth) s 43; *Telecommunications Act 1997* (Cth) s 138.
[86] Australian Law Reform Commission (n 19) [41.48].
[87] 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* (CUP, 2021) (forthcoming) pre-publication version at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717561.

from the clearly deceptive or manipulative message to the confirmatory or engaging – requires a revaluation of the role of information privacy in political campaigns. In the light of the emergence of data-driven personalisation as a central force in political communication and the ability of parties to leverage information about voters to advance their political agendas, we submit that the widespread concerns about personalised political communications need to be taken seriously. It can no longer be assumed that the imposition of any privacy-based restrictions would be inherently detrimental to democracy and incompatible with the freedom of political communication.

50. The practical effect of extending the *Privacy Act* to political actors would be to require them to comply with the APPs and other privacy standards. It 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 of political communication would merely be indirect and would impose some restrictions on current practices.

51. In our view, subjecting political parties and political acts and practices to the data-handling principles that apply to other organisations and to other acts and practices is conducive to promoting the constitutionally prescribed system of representative government. The link between privacy and democratic systems of representative government has long been recognised.[88] Privacy protection is an indispensable aspect of allowing voters to identify their preferred representatives and to come together to exercise their political choices.[89] Protecting voters from undue surveillance or interference with their personal information by political parties or other political actors, would clearly serve a legitimate end. It is not incompatible with the constitutional system of representative government and would, in fact, enhance it.

52. It is important to note that the APPs are open-textured. In line with objects of the Act, they have been adapted to promote not only the 'protection of privacy of individuals'[90] but also 'to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities'.[91] This is reflected, for example, in the collection limitation principle, which does not generally *mandate* consent (except in relation to specific categories of sensitive information); instead, its main limitation is that information must be collected 'only by lawful and fair means'[92] and must generally be collected only from the individual unless 'it is unreasonable or impracticable to do so'.[93]

[88] Volker Boehme-Neßler, 'Privacy: a matter of democracy. Why democracy needs privacy and data protection' (2016) 6(3) *International Data Privacy Law* 222, citing Beate Rössler, *Der Wert des Privaten* (Suhrkamp Verlag 2001) 331.
[89] Patricia Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press 1995) 126–127.
[90] *Privacy Act 1988* (Cth) s 2A(a).
[91] *Privacy Act 1988* (Cth) s 2A(b).
[92] Ibid, Australian Privacy Principle 3.5.
[93] Ibid, Australian Privacy Principle 3.6.

53. 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 that is necessary for the operation of a democratic system without unreasonably undermining the ability of political parties to communicate with voters. It follows 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.

54. We submit that the time has come to implement the recommendation of the ALRC and to abolish the political exemptions in the *Privacy Act*. This would align Australian law with international best practice. 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 transparency of profiling and targeted messaging and provide some regulatory oversight at the input and process side of these practices.

55. In our view, this move would help to stem further erosion of trust in political representation and campaigning. We submit that political parties claiming for themselves an immunity from the same data protection practices and principles that apply to the wider community do a disservice to democracy. 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.

56. In our view, the ALRC recommendations to abolish the political exemptions to the *Privacy Act* should be endorsed and implemented. 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 advent of big data, data-driven campaigning and political micro-targeting has created new threats to the privacy of personal information, has made the case for reform even stronger.

57. Data protection laws have an important role to play in limiting the processing of personal data and requiring practices to be designed in a manner that balances protects privacy and competing rights. Apart from providing greater transparency, the provisions in data protection statutes also require that data handlers follow fair information practices in relation to the collection, use, access, correction and security of personal information. These also give affected individuals a right of complaint to a data protection regulator.

58. We argue that removing special exemptions for political parties and political messaging would serve to enhance the privacy of voters without inappropriately undermining the important values inherent in the doctrine of freedom of political communication.

59. Our analysis of the implied freedom of political communication suggests that implementing the ALRC's recommendations would not conflict with the freedom of political communication. Any lingering doubt could be addressed through a saving provision that the *Privacy 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, as it is currently already in place for other legislation.

PART FOUR: PROTECTION OF PERSONAL INFORMATION AND GOOD PRIVACY PRACTICE

4.1 Obtaining Consent from Children

Question 33: Should specific requirements be introduced in relation to how entities seek consent from children?

16. Before considering the issue of regulatory reform it is important to consider why children's privacy requires specific attention.

17. As recognised internationally in the UN *Convention on the Rights of the Child*[94] ('CRC') and the Council of Europe's *Convention 108*,[95] children and young people may require special protections because of their potential vulnerability. The need for protection arises because children have diminished capacity to understand the importance of privacy, affecting their ability to consent and creating responsibilities for third parties, notably parents and guardians, in protecting their personal information. Importantly, as a child's capacity for decision-making develops, a child's rights approach requires that their views are given more prominence in order to safeguard children's agency.

Issues of Concern

18. In modern information societies, most interactions generate personal data that is routinely collected, aggregated and analysed. These practices also affect personal data about young people and children, who are increasingly engaging with technology, online platforms and social media.[96] Large quantities of data can be subject to processing via algorithms based on machine learning and artificial intelligence and used to inform many aspects of decision-making and to influence individuals (for example, in the context of advertising).[97]

19. Several privacy issues arise from this increased engagement and subsequent data collection, processing, storage and disclosure. The first relates to online data gathering activities of commercial organisations, which collect and use children's personal

[94] United Nations, Convention on the Rights of the Child, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990).
[95] Council of Europe, Convention 108+ art 15(2)(e), requiring data protection authorities to give specific attention to the data protection rights of 'children and other vulnerable individuals.
[96] See, eg, Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, 'Children's data and privacy online: growing up in a digital age: an evidence review' (2019, London School of Economics and Politics) <http://eprints.lse.ac.uk/101283>; Veronica Barassi, 'The Child as Datafied Citizen: Critical Questions on Data Justice in Family Life, in: Giovanna Mascheroni; Anna Jorge and Cristina Ponte (eds), *Digital Parenting: The Challenges for Families in the Digital Age* (Gothenburg: Nordicom), p. 169: Deborah Lupton and Ben Williamson, 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights' (2017) 19(5) *New Media & Society* 780.
[97] See, for example, Moira Paterson and Maeve McDonagh, 'Data protection in an era of big data: The challenges posed by big personal data' (2018) 44(1) *Monash University Law Review* 1.

information for the purposes of digital marketing to them.[98] Companies now regularly share children's data from social media platforms, mobile apps and the internet of toys for analytics, personalisation and advertising.[99] Emerging evidence suggests that while younger children are able to recognise the risks arising from information oversharing or revealing their real identities online, they are considerably less aware of the dangers of resulting from online tracking or game promotions.[100]

20. The second regards the increased exposure of children's personal information online by their parents. This occurs through parents posting on social media and other platforms (a phenomenon known as 'sharenting'[101]) and through the increased use of IoT applications such as smart home devices that give the device manufacturer access to the goings-on in the family home.[102]

21. In addition, young people's privacy rights raise special issues in part due to their reduced capacity for consent.[103] For example, it needs to be decided at what point children, rather than their guardians, should be allowed to make the relevant privacy choices.

Children's Consent in Australia

22. The *Privacy Act* makes no specific reference to children or young people and offers no additional protection for them. As a result, where data processing requires consent, the ordinary principles relating to consent, and the capacity to give consent, apply.[104] If a child provides consent, this consent is valid only if he or she has the requisite capacity to consent to the information processing. This requires that the child has sufficient understanding and maturity to understand what is being proposed. Capacity must generally be determined on the basis of individualised assessment.

23. This model for individualised assessment of capacity is consistent with the available research on development psychology, which suggests that children attain maturity at significantly different ages, making the use of bright line approaches based on age for

[98] UNICEF, *Children and Digital Marketing: Rights, risks and responsibilities*, Discussion Paper (2018).
[99] Karen Louise Smith & Leslie Regan Shade, 'Children's digital playgrounds as data assemblages: Problematics of privacy, personalization, and promotional culture (2018) 5(2) *Big Data & Society* 1; Esther Keymolen and Simone Van Der Hof, 'Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust' (2019) 4(2) *Journal of Cyber Policy* 143.
[100] Jun Zhao et al, '"I make up a silly name": Understanding Children's Perception of Privacy Risks Online', *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, arXiv:1901.10245v1.
[101] Claire Bessant, 'Sharenting: balancing the conflicting rights of parents and children' (2018) 23(1) *Communications Law* 7-24; Sonia Livingstone, Alicia Blum-Ross and Dongmiao Zhang, 'What do parents think, and do, about their children's online privacy? Parenting for a Digital Future', Survey Report 3 (LSE, 2018).
[102] Anne Pfeifle, 'Alexa, what should we do about privacy? Protecting privacy for users of voice activated devices' (2018) 93(1) *Washington Law Review* 421.
[103] Simone van der Hof, 'I agree… or do I? A rights-based analysis of the Law on Children's Consent in the Digital World' (2017) 34(2) *Wisconsin International Law Journal* 410.
[104] *Health Records and Information Privacy Act 2002* (NSW), s 7 contain detailed provisions on capacity to consent and the giving of consent by a representative. See *Privacy and Data Protection Act 2014* (Vic) s 28 and *Health Records Act 2001* (Vic), s 85.

determining capacity problematic. It is also consistent with the approach taken in Art 12(1) of the CRC, which requires states to:

> Assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.

24. However, this model requires decision-makers to make complex assessments and may create risks to children if there is failure to identify correctly any lack of capacity on their part. There is also the problem that there is currently no specific requirement for providers of services to children to draft privacy notices in a manner that children can understand easily, even though the ability to provide informed consent depends on a full understanding of the consequences involved.

25. The OAIC's Australian Privacy Principles Guidelines seek to address these problems by steering a middle ground between individualised assessment and practicability. The Guidelines affirm the general proposition that APP entities need to determine 'on a case-by-case basis'[105] whether an individual under the age of 18 has the capacity to consent and that capacity depends on 'whether they have sufficient understanding and maturity to understand what is being proposed'.[106] However, the Guidelines also suggest that, if it is not practicable or reasonable for an APP entity to assess a child's capacity on a case-by-case basis, the entity may rely on two presumptions: first, that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise; second, that a child under 15 does not have capacity to consent.[107]

26. This approach leaves a number of questions, including how exactly an entity is to determine the capacity of an individual under the age of 18; when an individual assessment will be considered to be not practicable or reasonable; and how conflicts between a child and a parent in relation to the giving of consent are to be resolved. Given that children's data rights are an area of increasing concern in overseas jurisdictions, it is surprising that there is very little information available on how Australian organisations handle children's personal data and how they conform with the requirements under the *Privacy Act*.

27. Another complex policy issue concerns the scope of the activities regulated. The commercial context is particularly important because, as noted recently by the United Nations Special Rapporteur on the right to privacy, 'an increasing number of corporations today already gather much more personal data than most governments ever can or will'.[108] However, devising appropriate rules to regulate commercial services is complex because it is necessary both to ensure that any rules imposed are

---

[105] OAIC, *Australian Privacy Principles Guidelines* (July 2019), <https://www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf>, B 56.
[106] Ibid, B57.
[107] Ibid, B58.
[108] Statement by Mr Joseph A Cannataci, Special Rapporteur on the right to privacy, at the 31st session of the Human Rights Council, 9 March 2016, <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21248&LangID=E>.

capable of working in practice and that they do not impose inappropriate constraints on young people's autonomy. This may require a combination of measures that impose constraints on data collection practices and ones that allow for the subsequent deletion of information volunteered by individuals while they were children.

Children's Consent in Overseas Jurisdictions

28. In the United States, children's online privacy is regulated at the federal level by the Children's Online Privacy Protection Act ('COPPA').[109] Protections provided under COPPA are, in some jurisdictions, supplemented by state regulation, as is the case in California with the Californian Consumer Privacy Act ('CCPA').[110] There is also a dedicated statute that applies to children's education records, but that is beyond the scope of this submission.[111]

29. The COPPA requires the US Federal Trade Commission (FTC) to promulgate regulations on the collection of children's personal information by operators of commercial websites, online services and mobile apps.

30. The relevant regulation known as the 'COPPA Rule' requires websites and other online services that collect personal information from children under the age of 13 to provide notice to parents[112] and to obtain verifiable parental consent[113] before collecting, using, or disclosing personal information from these children. The COPPA Rule also contains a right for parents to review personal information provided by a child,[114] to object to the further use or future online collection of their child's personal information[115] and to direct the online service provider to destroy personal information that has been collected so far.[116] The rule also outlaws specified unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.[117]

31. As a result of COPPA, most major companies take seriously compliance with its requirements of providing clear and child-appropriate privacy notices.[118] This has had the effect of protecting younger children from some practices of digitalised advertising that are in play in the case of teens and adults. Further, the rigid age limit (under 13) provides the benefit of clarity, however, as companies can more easily establish

[109] 5 U.S.C. §§ 6501–6506.
[110] The *California Consumer Privacy Act 2018*, contained in California Civil Code §§ 1798.100 to 1798.198.
[111] The *Family Educational Rights and Privacy Act 1974* protects such records from unauthorised disclosure and generally requires written consent by parents (and eligible students) before they can be shared. It also gives parents the right to access and seek to amend their children's education records.
[112] 16 C.F.R. § 312.4.
[113] 16 C.F.R. § 312.5.
[114] 16 C.F.R. §312.6.
[115] 16 C.F.R. §312.6 (a)(2).
[116] Ibid.
[117] 16 C.F.R. §312.3.
[118] Anthony D Miyazaki, Andrea JS Stanaland, and May O Lwin, 'Self-Regulatory Safeguards and the Online Privacy of Preteen Children' (2009) 38 *Journal of Advertising* 79, 83.

whether a child is 13 years of age than whether the child is of sufficient maturity to decide on its privacy protections.

32. However, a major weakness of the COPPA regime is that, while the FTC encourages operators also to adopt age-appropriate protocols for personal information collected from teenagers aged 13 and over,[119] COPPA imposes no statutory requirement for them to do so.

33. There is also no statutory requirement for operators of general audience websites to verify a user's age. The lack of user age verification, risks giving younger children access to content and platforms intended for teens and adults. For example, platforms that reserve access to certain content (such as advertising for alcohol, gambling etc) for adults could improperly make such content available by reference of the incorrect date of birth and thus before the user actually turns 18 years of age.

34. A further criticism of the COPPA approach to children's privacy regulation is that the COPPA Rule is underpinned by the notion that children (meaning those under the age of 13) are not sufficiently developed to make decisions that concern the use of their data, and therefore parents must give consent in their stead. It may be queried however whether children reach the development stage at which they can make an informed decision to provide businesses with their personal data at exactly 13 years of age. Indeed, children develop at differing rates, and it may be more appropriate to make the validity of consent dependent also on the character of the data, the uses the data is put to and the relationship between child and third party operator.

35. In addition, the imposition of a rigid 'age of digital consent' may have indirect consequences harmful to children. For example, business may decide to no longer offer services for young people under the relevant age limit and that young people choose to evade the age limits by deception. Indeed, many general audience social media companies provide in their terms of service that account holders must be 13 years of age or older.[120] These limits are set to avoid the restrictions imposed by COPPA. However, there is some evidence to suggest that children lie about their age in order to access these websites or that they manipulate verification procedures.[121] It is a matter of concern from a child rights perspective to exclude children from particular service rather than to develop protocols that allow children to use that service safely.

36. Another critical problem is that parents, while older, also often lack understanding of the legal regime around children's privacy or the digital literacy to assess the appropriateness of a particular data processing measure for their children. For example, Ofcom (the UK communications' regulator) reports relatively low levels of awareness amongst parents regarding the minimum age rules in leading social media

[119] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012) at 29, 60.
[120] This includes Facebook, Snapchat, Twitter, Instagram, Skype and YouTube. See Josh Constine, 'Instagram still doesn't age-check kids. That must change.' T*echCrunch* (3 December 2019) <https://techcrunch.com/2019/12/03/instagram-age-limit/>.
[121] See Ofcom, *Children and Parents: Media Use and Attitudes Report 2019* (4 February 2020) 19.

sites.[122] Even more concerningly, parent surveys also revealed that two in five parents whose child (aged between 5-15) uses social media or messaging services say that they would allow their child to use these platforms even before reaching the required minimum age.[123] This suggests that strict minimum age levels, combined with self-verification, are a problematic way of protecting the privacy of children online.

37. In California, the CCPA operates as a general data protection law that regulates the handling of the 'personal information' of Californian residents by businesses. The CCPA also contains specific provisions relating to children, including restrictions on the collection and handling of children's information, which creates a complex interrelationship with the COPPA.

38. The CCPA states that a business must not 'sell' a child's personal information if it has actual knowledge that the he or she is less than 16 years of age, unless he or she, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorised the sale of the consumer's personal information.[124] 'Sell' is defined broadly, meaning any disclosure for valuable consideration. Furthermore, the act deems a business that wilfully disregards the consumer's age to have had actual knowledge of it. While this requirement is confined to the sale of information, the requirement to ask young users their age so that they can determine their obligations in relation to the sale of that information triggers the collection limitation in the COPPA.

39. Another important feature of the CCPA, which is not specifically focussed on children but is beneficial for them, is a qualified right to request deletion of data. This permits a consumer to request a business or service provider to delete personal information collected by the business from the consumer if it is no longer necessary for the business or service provider to maintain that information for one of more specified purposes.[125] Allowing individuals to retrieve volunteered personal information once it is no longer required, is especially important in relation to children who may have volunteered their information without fully understanding the full implications of doing so.

40. In the EU, the GDPR refers specifically to children several of its articles and recitals. The articles set out the binding legal requirements that must be followed, while the recitals serve as a similar type of function to the explanatory memorandum for an Australian Act.

41. The GDPR contains a specific provision on exercise of children's data privacy rights, and a number of other provisions giving children special protections. The GDPR does not define the term 'child', but in the line with the CRC, it is understood as referring to

[122] Ofcom, *Children and Parents: Media Use and Attitudes Report, 2017* (29 November 2017) 260-1. In a survey of 1,388 parents of children aged five to 15, nearly 6 out of 10 parents did not know that there was a lower age restriction or what the age is set at. Higher numbers were reported for Snapchat and Instagram.
[123] Ibid, 262.
[124] California Civil Code § 1798.120(c).
[125] California Civil Code § 1798.105(a).

a child under the age of 18. Recital 38 explains that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. It also emphasises that this protection should apply in three situations, in particular:

i. the use of children's personal data for the purposes of marketing;
ii. the use of children's personal data for the purposes of profiling them; and
iii. the collection of children's personal data when they are using services offered directly to a child.[126]

42. The GDPR contains four key operative provisions that provide enhanced protection for children. These are article 8, which regulates the issue of children's capacity in the context of on the provision of online services by entities such as online marketers, apps and online content providers; article 6, which specifies the grounds on which personal data may lawfully be processed; article 12, which deals with transparency requirements; and article 17 concerning the right to erasure.

43. Article 8 specifies a cut off age of 16 for consent in respect of offers made directly to a child, but this can be varied to a minimum of 13 years by individual member states. Where a child is younger than 16 (or such lower age as is specified by a member country), consent is lawful only if, and to the extent that, consent is given or authorised by the holder of parental responsibility over the child. The GDPR provides little guidance on the verification of parental consent, leaving it largely up to the controller to make reasonable efforts to obtain verification.

44. The flexibility provided under article 8 has led to a bewildering lack of uniformity across the 27 jurisdictions.[127] Whereas some Member States (such as Germany or Ireland) chose not to derogate from the age of 16 years, the majority adopted 13, 14 or 15 years as the relevant age.

45. Article 6(1) ground (f) permits processing on the basis that it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child. The specific reference to children in this context draws attention to the fact that children have special interests and fundamental rights and freedoms that warrant particular attention.

[126] The other relevant recitals are recital 58 and 75. Recital 75 lists risks to the rights and freedoms of natural persons that may result from personal data processing and lead to physical, material or non-material damage. That list specifically refers to the 'processing of personal data of vulnerable natural persons, in particular of children'.

[127] In its first review of the operation of the GDPR, the Commission has identified the variation in age limits as problematic and calls for reform: European Commission, *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, p 7.

As a general rule, this makes it more difficult for data processing to be justified by reference to Art. 6(1), where the data subject is a child rather than an adult.

46. Article 12 requires controllers to provide the information required in privacy notices 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child'.[128] The specific reference to children is important because privacy notices play an important role in ensuring the informed exercise of consent and other rights under the Regulation, and this draws attention to the fact that children may require simpler language in notifications. This is reinforced in Recital 58 which emphasises that 'any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand'.

47. Finally, the GDPR contains a right to erasure in article 17. This article permits individuals to request the erasure of their personal data in specified circumstances, including where that processing has been grounded on consent and they wish to withdraw that consent. Significantly, recital 65 emphasises that this right is particularly relevant where consent to processing was given while the data subject was still a child and not fully aware of the risks involved, and later wants to remove this personal data. It also stresses that this is especially important where the data is located on the internet.

48. A key criticism of the protection provided under article 17, however, is that the right to erasure under the GDPR is not absolute. Indeed, the right depends on the existence of a specified ground for removal and is subject to a number of exceptions, including exceptions embodying considerations of free speech and public policy. In addition, there are considerable practical issues with removing data on social media sites, which may have already been saved and shared by other users. Finally, difficult questions arise about the age at which children should be able to make such requests, and the role of parents in making such requests for children.

49. The emphasis on protecting children's privacy in these articles is further reinforced by the requirement in Article 57 for the supervisory authorities that provide oversight over data protection in individual member states to give specific attention to public awareness activities that are addressed specifically to children. The European Data Protection Board (EDPB), which is tasked with ensuring that the GDPR is applied consistently across the EU, has announced the preparation of guidelines on children's data.

50. Finally Article 40, which requires member states and supervisory authorities to encourage the drawing up of codes of conduct to contribute to the proper application of the provisions in the GDPR, makes specific reference to children:

[128] See also Recital 58, which deals with transparency and emphasises that 'any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand'.

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained.

51. The protections in the GDPR are supplemented in some jurisdictions by domestic regulations. In the UK, for example, the ICO has developed the Age Appropriate Design Code.[129] Under the code, platforms and service providers need to put the interests of child users at the centre of the design process. The advantage of this approach over a pure notice and consent model is that it seeks to address the attendant risks to personal privacy at the design stage, rather than relying on the consent of children or their parents.

52. The Code applies to 'information society services' that are 'likely' to be accessed by children. It defines a child as anyone under the age of 18 but requires age-based application; i.e. taking a risk-based approach to recognise the age of the user and apply the standards of the Code effectively to children.

53. The 15 standards in the Code are centred on the principle that the best interests of the child should be the primary consideration when designing and developing apps, games, connected toys/devices and websites that are likely to be accessed by children. They cover a range of matters, including default settings; they require that settings are set by default to 'high privacy' and that options for profiling and collection of geolocation should be set to 'off'. They also require the collection and retention of only the minimum amount of data needed to provide a service and that children's data should not be shared unless a compelling reason can be demonstrated for doing so, taking into account the best interests of the child.

54. Consistently with the requirement in Article 12 of the UN Convention on the Rights of the Child, the involvement of children and young people was a critical component in the consultations leading to the development of the UK code. This ensured that their views were properly represented in the design of protections aimed at them and these protections were relevant to their needs.

55. The Irish Data Protection Commissioner has also engaged in extensive public consultation as a preliminary step to development of a new Irish code. This reform process has resulted in a report that identifies four key issues as being of concern to children and young people across all age groups. The first was simplicity; i.e. a desire for more child friendly communications. A second, closely related concern was transparency; the report identified that they 'asked for more detail on how their data is processed and, in particular, on the risks of giving companies access to their data'.[130] A further concern related to accessibility; 'Children felt that companies should be easier to contact and should do more to reach out to and inform them about their processing

[129] See Information Commissioner's Office, *Age Appropriate Design Code* (2 September 2020).
[130] Data Protection Commission of Ireland, 'SOME STUFF YOU JUST WANT TO KEEP PRIVATE!': Preliminary report on Stream II of the DPC's public consultation on the processing of children's personal data and the rights of children as data subjects under the GDPR (Report, July 2019), <https://www.dataprotection.ie/sites/default/files/uploads/2019-08/Some Stuff You Just Want to Keep Private_Consultation Report.pdf>

activities'.[131] The final concern related greater flexibility in their interactions with companies; they desired 'more freedom to restrict the amount of personal data they are obliged to disclose about themselves in order to use their preferred apps and service' and also felt that it should be easier to opt out 'of data collection without losing access to the service'.[132]

ACCC's Reform Recommendations

56. The Castan Centre broadly welcomes the ACCC's recommendations with regard to the enactment of privacy protections specific to children in its 2019 *Digital Platforms Report*.

57. The ACCC has rightly recognised that the risks associated with data collection and use could be particularly acute for children,[133] and that younger children, as a group of consumers, may lack the requisite technical, critical and social skills to engage with the internet in a safe and beneficial manner.[134]

58. The ACCC has made recommendations for the immediate reform of the *Privacy Act*, including a call to strengthen notice and consent requirements with regard to children. In particular, Recommendation 16(b) calls for the amendment of notice obligations in APP5 to require notices to consumers to be 'concise, transparent, intelligible and easily accessible, written in clear and plain language, provided free of charge, and clearly set out how the APP entity will collect, use and disclose the consumer's personal information'. It further recommends in respect of children that:

> *'Where the personal information of children is collected, the notice should be written at a level that can be readily understood by the minimum age of the permitted digital platform user'.*[135]

The thrust of this recommendation is commendable as it enhances transparency and the opportunities for young people to become informed agents in privacy matters.

59. However, the difficulty arises in the *implementation* of these recommendations. The ACCC acknowledges that the more elaborate notification requirements it recommends have the potential to add to the 'information burden' on consumers.[136] Indeed, research suggests that many consumers do not currently read privacy policies or terms of services, and it is likely that more detailed privacy notices may aggravate this problem.[137]

---

[131] Ibid.
[132] Ibid.
[133] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (2019) 447.
[134] Ibid 448.
[135] Ibid 461.
[136] Ibid 463.
[137] See, eg, Consumer Policy Research Centre, *Research: Australian consumers 'soft targets' in Big Data economy* (2018) <https://cprc.org.au/2018/05/13/research-australian-consumers-soft-targets-big-data-economy/>.

60. To address this issue, the Digital Platforms Report suggests a number of countermeasures, including multi-layered privacy notices or the use of standardised wording for particular categories of data or categories of third parties to whom personal information may be disclosed.[138] However, in response to these recommendations, Facebook also questions how these requirements sit with its practice of providing 'regular contextual privacy notices, reminders, and check-up prompts throughout the consumer's experience'.[139]

61. While useful, these countermeasures do little to address the widely-accepted weaknesses of a consent-based model. Critics of the 'notice and consent' model argue persuasively that it has been relied upon too extensively and that consent provides formal justification for a number of questionable data practices. It has been noted that many consumers do not have the time, inclination or literacy to read lengthy privacy notices. An undue number of privacy notices leads to consent fatigue and ultimately makes consumers more disengaged. In many circumstances, consumers have very limited choices, because a service or functionality is offered with a particular privacy setting only on a 'take it or leave it' basis. Many of these criticisms are not confined to young people, but rather concern all consumers. However, some of these dangers are heightened in the case of children.

62. The weakness of the 'notice and consent' approach as a justification for data processing should be countered with more substantive regulation of allowed and disallowed practices. However, academic Daniel Susser makes the important point that this does not mean that the notice component should similarly be scaled back.[140] Privacy policies remain an important instrument to inform consumers of the uses that their personal information is put to and therefore important for transparency. Against this background therefore, the ACCC's recommendation that notice requirements in Australian privacy law should be strengthened is welcomed.

63. Recommendation 16(c), relating to strengthening consent requirements and pro-consumer defaults, has a number of prongs. First, it seeks to expand the circumstances in which consumer consent is required. It is recommended that consent will be needed for every collection, use or disclosure of personal information, unless the personal information is necessary for the performance of a contract with the consumer, or is required by law or otherwise necessary for an overriding public interest reason. In alignment with the GDPR, this broadens the range of circumstances in which consent must be provided. However, unlike under the GDPR, the 'legitimate interests' of the data controller are not a sufficient legal basis for data processing.

64. Second, it strengthens the conditions for valid consent by providing that it must be 'a clear affirmative act that is freely given, specific, unambiguous and informed'.[141] Adopting similar requirements contained in the GDPR and in Convention 108+,[142] this

[138] ACCC, p. 463.
[139] Facebook Australia, Submission to the ACCC *Digital Platforms Inquiry* (3 March 2019) 108.
[140] Daniel Susser, 'Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't' (2019) 9 *Journal of Information Policy* 148.
[141] GDPR, Art 4(1).
[142] *Convention 108+*, art 5(2).

means that any settings for data practices relying on consent must be pre-selected to 'off' and that different purposes of data collection, use or disclosure must not be bundled. Both these recommendations are welcome updates to the *Privacy Act*, which would align Australia's *Privacy Act* more closely with recent European standards.

65. Recommendation 16(c) further proposes in respect of children that:

> *'Where the personal information of children is collected, consents to collect the personal information of children must be obtained from the child's guardian.'*

This suggestion deals with the issue that digital platforms are also often used by children who may *lack the capacity* to give informed consent.

66. While the aim of the recommendation is laudable, it appears that the recommendation is truncated. Taken literally, it would require the obtaining of the guardian's consent whenever the personal information of children is collected. This would be a retrograde step for teenage children who, because of their age, experience and understanding, have already developed the capacity to give consent. In line with current law and the practice in the EU and US, it is more appropriate to require the guardian's consent only in the case of younger children who lack capacity. As explained above, this approach is more supportive of children's developing ability to make informed privacy choices and is preferable from a child's rights perspective because it enhances and supports children's participation in matters affecting them.

67. In Recommendation 18 the ACCC recommends more targeted regulation of the data practices of digital platforms via an enforceable code of practice developed by the OAIC, in consultation with industry stakeholders. Suggested matters for inclusion in this code detailed in Recommendation 18 include:

> *'[R]equirements to provide consumers with specific, opt-in controls for any data collection that is for a purpose other than the purpose of supplying the core consumer-facing service and, where consents relate to the collection of children's personal information, additional requirements to verify that consent is given or authorised by the child's guardian; and*
>
> *additional restrictions on the collection, use or disclosure of children's personal information for targeted advertising or online profiling purposes and requirements to minimise the collection, use and disclosure of children's personal information'.*

68. The first of these follows logically from Recommendation 16(c), but verification is itself potentially problematic because it raises separate privacy issues and it is important to ensure that such measures contain sufficient safeguards to protect information provided solely for verification purposes. The second lacks sufficient detail to permit a detailed analysis. However, it provides scope for inclusion of some of the additional protections available under the GDPR.

Our Recommendations

69. As argued above, there is a good case for amending the *Privacy Act* to better protect the personal data of children in the online commercial context.

70. Insights from the US and EU examples make clear that data controllers need to be mindful of children's special vulnerabilities and design their data handling practices accordingly. This applies across a range of data handling activities, including privacy notices, seeking consent, use and disclosure of personal data, access, correction and erasure rights. While the exact requirements on data handlers are not always defined, children enjoy better protection under European law than under US law.

71. The ACCC's recommendations either embody, or provide scope for embodying, all of these features other than a right to request deletion of data. They also provide scope to address the key issues identified in Ireland as being of concern to children.

72. The recommendations for immediate amendments to the *Privacy Act* address the issue of child-friendly notices and also that of younger children lacking the ability to give informed consent. However, insofar as the latter is concerned, there is no discussion of appropriate age limits. In our view these should be set at somewhere between 13 and 16 after appropriate consultations with children and experts in development studies.

73. The further recommendations for a Code in Recommendation 18 would provide scope for inclusion of key features of the UK's age-appropriate design code, thereby addressing children's desire for increased transparency, accessibility and flexibility in their dealings with online service providers. As discussed above a key strength of this approach is that obviates problematic reliance on notice and consent requirements.

74. The only missing element in our view is a recommendation concerning the inclusion in the APPs of a specific right of deletion of data volunteered to an online collector. This would serve as a useful backstop given that the deletion of data goes a long way to resolving the privacy issues associated with its collection.

PART FIVE: DIRECT RIGHTS OF ACTION TO ENFORCE PRIVACY OBLIGATIONS

5.1 Enforcement powers under the Privacy Act and role of the OAIC

Question 53: Is the current enforcement framework for interferences with privacy working effectively?

75. Our submission on this question is limited to one particular aspect, the role of the Privacy Commissioner should have in investigating allegations of a serious invasion of privacy under the proposed statutory tort.

76. A person alleging a breach of their privacy rights under the *Privacy Act* can complain to the OAIC. The Privacy Commissioner is required to investigate a complaint if the act or practice in question may be an interference with the complainant's privacy and the complainant has first complained to the respondent. The term 'interference with privacy' has a limited and technical meaning. It is defined in s 13 of the *Privacy Act*, amongst other things, as an act or practice that breaches an Australian Privacy Principle (APP) or an applicable registered APP code.

77. When an act to which the *Privacy Act* applies constitutes an interference with privacy, the Commissioner has the power to make determinations under s 52. This power is not an unfettered discretion to grant the remedy that best fits the circumstances or that best redresses the harm; it is a power limited to the making of a number of specific declarations.

ALRC Recommendations

78. In its 2014 Report on serious invasions of privacy in the digital era, the ALRC recommended that consideration be given to making the complaints process available for alleged breaches of the proposed statutory privacy tort.[143]

79. The ALRC asked the Government to give consideration to extending the Privacy Commissioner's powers so that the Commissioner could investigate complaints about serious invasions of privacy and make appropriate declarations, which would then require enforcement by the Court.[144] This recommendation was intended to improve access to justice by utilising an established complaints process and to give the Commissioner greater visibility and responsibility in addressing privacy harms.

Our Recommendation

We submit that this recommendation of the ALRC be adopted.

[143] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014) Rec 16-1.
[144] Ibid.

5.2 Direct Right of Action

Question 56: How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

80. In the Final Report of the Digital Platform Inquiry, the Australian Competition and Consumer Commission ('ACCC') recommends the introduction of a direct right to bring actions and class actions under the *Privacy Act*.[145] The ACCC argues that this right 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*.[146]

81. In addition to giving the law greater effectiveness, the ACCC also expects that a greater role for courts in the enforcement of privacy rights would add to clarity and certainty and bring Australia in line with overseas jurisdictions, including the European Union and New Zealand, which grant direct rights.[147] A private right of action is also contained in the Canadian bill for a new Consumer Privacy Protection Act.[148]

82. We submit that this recommendation, which the government supports in principle, should be enacted. 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.[149]

83. The objection that it is unnecessary to have two avenues of redress[150] is not well-founded. While there may indeed be overlap between a statutory tort of serious invasion of privacy and the direct claim right under the *Privacy Act*, there are a range of situations in which only one or the other right would apply. In its report, the ACCC lists instances in which the *Privacy Act* does not apply to a particular invasion of privacy, such as when conduct interferes with spatial or physical privacy, or when one of the many exemptions applies, such as exemption for an individual's personal, family or household affairs,[151] the exemption for small business,[152] the exemption for

[145] Australian Competition and Consumer Commission, *Digital Platforms Inquiry,* Final Report (2019), Recommendation 16(e).
[146] Ibid, p. 473.
[147] *General Data Protection Regulation* (EU), art. 82(1); *Privacy Act 1993* (NZ), s 88.
[148] A privacy tort for Australia? A critical appreciation of the ALRC report on serious invasions of privacy' (2015) 12 *Privacy Law Bulletin* 106.
[149] 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>.
[150] See, eg, Facebook, Facebook's response to the Digital Platforms Inquiry (September 2019), <https://fbnewsroomus.files.wordpress.com/2019/09/facebook-submission-to-treasury-on-digital-platforms-inquiry.pdf>, pp. 121–2.
[151] *Privacy Act 1988* (Cth), s 7B(1).
[152] *Privacy Act 1988* (Cth), s 6C(1), 6D.

practices in the course of journalism[153] or the exemption for political acts or parties.[154]

84. Conversely, the statutory cause of action for serious invasion of privacy would not be available for all interferences with privacy under the *Privacy Act*, because an interference may not be sufficiently 'serious', may not be 'intentional or reckless' (if - contrary to our submission - this fault standard was enacted) or does not constitute an 'misuse of personal information' as defined under the Act. This may, for example, be the case where an organisation or agency has committed a negligent breach of the APPs, such as when it carelessly fails to adopt state-of-the-art protocol for securing personal information. The two causes of action are therefore complementary and should both be introduced.

85. We submit that access to the direct act of action should not be curtailed by threshold mechanisms. The objectives pursued with a direct right of action identified above would be best achieved if access to the court was unfettered. It is unlikely that the direct right of access to the court would be abused 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. Requiring that a complaint must first undergo conciliation by the OAIC or some other administrative 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 only indirect. Furthermore, many courts, including the Federal 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.

86. In our view, there is also no need to put a cap on the amount of damages available. Damages under the Act are compensatory, which means that the amount of damages awarded would be commensurate with losses suffered. The existing body of determinations issued by the Privacy Commissioner suggests that compensation under the Act is assessed quite moderately, probably too modestly.[155] Any cap on damages would therefore have the effect of leaving a plaintiff who has suffered an extraordinarily large loss to be partially uncompensated. However, if a cap was introduced, consideration would also need to be given to its effect on class actions. A cap could apply per claim or per loss-causing event. If the cap were to apply to the loss-causing event (such as a data breach) regardless of the number of individuals affected, it would protect a defendant but would create a disincentive to bringing class actions in cases affecting a very large class. We submit that, overall, the disadvantages of caps would outweigh their potential benefits.

---

[153] *Privacy Act 1988* (Cth), s 7B(4).
[154] *Privacy Act 1988* (Cth), s 7C.
[155] 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), p 377.

87. The direct rights of action provisions in other jurisdictions, such as Canada, New Zealand and the EU, also do not contain particular limitations on access or caps on damages.

PART SIX: STATUTORY TORT FOR SERIOUS INVASIONS OF PRIVACY

6.1 Statutory Tort

Question 57: Is a statutory tort for invasion of privacy needed?

88. At present, victims of privacy invasions in Australia have access to judicial remedies only if existing causes of action, such as trespass, nuisance or breach of confidence, incidentally provide protection. Nearly 20 years have passed since the High Court declared in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*[156] 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*.[157] Yet, despite this assurance, no Australian appellate court has to date seen fit to recognise the existence of a privacy tort.

89. 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*.[158] 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.[159] 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 personal confidence can include an award to compensate for non-pecuniary harm, in particular injury to feelings.[160]

90. Where the alleged privacy invasion involves information handling, the victim can also lodge a complaint with the OAIC, provided that the alleged privacy invasion constitutes a breach of the *Privacy Act 1988* (Cth). On receiving a complaint, the Privacy Commissioner will consider whether to investigate the matter and, if he does and regards the complaint as well-founded, will usually seek to resolve it through conciliation. The Commissioner also has the power to make formal decisions, which can include orders to apologise, pay compensation or change privacy practices, but such determinations are rare. On the whole, the redress available under the *Privacy Act* is in many respects limited.

91. A statutory right to privacy, actionable in tort law, would not supplant the existing redress mechanism, but fill the current gaps in the protection of privacy interests and

[156] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [2001] HCA 63.
[157] (2020) 376 ALR 575, [2020] HCA 14, [86]–[87] (Kiefel CJ, Bell J, Keane J); [244] (Edelman J).
[158] *Giller v Procopets* (2008) 24 VR 1, [2008] VSCA 236.
[159] Ibid, at [167]–[168] (Ashley JA) and [447]–[452] (Neave JA, Maxwell P agreeing).
[160] The plaintiff was awarded $50,000 damages (including aggravated damages) for mental distress.

provide suitable remedies to victims of privacy invasion, including damages and injunctions.

Privacy not adequately covered by other causes of action

92. Despite the above mentioned 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 bypassed if a specific privacy tort was recognised or enacted.

93. 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.[161]

94. 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.[162]

95. 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.[163] 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*.[164] Despite the relative dearth of Australian authority on the issue, it is likely that the

[161] *Moorgate Tobacco Co Ltd v Philip Morris Ltd (No 2)* (1984) 156 CLR 414, 438 (Gibbs CJ, Mason, Wilson, Deane and Dawson JJ).
[162] *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.
[163] [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'.
[164] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [2001] HCA 63, Gleeson CJ at [36]; see also Gummow and Hayne JJ at [101]; *Wilson v Ferguson* [2015] WASC 15. See further discussion in *Smethurst v Commissioner of Police* [2020] HCA 14.

approach signalled by Lord Goff may prevail,[165] 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 as 'surreptitious or improper' obtaining.

96. However, a statutory tort would mean that the law of confidence no longer needs to be 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.[166]

97. 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,[167] or constitute a criminal offence under surveillance legislation[168] or so-called 'upskirting' laws in some jurisdictions,[169] but the protection offered by these mechanisms remains ad hoc and is likely to leave some gaps.[170]

---

[165] Lord Goff's 'broad principle' was cited with approval in *Streetscape Projects (Australia) Pty Ltd v City of Sydney* (2013) 85 NSWLR 196, [2013] NSWCA 2, [155] (Barrett JA, Meagher and Ward JJA agreeing).

[166] In *PJS v News Group Newspapers Ltd* [2016] AC 1081, [2016] UKSC 26, 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 (at [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 (at [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: at [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.

[167] 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] 2 WLR 1081, [2020] EWCA Civ 104.

[168] *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).

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

[170] Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era, Final Report, ALRC Report 123 (2014) Ch. 3.

98. There also remains uncertainty about the available defences and the availability of compensation for mental distress. For example, it is unclear whether Australian law recognises a public interest defence that is separate from the traditional iniquity defence, and in what circumstances these defences apply.[171] 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,[172] that it was available under the Victorian version[173] of Lord Cairns' Act.[174] While this decision provided suitable relief to the plaintiff,[175] some commentators continue to doubt that this remedy should be available.[176] 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.[177]

Judicial Reluctance to Recognise a Common Law Right to Privacy

99. A statutory privacy tort would help overcome the reluctance of Australian courts to recognise a right to privacy and ensure that Australia's privacy protection no longer lags behind its counterparts in other common law jurisdictions. Australia is now virtually unique among major common law jurisdictions in not recognising a legally enforceable right to privacy.

100. In the majority of comparable jurisdictions, privacy protections have been developed through the courts. This has been the case in the United Kingdom, New Zealand and, to some extent, in Canada. In all these countries, 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. In Australia, however, the absence of a federal human rights instrument

---

[171] See discussion in *Australian Football League v Age Company* Ltd [2006] VSC 308.
[172] *Giller v Procopet*s (2008) 24 VR 1, [2008] VSCA 236, Neave JA, with whom Maxwell JA agreed; Ashley JA dissenting.
[173] *Supreme Court Act 1986* (Vic) s 38.
[174] *Chancery Amendment Act 1858*, 21 & 22 Vict, c 27.
[175] 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.
[176] 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 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) 165, 166–173 for further discussion.
[177] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Final Report, ALRC Report 123 (2014) Rec. 13-1.

has stultified the development of a common law right to privacy. It is that gap in the law that the proposed statutory privacy tort would close.

101. The courts in other common law jurisdictions have taken a much more active role in the recognition of privacy wrongs. The courts in the USA have for many years accepted the existence of several privacy torts. In the classification of the *Restatement on Torts* (2nd),[178] which in turn accepted the classification by American torts scholar, Professor Dean Prosser, they are:

a) Intrusion upon the plaintiff's seclusion or solitude into his private affairs.
b) Public disclosure of embarrassing private facts about the plaintiff.
c) Publicity which places the plaintiff in a false light in the public eye.
d) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[179]

Equally, the UK, NZ and Canada have left Australia behind in this area and enhanced the protection of privacy at common law. The prime example for the assistance that a human right of privacy can provide for the development of domestic law is the United Kingdom. The *Human Rights Act 1998* (UK) was intended to give the provisions of the European Convention on Human Rights domestic effect. Soon after the Act came into force in 2000, the courts responded to the new environment by enhancing privacy protection at general law.[180] Initially, they expanded the traditional action for breach of confidence, and then – after the decision in *Campbell v MGN* by the House of Lords – they expressly acknowledged the existence of a new tort of misuse of private information.[181] This tort is now well-accepted in the UK, but still maintains its close links with the rights afforded under the European Convention on Human Rights, as is particularly evident from the elements of this tort, which is establish in a two-stage enquiry:

a) If a claimant can establish a reasonable expectation of privacy then the right to respect for private life in art. 8 of the ECHR is 'engaged' and the first hurdle in the misuse of private information action is cleared.
b) In the second stage, it is then up to the defendant to show that that right is outweighed by some other interest, usually the right to freedom of expression guaranteed by art. 10 of the ECHR.[182]

102. The situation in New Zealand and Canada is comparable, although the path to recognition of a privacy tort was somewhat different. In both jurisdictions, the effect of human rights law was more indirect because neither the *Canadian Charter of Rights and Freedoms* nor the *New Zealand Bill of Rights Act 1990* contain a broad right to

[178] American Law Institute, *Restatement of the Law (Second) of Torts* (1977) § 652A.
[179] William L Prosser, 'Privacy' (1960) 48 *California Law Review* 383, 389.
[180] *Douglas v Hello! Ltd* [2001] QB 967, [2005] EWCA Civ 595.
[181] *Campbell v MGN Ltd* [2004] 2 AC 457, [2004] UKHL 22.
[182] *McKennitt v Ash* [2008] QB 73, [2006] EWCA Civ 1714. See also *PJS v News Group Newspapers Ltd* [2016] AC 1081, [2016] UKSC 26.

respect for private life, as under European human rights law or the International Covenant on Civil and Political Rights (ICCPR). Instead, these instruments provide more limited protection against 'unreasonable search and seizure'.[183] The human rights framework was nonetheless an important driver of law reform. In Canada, four provinces had already established a statutory privacy tort[184] when, in 2012, the Ontario Court of Appeal recognised in *Jones v Tsige* the tort of intrusion into seclusion.[185] In subsequent cases, the Ontario Superior Court of Justice recognised, for the first time in Canada, the privacy tort of 'publication of embarrassing private facts' (2016)[186] and the 'false light' privacy tort (2019).[187]

103. The New Zealand *Bill of Rights Act 1990* also does not explicitly recognise a right to privacy, but merely a right to be secure against unreasonable search and seizure. Nonetheless, the New Zealand Court of Appeal engaged in a detailed analysis of the human rights context, when it recognised, in *Hosking v Runting*,[188] the existence of a cause of action protecting in relation to publicising private information. In 2012, the New Zealand High Court further developed the law when it accepted, for the first time, the existence of a tort against privacy intrusion in the case of *C v Holland*.[189]

104. Australia has the disadvantage that it does not have a constitutional bill of rights at federal level, but only state and territory human rights legislation in the ACT, Victoria and now Queensland.[190] Australia, like most countries, is a signatory of the ICCPR, which in its art. 17 imposes on state parties an obligation to protect everyone against arbitrary or unlawful interference with their privacy, family, home or correspondence. However, the ICCPR does not form part of domestic Australian law. While the High Court has held that statutory interpretation must 'favour construction [of legislation] which is in conformity and not in conflict with Australia's international obligations',[191] there is little overt influence of international human rights obligations on the Australian common law. More generally, Australian courts also express discomfort at the prospect of recognising relatively high level concepts as the basis of new rights. This is apparent

[183] *Canadian Charter of Rights and Freedoms*, s 8*; New Zealand Bill of Rights Act 1990*, s 21.
[184] British Columbia: *Privacy Act* RSBC 1996, c 373, s 1; Saskatchewan: *Privacy Act* RSS 1978, c P-24, s 2; Newfoundland: *Privacy Act* RSNL 1990, c P-22, s 3; and Manitoba: *Privacy Act* CCSM 1987, c P125.
[185] *Jones v Tsige* (2012) 108 OR (3d) 241, [2012] ONCA 32. For further discussion, see Jeff Berryman, 'Remedies for Breach of Privacy in Canada', in Jason N E Varuhas and Nicole A Moreham (eds), *Remedies for Breach of Privacy* (Oxford: Hart Publishing, 2018), p. 323.
[186] *Jane Doe 464533 v ND* (2016) 128 OR (3d) 352, 2016 ONSC 541; see also *Jane Doe 72511 v N.M.*, [2018] O.J. No. 5741, 2018 ONSC 6607.
[187] *Yenovkian v Gulian*, 2019 ONSC 7279.
[188] *Hosking v Runting* [2005] 1 NZLR 1, [2004] NZCA 34.
[189] *C v Holland* [2012] NZHC 2155. For further discussion, see Chris DL Hunt, 'New Zealand's New Privacy Tort in Comparative Perspective' (2013) 13 *Oxford University Commonwealth Law Journal* 157.
[190] *Human Rights Act 2019* (Qld); *Charter of Human Rights and Responsibilities Act 2006* (Vic); *Human Rights Act 2004* (ACT).
[191] *Minister for Immigration and Ethnic Affairs v Teoh* (1995) 183 CLR 273 at 287 (Mason CJ and Deane J); *Plaintiff M70/2011 v Minister for Immigration and Citizenship* (2011) 244 CLR 144, [2011] HCA 32, [247] (Kiefel J).

not only in the context of privacy but, for example, also from the reluctance of embracing concepts such as unjust enrichment[192] or good faith in contract law.[193]

105. The absence of a federal human rights instrument in Australia has stultified the development of a common law right to privacy. It is that gap in the law that the proposed statutory privacy tort would close.

Improving Access to Justice

106. The long history of courts avoiding a decision on a common law right to privacy has made plaintiffs with a privacy claim reluctant to argue for the recognition of such a right. The recent decision of the High Court in *Smethurst v Commissioner of Police* exemplifies the issue.[194] In this case, a journalist successfully argued that a warrant for the search of her home by the Australian Federal Police was invalid, but a majority of the Court refused to grant her a mandatory injunction for the destruction or delivery up of material obtained under the invalid warrant. In her application, Ms Smethurst did not bas her claim on a common law right to privacy,[195] which allowed the Court again to sidestep a decision on the existence of such a right.[196] Instead, Ms Smethurst relied upon privacy in an indirect manner by arguing (unsuccessfully) that the mandatory injunction was required in order to reverse the consequential effect on her privacy of the tort of trespass to chattels that was committed by the Australian Federal Police. That submission was considered by Kiefel CJ, Bell J and Keane J, and accepted by Edelman J, but not discussed in the other judgments. Given that the case for recognition of a common law right to privacy was not argued, it is understandable that the High Court did not engage further with that issue. However, the case illustrates that plaintiffs consider arguments in favour of a common law right as a risky strategy and seek to rely on other avenues of redress where available, or plead a right to privacy in the 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.

The Relationship with Criminal Law

---

[192] *Mann v Paterson Constructions Pty Ltd* (2019) 93 ALJR 1164; [2019] HCA 32, [79] (Gageler J), [119] (Nettle, Gordon, Edelman JJ); *Roxborough v Rothmans of Pall Mall Australia Ltd* (2001) 208 CLR 516, 543–544 ([71]–[73]) (Gummow J).

[193] The High Court has so far left open whether a general obligation to act in good faith in the performance of contracts should be recognised: *Commonwealth Bank of Australia v Barker* (2014) 253 CLR 169, [2014] HCA 32; see also Jeannie M Paterson, 'Good Faith Duties in Contract Performance' (2014) 14 *Oxford University Commonwealth Law Journal* 283.

[194] *Smethurst v Commissioner of Police* [2020] HCA 14.

[195] *Smethurst v Commissioner of Police* [2020] HCA 14, at [242]–[244] (Edelman J).

[196] *Smethurst v Commissioner of Police* [2020] HCA 14, at [197] (Gordon J), at [242]–[244] (Edelman J).

107. The Issues Paper refers to a range of new criminal law offences in Commonwealth, state and territory legislation that focus image-based abuse as well as voyeurism and 'upskirting'.[197] While these provisions do provide protection against some serious invasions of privacy, they are quite limited in scope. They do not apply to serious invasions of privacy in other contexts and should therefore be complemented by a broadly-based privacy tort. The ALRC tort contains a broad range of civil remedies should be available to successful privacy claimants.[198] These include traditional tort remedies such as damages, including compensation for emotional distress, injunctions, an account of profits and – in exceptional cases – an award of exemplary damages. In addition, the report also recommends to give the court the power to make orders that are more specifically directed at remedying privacy harms, such as declarations, orders for apologies and corrections. Most of these plaintiff-focused remedies would not be readily available in criminal law proceedings because criminal law and civil law, despite some overlap, have different objectives. Whereas the criminal law is defendant-focused and its sanctions primarily seek to punish and deter, the remedies in civil law are primarily plaintiff-focused and seek to restore and compensate. While the tort of breach of statutory duty allows enables a right to sue where a defendant has contravened a statute, it is contentious in what circumstances this tort is available where the duty breached was a criminal prohibition.[199]

108. The National Statement of Principles Relating to the Criminalisation of the Non-Consensual Sharing of Intimate Images therefore appropriately acknowledges the importance of 'a variety of responses',[200] including civil recourse, to address the problem of image-based abuse. This holistic approach is also supported in the criminological literature:

> Such offences should complement, and be seen as part of a range of, graduated responses from self-help to public education to the availability of a range of civil legal remedies and existing criminal laws.[201]

Our Recommendations

109. We therefore submit that the existence of criminal law offences for some serious invasions of privacy resulting from image-based abuse, voyeurism and 'upskirting' does not obviate the need for a statutory privacy tort.

---

[197] Australian Government, Attorney-General's Department, *Privacy Act Review*, Issues Paper (October 2020), p 71.
[198] Ibid, Ch. 12.
[199] *Jane Doe v Fairfax Media Publications Pty Ltd* [2018] NSWSC 1996 (no private claim in tort for breach of statutory duty arising from contravention of Crimes Act 1900 (NSW) s 578A by publication of material that identified a rape victim).
[200] Law, Crime and Community Safety Council, *National Statement of Principles Relating to the Criminalisation of the Non-Consensual Sharing of Intimate Images* (2017) p 2.
[201] Tyrone Kirchengast and Thomas Crofts, 'The legal and policy contexts of 'revenge porn' criminalisation: the need for multiple approaches (2019) 19(1) *Oxford University Commonwealth Law Journal* 1, 3, DOI: 10.1080/14729342.2019.1580518.

110. The preceding discussion demonstrates that, despite the existing protections of privacy at general and statute law, there is an unmet need for a privacy tort. This view also coincides with the weight of submissions to the inquiries who expressed valid concerns about increasing threats to privacy and favoured the introduction of a tort. In the most recent Australian Community Attitudes to Privacy Survey 2020, there was also overwhelming support for the right to seek compensation in the courts for a breach of privacy.[202]

111. We support the ALRC's proposals for a statutory cause of action, as well as similar calls for law reform made by the ACCC and AHRC. In July 2019, 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 ALRC in 2014.[203] In December 2019, in the context of its ongoing inquiry into Human Rights and Technology, the Australian Human Rights Commission (AHRC) also proposed that this ALRC recommendation be implemented.[204] Although both Commissions made their proposals in different contexts, their respective calls for legislative action responds to the common threat that the rise of modern data-driven technology poses for individual privacy.

112. We also recognise that while the ALRC proposal has many strengths, it also has a few shortcomings that the future law reform process should still seek to address. We therefore recommend that the proposal to limit the tort to intentional and reckless invasions of privacy also extend to include fault-based invasions of privacy. [**See below]**

113. We further submit that the general tort of serious invasion of privacy should be complemented by a direct right of action under the *Privacy Act* [See above]. This would give individuals greater protection and control if their statutory information privacy rights are interfered with.

Question 58: Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?

114. We submit that a statutory privacy tort would substantially expand the redress available to victims of privacy invasion. As explained above, criminal law and a statutory tort are complementary responses. They have different functions and objectives, and are both needed.

115. The comparative review into the law of other Commonwealth jurisdictions also supports the position that these two regulatory approaches are not alternatives. Canada, New Zealand, the UK and the USA all have statutory or common law privacy

[202] Office of the Australian Information Commissioner and Lonergan, *Australian Community Attitudes to Privacy Survey 2020* (September 2020) p 67.
[203] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital* Era (Report 123, 2014).
[204] Australian Human Rights Commission, *Human Rights and Technology* (Discussion Paper, December 2019), Proposal 4 (p. 92).

torts. The introduction of the proposed cause of action would ensure that Australia's privacy protection in that regard no longer lags behind internationally accepted standards. The proposed elements of the cause of action do not differ greatly from their counterparts in other common law jurisdictions, but where they do, they tend to define the tort somewhat more tightly than elsewhere.

116. 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.

117. The alternative – also considered in the ALRC report – would be to leave the development of the law completely in the hands of judges. That approach would create more uncertainty and higher costs to litigants, 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.

Question 59: What types of invasions of privacy should be covered by a statutory tort?

118. ALRC Report 123 provides a careful analysis of the need for a statutory action to protect privacy. The recommendations of the ALRC are the result of extensive community consultation and take into account comparative research into the law in other jurisdictions. We submit therefore that the ALRC recommendations for a statutory privacy tort serves as a useful starting point for development of a statutory tort.

119. ALRC's recommendations, the tort should focus on the following types of invasion of privacy: 'intrusion into seclusion' and 'misuse of private information'.

120. **Intrusion** includes activities such as physically intruding into the plaintiff's private space or by watching, listening to or recording the plaintiff's private activities or private affairs. A **misuse** of private information occurs by activities such as collecting or disclosing private information about the plaintiff.

121. 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'.[205] We submit however that the ALRC formulated some of the elements of the cause of action too narrowly.

122. A regards types of invasion of privacy included in the tort, we submit that a *broad* formulation of the cause of action that provides redress against all presently recognised forms of privacy infringement and allows for future development of the law by the courts if and when new forms of privacy infringement arise, is preferable.[206]

---

[205] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014) [5.76].

[206] Reasons for this are detailed in Normann Witzleb, Submission No. 116 to ALRC Discussion Paper 80 <https://www.alrc.gov.au/sites/default/files/subs/116._n_witzleb.pdf>.The present submission reproduces some of the material of the ALRC submission.

123. This stands in contrast to the recommendation made by the ALRC in Report 123, which proposes to 'confine'[207] the cause of action to the categories of 'intrusion' and 'misuse/disclosure'. Specifically, the proposed tort is –

> *'not designed to capture the two other so-called "privacy torts" in the United States, namely, "publicity which places the plaintiff in a false light in the public eye" and "appropriation, for the defendant's advantage, of the plaintiff's name or likeness"*.[208]

At the same time, ALRC Report 123 suggests:

> *'The tort in this Report is certainly not designed to deny relief where the plaintiff has been put in a false light, or had their name or likeness appropriated. But it is not intended to capture these other wrongs per se. Other causes of action will more directly relate to these wrongs*'.[209]

124. Our concern is that an approach that relies on the *incidental* protection of privacy interests through other causes of action carries the risk that some privacy invasions may go unremedied.

125. The cause of action proposed by the ALRC appears to provide incidental protection where a false light or appropriation claim can (also) be subsumed under the 'intrusion' or 'misuse/disclosure' labels. In relation to the 'false light tort', this follows from recommendation 5-2 that 'private information' includes untrue information, but only if the information would be private if it were true'.

126. We therefore recommend the extension of the cause of action to also include **'false privacy'** claims because the misuse or disclosure of untrue private information can be just as damaging as the misuse or disclosure of true private information. There is no reason to limit the protection to true information. Limiting the tort to true information would require a plaintiff to confirm or admit in court the veracity of information which she would not like to see in the public domain, at all. This would be likely to unfairly prejudice the plaintiff's interests in protecting her private life from publicity.

127. Not requiring the plaintiff to establish the truth of the information disclosed or misused is also in line with the law in other jurisdictions, most notably the UK. In *McKennitt v Ash*,[210] the defendant argued that the plaintiff could not have a reasonable expectation of privacy in relation to false statements. The Court of Appeal rejected this argument. Longmore L.J. stated:

> *The question in a case of misuse of private information is whether the information is private, not whether it is true or false. The truth or falsity is an*

[207] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014), [1.4].
[208] Ibid, [5.67].
[209] Ibid, [5.70].
[210] *McKennitt v Ash* [2008] QB 73; [2006] EWCA Civ 1714.

> *irrelevant inquiry in deciding whether the information is entitled to be protected*.[211]

128. While it is appropriate that the proposed cause of action would provide redress for conduct involving untrue information relating to a person's private life, this raises some doubt in relation to the ALRC's declared preference not to include 'false light' wrongs in the statutory tort.

129. Similar concerns arise in relation to the '**misappropriation tort**'. While ALRC Report 123 does not wish to deny relief for such wrongs, it does not clarify in what circumstances the appropriation of a plaintiff's name, image or other characteristics would constitute a 'misuse'. The ALRC explains the reluctance to legislate for misappropriation wrongs with the following consideration stated by Gummow and Hayne JJ stated in *ABC v Lenah Game Meats Pty Ltd*:

> *Whilst objection possibly may be taken on non-commercial grounds to the appropriation of the plaintiff's name or likeness, the plaintiff's complaint is likely to be that the defendant has taken the steps complained of for a commercial gain, thereby depriving the plaintiff of the opportunity of commercial exploitation of that name or likeness for the benefit of the plaintiff.*[212]

130. However, whilst misappropriation of a person's name or likeness may often primarily affect commercial and proprietary interests,[213] this is not invariably the case. A recent US-example illustrates the point: Harris Faulkner, a well-known journalist and Fox News anchor has filed a lawsuit against Hasbro, a large toy manufacturer, which sells a hamster doll under the name of Harris Faulkner.[214] The packaging of the hamster warns that it is a choking hazard for young children. According to the suit, the hamster also bears physical resemblance to Faulkner's traditional professional appearance, in particular the tone of its complexion, the shape of its eyes, and the design of its eye makeup. Ms Faulkner seeks damages on the basis that the toy hamster produced by Hasbro wrongfully appropriates her name and distinctive persona. She alleges that she was 'extremely distressed' to have her name attached to a potential choking hazard.

131. In the absence of a broad privacy wrong, an Australian plaintiff would be required to seek protection under the torts of passing off and defamation. The former only protects against commercial losses, but does not protect against the emotional distress and embarrassment arising from an unauthorised use of one's name and likeness. A defamation claim may provide a measure of protection against the loss of reputation but not against the insult of being portrayed as a rodent. Provided the plaintiff can establish the relevant cause of action, her interests should be protected directly

---

[211] Ibid, [86].
[212] *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63, (2001) 208 CLR 199, 255.
[213] These interests are affected when the defendant's conduct prejudices the plaintiff's ability to commercialise aspects of their personality, such as a product endorsement or a paid 'exclusive' on a significant life events.
[214] BBC News, *Fox News anchor Harris Faulkner sues Hasbro over hamster toy* (2 September 2015), available at http://www.bbc.com/news/world-us-canada-34133723.

through tort, rather than incidentally through other causes of action, which do not seem adapted to the specific claim.

132. If a misappropriation were to constitute a misuse, it would presumably be actionable under the general requirements of the proposed tort, i.e. where the plaintiff has a reasonable expectation of privacy in relation to the information in question, where the invasion is serious and where the plaintiff's interest in privacy is not outweighed by the defendant's interest in freedom of expression and any broader public interest.

133. Some of the proposed remedies available for an invasion of privacy, in particular an account of profit and a notional license fee, also indicate that the cause of action intends to target conduct engaged in for financial gain. Both of these gain-based remedies aim at ensuring that a defendant who benefits financially from breaching the plaintiff's privacy will not be able to retain the proceeds of the wrong.

134. In light of the above considerations, we submit that the two branches of the proposed tort *can* be understood as being broad enough to cover conduct that, in the classification of the US Restatement, would fall under the false light and misappropriation torts.

135. For the sake of clarity, however, we submit that it would be useful to state expressly that 'false light' and 'appropriation' claims are not excluded from the ambit of the new tort. These wrongs should be actionable if the defendant's conduct satisfies the elements of the cause of action. The legislation should clarify that 'private information' includes untrue information if the information would be private if it were true. It should further clarify that an 'appropriation of the plaintiff's name, likeness and other characteristics' may constitute a 'misuse' of personal information.

Question 60: Should a statutory tort of privacy apply only to intentional, reckless invasions of privacy or should it also apply to breaches of privacy as a result of negligence or gross negligence?

136. We submit that the statutory tort of privacy should *not* be confined to intentional or reckless invasions of privacy, and that negligent invasions of privacy should also be actionable.

137. In our view, limiting liability to intent and recklessness, as the ALRC recommended in Report 123, would set the *bar too high*. It would leave plaintiffs without redress in some circumstances where they deserve protection. We also submit that the limitation to intentional and reckless privacy invasions 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

138. The case of *Jane Doe v ABC*[215] provides a striking example of why limiting liability to intentional and reckless acts would exclude some deserving cases. In that case, the 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'.[216] 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.

139. 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,[217] 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.[218] 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*.

140. 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

[215] *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.
[216] *Ibid*, [163].
[217] Office of the Australian Information Commissioner, *Data breach notification guide: A guide to handling personal information security breaches* (August 2014) p 2.
[218] 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/>.

a cause of action against serious invasions of privacy which is based on *fault-based* standard, rather than requiring intention or recklessness.219

Coherence with Privacy Law

141. 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.

142. 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',[220] 'reasonably necessary',[221] or based on a 'reasonable belief'.[222] 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.

143. 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'.[223] 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.[224] 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[225] and based on fundamental human interests such as respect for dignity and autonomy.[226] 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.

144. 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

[219] 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 1998* (UK), s 13: *Secretary of State for the Home Department v TLU* [2018] 4 WLR 101, [2018] EWCA Civ 2217.
[220] Eg., APP 1, APP 4, APP 5, APP 8, APP 10, APP 11.
[221] Eg., APP 3, APP 6, APP 8, APP 9.
[222] Eg., APP 3, APP 6, APP 8, APP 12.
[223] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014), [7.63].
[224] See, e.g., *Civil Liability Act 2002* (NSW), s 5B.
[225] See, eg. Article 17 of the International Covenant on Civil and Political Rights.
[226] *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63, 208 CLR 199.

interests do not outweigh the privacy interest of the plaintiff. This provides a sufficient protection to defendants against undue encroachment of their rights and 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

145. 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'.[227] However, it is doubtful whether a privacy invasion would remain actionable under the tort of negligence if a statutory privacy tort were enacted.

146. In *Sullivan v Moody*,[228] 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'.[229] 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'.[230] 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

147. 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.

148. 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*.[231]

[227] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014), [7.50].
[228] *Sullivan v Moody* [2001] HCA 59, 207 CLR 562; see also *Tame v New South Wales* [2002] HCA 35, (2002) 211 CLR 317.
[229] *Sullivan v Moody* [2001] HCA 59, 207 CLR 562, at [54].
[230] Ibid.
[231] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014), [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.*[232]

149. 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.

150. 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,[233] or that publication was justified in light of overriding interests,[234] or – in many cases – both.[235] 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 in which courts were divided[236] or in which first instance decisions were reversed on appeal[237] attest to. 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.

Recommendations by Others

151. In 2016, the NSW Legislative Council Standing Committee on Law and Justice recommended that NSW introduce a statutory privacy tort that should be based largely on the ALRC model,[238] but that consideration be given to 'incorporating a fault element

---

[232] Ibid, [7.35] (citations omitted).
[233] *Murray v Express Newspapers plc* [2008] EWCA Civ 446, [2009] Ch 481.
[234] *AAA v Associated Newspapers Ltd* [2012] EWHC 2103 (QB).
[235] *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.
[236] *Campbell v MGN Ltd* [2004] 2 AC 457.
[237] *Murray v Express Newspapers plc* [2008] EWCA Civ 446, [2009] Ch 481; *ETK v News Group Newspapers Ltd* [2011] EWCA Civ 439.
[238] Parliament of New South Wales, Legislative Council, Standing Committee on Law and Justice, *Remedies for the Serious Invasion of Privacy in New South Wales*, Report (March 2016), Recs. 3 and 4.

of intent, recklessness and negligence for governments and corporations, and a fault element of intent and recklessness for natural persons'.[239]

152. This innovative approach should be further considered in the reform process. Limiting the liability of natural persons to intentional and reckless conduct would mean that an individual would not incur liability if, say, he or she mistakenly encroaches into another's private sphere or thoughtlessly posts on social media photographs depicting friends, family or strangers in embarrassing situations. Differentiating between individuals and corporations and allowing liability for negligence for the latter would ensure that corporations would be held to a higher standard. Corporate actors would remain liable for conduct that fails to comply with a standard of reasonable care. In that way, media organisations would be required to engage in responsible journalism that has proper regard to legitimate claims for privacy. Government entities would incur liability when they fail to put in place reasonable security safeguards to protect private information against unauthorised access or loss.[240]

153. A differentiation between individuals and corporations would also respond to the concern acknowledged by the ALRC that there should be adequate deterrence, and remedies, against privacy invasion by corporate and government entities.[241] With the greater potential of many businesses and governments to commit significant privacy invasions, they should also have greater responsibilities to guard against them. In addition, corporations will often have better resources to ensure (e.g. through training of officers and employees or seeking professional advice) that their practices comply with accepted standards and community expectations on privacy safeguards. Corporations will also generally find it easier to carry the burden of liability for breach, such as through public liability insurance, professional indemnity insurance or pricing mechanisms.

154. The rationale for imposing an intention and recklessness standard is based on the concern of avoiding liability that is too onerous. However, not all remedies are equally invasive. Another possibility is therefore that a future statutory privacy tort restrict a claim for damages against an individual to privacy invasions that are intentional or reckless, whereas all other remedies are available whenever the defendant – whether an individual or a corporate or government entity – acted (at least) with negligence. For example, if an individual was merely careless when posting privacy-invasive photographs on social media, the person affected would not be able to sue for damages but would be able to seek an injunction, an order for delivery up,

---

[239] Ibid, Rec. 5. See also a Civil Remedies for Serious Invasions of Privacy Bill 2020, <https://www.parliament.nsw.gov.au/bills/Pages/bill-details.aspx?pk=3723>.

[240] See, for example, Office of the Australian Information Commissioner, *Department of Immigration and Border Protection: Own motion investigation report* <http://www.oaic.gov.au/privacy/applying-privacylaw/commissioner-initiated-investigation-reports/dibp-omi>; 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 1998* (UK), s 13: *Secretary of State for the Home Department v TLU* [2018] 4 WLR 101, [2018] EWCA Civ 2217.

[241] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014), [7.66].

destruction or removal of the material, a correction order (in the case of a false attribution) or a declaration that his or her privacy was wrongfully invaded. Depending on the facts, one or more of these non-monetary remedies might provide highly suitable redress for the victim of a privacy invasion, while imposing little, if any, financial burden on the defendant. The *Copyright Act 1968* (Cth), s 115 (3) contains a similar provision that bars damages for innocent infringements of copyright, whereas other relief is available also in the absence of fault.

Our Recommendations

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

156. 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.

157. A negligence standard would be in line with 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.[242] 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.

158. 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.

Question 61: How should a statutory tort for serious invasions of privacy be balanced with competing public interests?

[242] New South Wales Law Reform Commission, *Invasion of Privacy*, Report 120 (2009); Victorian Law Reform Commission, *Surveillance in Public Places*, Final Report 18 (2010).

159. The tort recommended by the ALRC contains several mechanisms designed to ensure the appropriate balancing of privacy and public interests. These are:

a) The new tort is actionable only where a person in the position of the plaintiff would have had a reasonable expectation of privacy, in all of the circumstances.
b) The scope of the tort is limited by introducing a threshold requirement that the invasion must be serious.
c) The restrictive aspects of the tort include the fact that it requires intentional or reckless conduct (although we recommend that negligent invasions of privacy should also be actionable).
d) Importantly, it is proposed that an action can only succeed if the court is satisfied that the public interest in privacy outweighs any countervailing public interests. This requirement for a balancing exercise will ensure that conflicting interests such as freedom of speech, freedom of the media, public health and safety, and national security are not disproportionately curtailed.
e) Finally, the balance between privacy rights and public interests is further protected by the existence of a number of defences and exemptions, such as consent, necessity, absolute privilege, and fair report of proceedings of public concern for the defendant to rely on where a plaintiff does establish that the tort has occurred.

160. It is sometimes suggested that a statutory privacy tort has the potential to stifle media expression. 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 a finely calibrated mechanism to balance competing public interests 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.

161. In principle, we support the adoption of these mechanisms. The ALRC was at pains to limit the scope of the privacy tort and 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. In particular, the following issues that favour defendants should be noted and possibly reconsidered:

162. 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'.[243] It has

[243] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014), [8.15].

been argued, however, that this design feature has the potential to cause 'duplication'[244] and may not be necessary to deter or exclude trivial claims.

163. In addition, 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.

164. There remains a question as to whether it is appropriate to impose the onus of establishing fault on the plaintiff. While this approach would align the proposed statutory tort with negligence liability, there are also a range of other wrongs, in which the onus of disproving fault is on the defendant (most prominently, actions in trespass), or which are not dependent on proof of fault, at all (such as defamation and breach of confidence). If the fault requirements of the proposed statutory privacy tort were too restrictive, privacy claimants would need to continue to rely on other available remedies if they were unable to meet the more stringent requirements under the privacy tort. This has the potential to complicate litigation and to undermine the effectiveness of the new privacy regime.

165. Apart from ensuring coherence with the fault requirements of existing causes of action that protect similar interests, the interplay of a privacy tort and a future direct right of action under the *Privacy Act* also needs to be taken into account. Compensation for an interference with statutory information privacy rights would be unlikely to depend on proof of fault, which again would create incentives for claimants to rely on that claim right in preference over the statutory tort, where a particular interference is actionable under both causes of action. The arising questions are complex and require detailed further consideration that is beyond the scope of this submission.

[244] 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.