AUSCL

THE ALLENS HUB
FOR TECHNOLOGY, LAW & INNOVATION

LAW BUILDING F8, UNSW SYDNEY NSW 2052 AUSTRALIA
T +61 (2) 9385 2254 | ABN 57 195 873 179 | CRICOS Provider Code 00098G

6 December 2020

Attorney General's Department
Via email: PrivacyActReview@ag.gov.au

Review of the Privacy Act 1988

About Us

This is a joint submission by the Allens Hub for Technology, Law and Innovation and the Australian Society for Computers & Law.

The Allens Hub for Technology, Law and Innovation ('the Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Allens Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society, and the broader community. More information about the Allens Hub can be found at http://www.allenshub.unsw.edu.au/. Our submissions reflect our views as researchers and are not an institutional position.

The Australian Society for Computers & Law is a registered Australian charity established for the purpose of advancing education and advocacy on critical issues at the intersection of law, technology and society. Its predecessor association was established in 1981 and continues to provide an important forum for learned discussion and debate between academics, practitioners, industry leaders and government, seeking to promote equality, governance and the rule of law.

About this Submission

While we are grateful for this opportunity to make a submission, a short time frame at a busy time of the academic year prevents a more substantial contribution. In particular, we echo the concerns raised by Peter Leonard in the Data Synergies submission. We discuss briefly our views on some of the questions raised on the Issues Paper and look forward to further engagement in 2021.

We focus on aspects of the following questions that intersect with our research:

- Objectives the *Privacy Act* (Question 1)
- Definition of personal information (Questions 2-5)
- Flexibility of the APPs (Question 6)
- Exemptions, at a high level, and then specifically in relation to employee records and media (Questions 7-19)
- Limiting information burden (Questions 24, 25)
- Consent (Questions 26-30)
- Inferred sensitive information (Questions 35, 36)
- Access, quality and correction (Question 45)
- Right to erasure (Questions 46, 47)
- Direct right of action and statutory tort (Questions 57-62)

- Legislative complexity (Questions 66-68)

We also believe broader questions ought to be asked in the course of the consultation, including:

- whether privacy law should be modelled on Europe's General Data Protection Regulation (GDPR);
- whether privacy law can be drafted, or guidance given, to avoid "because of the *Privacy Act"* excuses for poor cyber security practices (such as requiring individuals to provide identifying information in phone calls *to* that individual);
- whether privacy law can be better designed to integrate with related and pre-existing areas of governance such as media law, social media regulation, and competition law;
- whether there can be a co-ordinated and more centralised regulatory structure – at present a number of regulators overlap, but often without adequate control or resources; and
- whether privacy law reform can be leveraged to reduce the ability of foreign actors to interfere in domestic elections and politics.[1]

Objectives of the Privacy Act (Question 1)

We recommend a broader set of objectives of the Privacy Act, and in particular the greater emphasis on privacy protection for individuals including protection against misuse of data and empowering consumers to make informed choices.

Definition of personal information (Questions 2-5)

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

The definition of 'personal information' in the Privacy Act should be updated to clarify that it captures technical data such as IP addresses, automated vehicle generated data, device identifiers, geo-location data. The current Australian approach here is overly narrow and restricts the ability of citizens to seek access to their own private information including metadata. The limits of our current and earlier frameworks are exemplified in the full Federal Court's decision in *Telstra v Privacy Commissioner*.[2] In that decision, the statutory focus on personal information *about* an individual prevented someone from accessing all the metadata held in relation to a mobile phone service. The decision illustrates that privacy law in Australia is out of step with comparative developments that better protect personal data and human rights.[3]

The advantages of reworking the definition of 'personal information' can be illustrated through the example of automated vehicles (AVs) and co-operative intelligent transport systems (C-ITS). As we explain in our report for the National Transport Commission, under EU law, a range of technical information, such as data related to automated vehicles including geo-location data collected by C-ITS and AVs, qualifies as 'personal data' for any party that may be able to link such data to a specific individual with reasonable and legal means available to them.[4] Technical data will be considered personal data under EU law where such data alone or in conjunction with other information identifies an individual (for example, the driver, a passenger or a pedestrian) through their patterns of

[1] See our submission (with others at Queensland University of Technology and IEEE's Society for the Social Implications of Technology) on the Senate Inquiry into foreign interference through social media (3 April 2020).

[2] [2017] FCAFC 4.

[3] Genna Churches and Monika Zalnieriute, 'A Window for Change: Why the Australian Metadata Retention Scheme Lags Behind the EU and USA', *AUSPUBLAW* (26 February 2020) <https://auspublaw.org/2020/02/26/>.

[4] David Vaile, Monika Zalnieriute and Lyria Bennett Moses, *The Privacy and Data Protection Regulatory Framework for C-ITS and AV Systems* (Report, The Allens Hub, 2 July 2018) 1 <https://www.ntc.gov.au/sites/default/files/assets/files/UNSW-report-privacy-and-data-protection-regulatory-framework-for-avs.pdf>.

movement.[5] Various data collected by C-ITS or AV sensors, such as information about speed, acceleration and use of brakes, which could be either supporting the operation of automated functions or collected by Event Data Recorders (EDR), *could* constitute personal data in the opinion of EU Court of Justice,[6] the EU Commission,[7] EU data protection authorities and the Article 29 Working Party.[8] The GDPR has also explicitly clarified the status of geo-location data by expressly stating that an individual can be identified directly or indirectly by reference to "location data."[9] It is irrelevant in the EU whether such data is technical, C-ITS-generated or provided by the data subject.[10] A similar approach is needed in Australia.

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

The Privacy Act should cover the inferred information, particularly where inferred information includes sensitive information, such as information about an individual's health, religious beliefs, political affiliations, or sexual orientation. As Dr Monika Zalnieriute explains in her work on privacy and fundamental rights of LGBTI communities, a lot of publicly available data, such as Facebook friend information or individual music playlists on Youtube, can be used to infer individual traits, such as sexual preference, with high levels of accuracy.[11] The accuracy of predictions from the online trail of information we leave is higher than what friends know about an individual's personality.[12] If widely-traded advertising information can discriminate between e.g, homosexual and heterosexual men in 88% of cases,[13] then most Internet users should assume that all companies advertising to them can predict their sexual orientation with a high degree of accuracy – and are likely to do so in order to sell them products. Issues go well beyond simple product advertising, and can potentially include different treatment in areas such as health and life

---

[5] See Article 29 Data Protection Working Party – *Opinion 13/2011 on Geolocation services on smart mobile devices,* available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2011/wp185_en.pdf 22, which states location data collected by smartphones is considered personal data because individuals can be directly or indirectly identified through their patterns of movement.

[6] European Court of Justice, Judgment of 19 October 2016, *Patrick Breyer* v. Bundesrepublik Deutsch- land – C-582/14. The Court further states, that for a qualification of data as personal it is not required "*that all the information enabling the identification of the data subject must be in the hands of one person*".

[7] EU Commission, A European strategy on Cooperative Intelligent Transport Systems, a mile- stone towards cooperative, connected and automated mobility, COM(2016) 766 final, 30 November 2016, p. 8, ec.europa.eu/energy/sites/ener/files/documents/1_en_act_part1_v5.pdf, visited 15/05/2018. See also EU C-ITS Platform Final Report, September 2017, available at https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf, p.28. The C-ITS platform is an initiative of Directorate for Transport and Mobility of the EU Commission, which started at the end of 2014 with the creation of specialized working groups, each addressing various aspects of C-ITS deployment, ranging from security, to technical standardization, to data protection. The Data Protection and Privacy Working Group of C-ITs stated that broadcast messages exchanged by vehicles are personal data because: 1) the messages contain authorisation certificates that are univocally associated to the sender, and; 2) the messages contain heading, timestamp, location data and the dimension of the vehicle.

[8] Article 29 Working Party, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), available file:///Users/monika/Downloads/20171020_wp252_enpdf.pdf, visited 15/05/2017, p. 6. The Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

[9] Article 4(1) GDPR.

[10] For an EU perspective on how user generated personal data has been exposed to access in contravention of the GDPR see Genna Churches and Monika Zalnieriute, '"Contracting Out" Human Rights in International Law: Schrems II and the Fundamental Flaws of U.S. Surveillance Law' (2020) *Harvard International Law Journal Online* <https://harvardilj.org/2020/08/contracting-out-human-rights-in-international-law-schrems-ii-and-the-fundamental-flaws-of-u-s-surveillance-law/>.

[11] Monika Zalnieriute, 'Digital Rights Of LGBTI Communities: A Roadmap For A Dual Human Rights Framework' in Ben Wagner, Matthias C Kettlemann and Kilian Vieth (eds), *Research Handbook on Human Rights and Digital Technologies* (Edward Elgar, 2019) 464; Monika Zalnieriute, 'The Anatomy of Neoliberal Internet Governance: Queer Critical Political Economy Perspective' in *Queering International Law: Possibilities, Alliances, Complicities, Risks* (Taylor & Francis, 2017) <https://papers.ssrn.com/abstract=2894136> ('The Anatomy of Neoliberal Internet Governance').

[12] Youyou, Wu, Michal Kosinski, and David Stillwell. 2015. "Computer-Based Personality Judgments Are More Accurate than Those Made by Humans." *Proceedings of the National Academy of Sciences* 112(4): 201418680.

[13] Kosinski, Michal, David Stillwell, and Thore Graepel. 2013. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior." *Proceedings of the National Academy of Sciences of the United States of America* 110(15): 5802–5.

insurance,[14] employment[15], and law enforcement contexts.[16] It is therefore important to ensure that inferred information is covered by the Privacy Act. See also Questions 35, 36 on inferring sensitive information below.

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

De-identification is a process rather than an end-state – there is thus no de-identified information only information that has been through a de-identification process.[17] This is not mere semantics – identifiability is a risk scale (likelihood of and severity if different entities re-identify individuals in a data set). Where there is a real possibility of re-identification, information should not lie entirely outside data privacy protection.

At a minimum, Australia's anonymisation provisions should be aligned with those of the EU's GDPR. Under EU law, data is no longer regarded as personal data if it is "*rendered anonymous in such a way that the data subject is no longer identifiable*".[18] However, as defined by the CJEU in *Breyer* case, *identifiability* of data subject depends on the knowledge of the data controller and the reasonable means they are able to deploy to re-establish the identity of data subject. Therefore, anonymity of data is relative: as long as some data controllers may link a data item to a unique identifier that can be associated with a person, the data qualifies as personal data in relation to that specific data controller.[19]

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

Yes, the definition of 'personal information' in the *Privacy Act* should be amended to clarify that it encompasses data drawn from the profiling or tracking of behaviours or movements such that an individual can be singled out (i.e. disambiguated from a crowd or cohort) and thus can be subjected to targeting or intervention.[20] Protection or personal data may be required even though an individual cannot be 'identified', in the conventional sense, from the data or related data. The Government should consider such an amendment, which would bring Australia's Privacy Act in line with latest laws, such as California Privacy Act,[21] dealing with the harms arising of the novel technologies, such as gait recognition.

Flexibility of the APPs in regulating and protecting privacy (Question 6)

A level of flexibility in privacy protection legislation is necessary not only to balance *interests* of individuals, governments and corporations, but also to better protect the *rights* of individuals.

The question of privacy protection needs to be considered in a wider context of the use (and usefulness) of personal data, so that law and regulation contribute to adoption of rights-enhancing processes. In this context, we submit that the link between privacy protection and the issue of algorithmic discrimination and unfairness should be addressed through adequate flexibility of the Privacy Act framework. Diversity, non-discrimination and fairness are requirements for trustworthy AI

---

[14] Angela Daly, 'The Law and Ethics of "Self Quantified" Health Information: An Australian Perspective' (2015) 5(2) *International Data Privacy Law* 144 ('The Law and Ethics of "Self Quantified" Health Information').

[15] Kim, Pauline T. "Data-driven discrimination at work." *Wm. & Mary L. Rev.* 58 (2016): 857.

[16] Potential discriminatory outcomes in law enforcement and criminal justice are discussed by Monika Zalnieriute, Lyria Bennett Moses and George Williams, 'The Rule of Law and Automation of Government Decision-Making' (2019) 82(3) *The Modern Law Review* 425.

[17] Michael Guihot and Lyria Bennett Moses, *Artificial Intelligence, Robots, and the Law* (LexisNexis, 2020) 200–203.

[18] Recital 26 GDPR.

[19] Vaile, Zalnieriute and Bennett Moses (n 4).

[20] Zalnieriute, 'Digital Rights Of LGBTI Communities: A Roadmap For A Dual Human Rights Framework' (n 10).

[21] California Consumer Privacy Act of 2018 (CIV).

systems.[22] It is essential that algorithms are trained, and then tested, on representative data sets that are inclusive and complete.[23] It has been demonstrated that denying a machine learning system access to protected attributes, such as gender or race, during training may exacerbate discrimination instead of preventing it.[24] This is similarly important in the context of testing for (and potentially correcting) algorithmic discrimination.[25] This means that public and private entities, and in particular research organisations, health services providers and all types of commercial services providers, who deploy AI systems using individuals' data in their work, need to have access to representative data sets that also include features relative to protected attributes. A sensible approach should be developed, that would allow for inclusion of potentially sensitive information to be included in data sets used, but only under conditions that guarantee privacy protection and security.

One solution is to draw on work of the Information Commissioner's Office in the UK. There, a controlled environment or "regulatory sandbox" ensures supervision of an entity exploring how sensitive data can be used safely to enhance fairness, while protecting individuals' privacy.[26] The UK approach allows participants to access the regulator's expertise and support in achieving compliance with data protection rules. The sandbox environment is "controlled" in that the regulator is working closely with the entity making sure they are complying with the law and helping them identify and address potential issues. The participating entity takes part in workshops, meetings, and other consultations, and has a case officer assigned to them, who oversees their sandbox participation. For example, Onfido Limited, a provider of remote biometric identity verification technology, entered the ICO's Regulatory Sandbox with the aim of measuring and mitigating bias in their facial recognition technology in a manner which complied with data protection law.[27] Sandbox's participation allowed them to address issues such as lawful basis for processing of personal information including biometrics, while researching technical means of measuring and mitigating bias.

Exemptions (Questions 7-19)

Removal of the many unjustifiable exemptions from the Privacy Act was one of the major recommendations of the Australian Law Reform Commission in its review of the Privacy Act. For example, blanket exemptions for sectors, such as the so-called 'small business exemption' is a major obstacle to Australia obtaining a positive adequacy assessment from the EU, and provisions in Japan's laws with similar effect were removed from its law prior to its adequacy application. In addition, we make the following more specific points.

Employee records exemption (Questions 13-15)

The professional sporting context, where sensitive health information is closely related to employee performance, demonstrates the potential overreach of the employee records exemption. We therefore recommend that this exemption be removed.[28]

Media exemption (Questions 17-19)

Currently the Privacy Act offers an exemption to media organisations if the relevant act or practice relates to journalism and the organisation is publicly committed to observe published privacy

[22] See High-Level Expert Group on Artificial Intelligence (set up by the European Commission), *Ethics Guidelines for Trustworthy AI* (8 April 2019) Section B. Framework for Trustworthy AI, 6ff.

[23] Ibid 18.

[24] See e.g. Gradient Institute, *Practical Challenges For Ethical AI* (White Paper, 3 December 2019) in particular 6-7.

[25] Anya E.R. Prince, Daniel Schwarcz, 'Proxy Discrimination in the Age of Artificial Intelligence and Big Data' (2020) 105 *Iowa Law Review* 1257, 1313-1315.

[26] See Information Commissioner's Office website, 'What is the Sandbox?' https://ico.org.uk/sandbox.

[27] Information Commissioner's Office, *A summary of Onfido's participation in the ICO's Regulatory Sandbox Beta* (Regulatory Sandbox Final Report: Onfido, September 2020), see especially pp. 5-6, para 1.6.

[28] For a more detailed explanation, see the submission of the Minderoo Tech & Policy Lab at UWA Law School.

standards such as those contained within the *Broadcasting Services Act 1992* (Cth) or the Australian Press Council Privacy Standards.[29]

There is clearly room to better integrate media regulation in this area given digital convergence, but there is also a danger that without media freedom and public interest reportage exemptions or defences available, removing the current exemption will simply result in further damage to media freedom. Thus, any changes need to be considered in light of the broader media law landscape. Without appropriate protections elsewhere for media freedom, an exemption remains necessary. If a statutory cause of action for serious invasion of privacy is introduced, it would be hard to justify an exemption in terms of the cause of action, but there would still need to be appropriate public interest reportage defences available. A definition of journalism may assist here but might also create its own problems given the digital and citizen media environment.

Limiting information burden (Questions 24, 25)

Currently, people wishing to make deliberate decisions about how their data is used need to read natural language privacy policies that, despite their length, often do not provide sufficient information for individuals to estimate the risk. On the other hand, it is possible to conduct an image search online that only displays results where copyright-related criteria are met (eg "free for non-commercial use"). It ought to be similarly possible for people to search an app store or the web and only reveal results where personalised criteria are met. Those criteria can be selected based on issues of concern to consumers, for example whether information used in marketing solicitations, whether information passed on to other entities, whether storage meets cyber security standards, whether information used to build a consumer profile for differential treatment, and so forth. This would require privacy policies to be written, in part, in a machine-consumable format at least in so far as relates to nominated criteria. However, the result would be an easier system for consumers to exercise choice (through privacy settings in app stores and browsers), creating a market opportunity for privacy-protective applications and products. This possibility would require further research, in particular to identify issues of particular concern to consumers.

Consent to collection, use and disclosure of personal information (Questions 26-30)

Australian consumers are concerned about the privacy of their data, and want more control and choice over how their data is used and shared.[30] This is in contrast to the practices of entities across various industries in Australia, as our ongoing research of privacy policies reveals. Particularly concerning is the widespread use of practices such as consent bundling, personal information sharing with undisclosed third parties, cross-referencing between privacy policies of various entities, as well as use of vague and unclear terms to describe how and for what purposes the information will be used. Such practices may in some cases be unlawful (see e.g. *Australian Competition and Consumer Commission v HealthEngine Pty Ltd* [2020] FCA 1203 where information sharing with third parties without adequate consent was considered as breach of consumer law), but very often relies on the wording of the *Privacy Act*. Where such practices are not unlawful, they are still harmful to individuals, who do not have the desired control over their personal data. Often, consumers would be surprised to find out how their data may be used. Our ongoing research on the insurance industry provides a useful example. Information sharing, for example between entities belonging to the same corporate group, means that the data collected through supermarket loyalty schemes could be then used for the purposes of insurance contracts underwriting.

---

[29] David Rolph, Matt Vitins, Judith Bannister and Daniel Joyce, *Media Law: Cases, Materials and Commentary*, Second Edition (Oxford University Press, 2015) p 541.

[30] OAIC, Australian Community Attitudes to Privacy Survey 2020 (Prepared for the Office of the Australian Information Commissioner by Lonergan Research, September 2020) 51.

A potential solution would be to require individuals' express consent to such practices, as well as more general requirements as to transparency, legibility, and clear wording of the privacy policies. However, studies have consistently demonstrated that individuals do not read privacy policies due to the so-called 'consent fatigue'.[31] Therefore, providing them with even more information would be counterproductive. Instead, emphasis should be placed on shifting the burden from consumers to the entities, who would need to ensure that their privacy policies allow for collection, disclosure and use of the personal information within what can be reasonably expected by consumers. As with the insurance sector example, individuals cannot reasonably expect that the information relative to their grocery shopping may ever be used to price their insurance policy. In the light of our points about consent fatigue and long, unclear privacy policies, it is important to note that just including in a privacy policy a notice regarding ways in which personal information can be used should not be enough for the entity to be able to demonstrate individuals could have reasonably expected it.[32]

We therefore submit that the requirement on entities to act fairly, currently applicable to the information collection (collecting personal information by lawful and fair means, APP 3), should be extended to information use and disclosure. Furthermore, means of enforcing these requirements by regulators, as well as private means of redress available to individuals, should be provided.

Inferred sensitive information (Questions 35, 36)

As correctly observed in the Issues Paper, with an increasing use of sophisticated artificial intelligence techniques, it is becoming possible and likely that entities will generate inferred personal information, including sensitive information, to collection and use of which an individual has not consented.[33] The problem is however even more complicated, as AI systems are often opaque, which means it is not possible to provide meaningful reasons for a decision. In such case, the system may provide an outcome, which cannot be traced to a specific piece of inferred information, as it does not materialise in a tangible way. An example based on our ongoing research in the sphere of insurance contracts and proxy discrimination could be when an insurer uses an AI system for the purpose of pricing risk and life insurance contracts underwriting. The system is provided with some input data, such as e.g. person's grocery shopping history, obtained through a supermarket loyalty scheme. We cannot know whether the decision on how to price a prospective insured's risk is, for example, related to information on certain health conditions inferred from the grocery shopping data. The system does not "think" like humans. Rather, it looks for correlations that may indicate a higher risk. The intermediate step (inference as to health condition) may not be explicitly coded and may be difficult to observe or infer. The problem therefore is that sensitive health-related information may be effectively used by an automated decision-making system, even though it only materialises as an internal encoding of the artificial intelligence model and is not recorded in a human-understandable way.

Therefore, regulatory focus should not be placed primarily on the concept of information "collection" (which involves information being "included in a record" by entities[34]) but rather on *how*, *for what purpose* and *by whom* it is potentially used. Privacy law should address scenarios where sensitive information may potentially be used and ensure sufficient transparency as to such intermediate use. This implies the need to coordinate sector-specific rules, AI-focused standardisation, and privacy law. See also questions 2-5 considered above and question 45 below.

---

[31] See e.g. Hanbyul Choi, Jonghwa Park, Yoonhyuk Jungb, 'The role of privacy fatigue in online privacy behavior' (2018) 81 *Computers in Human Behavior* 42.

[32] Allens Hub have covered issues of consent and data sharing under the proposed Data Availability and Transparency Bill 2020; see Lyria Bennett Moses, Genna Churches, Fleur Johns, Lauren Parnaby (intern), Monika Zalnieriute, Submission to the Office of the National Data Commissioner, Draft Data Availability and Transparency Bill 2020, 6 November 2020.

[33] See, e.g, Zalnieriute, 'Digital Rights Of LGBTI Communities: A Roadmap For A Dual Human Rights Framework' (n 10).

[34] S 6(1) Privacy Act 1988.

Access, quality and correction (Question 45)

Two aspects of information collection and use need to be addressed.

First, the Act should address the question of information an entity holds about an individual (independent from questions of use). The Act recognises the right of individuals to access (APP 12) and, if necessary, correct information being held about them (APP 13). This right needs to be strengthened through enhanced transparency, especially regarding omnipresent data collection by various entities.[35] Individuals should be entitled to know the source of the data held about them, which as we know could be anything from their digital presence (including social media activity, browser history, cookies, smartphone apps etc.) to participation in various loyalty schemes, or data collected by various entities they have interacted with.

Increased general transparency would help address problems related to the *use* of information. This brings us to the second more specific question, regarding individuals' right to information about how their data is processed. As discussed in relation to questions 2-5, 35-36 above, inferred information may not be recorded and held by entities in traditional sense. This would mean individuals will not be able to access *all* information that may have potentially been used in making a decision that affected them. Further, even if individuals had access to all the variables *relating to them* used in drawing inferences or making decisions about them, this would be too vast for them to process. For someone affected by automated decision making where they would ordinarily be entitled to an explanation of that decision, their right to such an explanation should not be lost by virtue of the use of particular techniques (such as deep neural networks).

There is extensive work being done on new techniques to enhance the explainability of decisions made using artificial intelligence techniques such as machine learning.[36] The Australian Law Reform Commission is also proposing work on administrative law and automated decision-making, which would likely include consideration of the right to reasons. Thus, in addition to recommending greater transparency about data collection and data use, we also suggest co-ordinating changes in the *Privacy Act* with law reform in other areas, including administrative law, consumer law, and discrimination law. We make this point at greater length in our recent submission on the AI Action Plan.

Right to erasure (Questions 46, 47)

A right to erasure should be considered as part of the reform process, especially if a wider move towards data protection is embraced. There needs to be a balancing of interests in personal and private information as against countervailing public interest considerations including free speech, media freedom, access to information, administration of justice, public health and safety, and national security concerns. Article 17 of the GDPR provides an appropriate template for the key features of such a right and the UK's implementation of a right to erasure in its data protection legislation is illustrative of how a domestic common law system can enact such a right.

By aligning with the best regional and comparative standards in this area, Australian courts and regulators will also benefit from an emerging comparative jurisprudence dealing with many of the complexities involved.[37] There may be financial implications for digital platforms, but these are a necessary part of their acceptance of consumer and human rights protections given the ubiquity, social significance and profitability of their businesses. The ACCC's insight that such a right will help to address the power imbalance between citizen consumers and platform power is valuable. Self-regulation has clear limits here. Introducing such a right will assist with ensuring that digital platforms and other similar entities remain committed to privacy protection and developing accessible ways for

[35] On the need for transparency in data collection process, see Monika Zalnieriute and Genna Churches, 'When a "Like" Is Not a "Like": A New Fragmented Approach to Data Controllership' [2020] *Modern Law Review* 20 ('When a "Like" Is Not a "Like"').

[36] See e.g. Marco Tulio Ribeiro, Sameer Singh, Carlos Guestrin, '"Why Should I Trust You?" Explaining the Predictions of Any Classifier' (2016) arXiv:1602.04938, available at: https://arxiv.org/abs/1602.04938.

[37] For a discussion of the Court of Justice of the European Union jurisprudence on right to erasure, see Monika Zalnieriute, 'Google LLC v. Commission Nationale de l'informatique et Des Libertés (CNIL)' (2020) 114(2) *American Journal of International Law* 14.

Australian consumers to seek the removal of problematic information concerning them. Without such a right, it remains a practical problem to do so and one which is made more complex by questions of jurisdiction.

Direct right of action and statutory tort (Questions 56-62)

Both a direct right of action and a statutory tort should be introduced.

A statutory tort should be introduced to provide a remedy in the court system for individuals or classes of individuals who are victims of more serious violations of privacy. The common law in Australia has failed to develop a cause of action in tort unlike other jurisdictions including the UK and New Zealand. This has left Australian plaintiffs without an adequate cause of action for serious invasion of privacy. While, in some cases, invasions of privacy can also be dealt with by criminal laws, defamation, breach of confidence and even trespass, the current framework is piecemeal and lacks conceptual coherence and integrity. This creates problems in terms of application and accessibility. A useful and current template for reform here is the ALRC's report and recommendation for a statutory cause of action for serious invasion of privacy. There are further issues to consider in relation to the ALRC's recommendations, including a defence for public interest journalism of the kind now envisaged by recent defamation law reforms adopted in NSW and Victoria. Nevertheless, that ALRC process provides a strong foundation upon which to further develop a broader statutory cause of action. The cause of action should lie against any individual, company or other entity - irrespective of whether it is subject to the *Privacy Act*. The tort should also extend to non-digital invasions of privacy – such as intrusions of individual's physical, bodily or social privacy. The fault standard for the tort should be one of negligence. This is because most data breaches result from failure to remedy known vulnerabilities[38] or human error.[39] The risk of either of these causing a breach can be mitigated by implementing (reasonable) technical and organisational measures. Recklessness and intention should be treated as aggravating factors in assessing damages. We note that in some situations, intentional violations of digital privacy will also constitute criminal offences.[40] As with the direct right of action, both material and non-material harm should be compensable. Finally, there will need to be well defined public interest exceptions for media reporting and political communications.

The direct right of action should be shaped to permit the 'just quick and cheap'[41] resolution of less serious misconduct relating to the collection, use, or disclosure of personal information. It would be handled initially by the OAIC, although that gives rise to resourcing concerns that would need to be addressed. Alternatively, and to ensure that the direct right of action is accessible, jurisdiction at first instance could be vested in a civil tribunal and on a no-cost basis. A statutory range of damages (including a cap) should be considered, and thought will need to be given to develop appropriate defences including a defence relating to public interest reporting.

Legislative complexity (Questions 66-68)

In Australia, in addition to having separate privacy laws for different jurisdictions, information handling requirements for government data are often managed one agency at a time or one dataset at a time. There are, for example, specific rules for categories such as COVIDSafe app data, protected taxation information, protected social security information, migration data, and different categories of health information. Context-specific rules can inadvertently restrict the technical options for using information, limiting them to procedures available at the time of each statute's enactment. More

[38] See eg Ponemon Institute, *Costs and Consequences of Gaps in Vulnerability Response* (2019) available at https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf.

[39] OAIC Notifiable Data Breaches Report: January–June 2020 available at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2020/.

[40] *Commonwealth Criminal Code 1995* (Cth) Part 10.7; *Crimes Act 1900* (NSW) parts 6, 15B and 15C.

[41] *Civil Procedure Act 2005 (*NSW) s 56; see also Federal Court of Australia Act s 37M.

broadly, the complexity compromises the government's ability to build platforms for efficient, appropriate, lawful information sharing among agencies.[42] There are not even common terms across legislation for identifying the entity or entities with decision powers over or responsibilities for data.[43]

While there should be different levels of protection for different categories of data based on different levels of risk, this need not be done with different pieces of legislation and complex narrowly applicable rules. Rather, a similar outcome could be achieved by bringing all data protection requirements into a single Act with different levels of protection applying to different categories of information. Similar rules and principles could then apply to all highly sensitive government datasets (for example, use only for listed purposes, deletion requirements, etc). Reform of the Privacy Act should thus focus on reducing complexity, within and beyond that Act.

Without a broader frame, there is a risk that further reforms will fail to address the need for clarity, remedial accessibility, and integration in what is a rapidly developing area. Peter Leonard noted that our earlier privacy framework became 'a confusing landscape, with forests of regulation to get lost in, unexplored corners and poorly signposted and potholed roads'.[44] Privacy reform is overdue and must avoid such legislative complexity. Here too there is a need to not only keep up with international and comparative contexts and developments, but to learn from them in developing an improved *Privacy Act*.

Reform should also take account of the position of law enforcement and national security agencies. There are few organisations or bodies that hold more sensitive data about an individual. Privacy requirements should apply to such bodies, albeit with modifications set out in legislation. This would avoid many regulatory gaps. For example, current arrangements for accessing telecommunications data (metadata), often have no deletion period.[45] Evidence at the 2020 Review of the mandatory data retention regime by the PJCIS suggests that agencies do not delete accessed telecommunications data, and draw upon it for future investigations and make secondary disclosures to other agencies in case of a suspected breach of the law.[46] The Parliamentary Joint Committee on Intelligence and Security have recommended that the *Telecommunications (Interception and Access) Act 1979* (Cth) be amended to require deletion when the data is no longer required.[47] However, an overarching requirement that data must be deleted after two years unless the agency can justify why it needs to be kept would create a positive obligation on law enforcement and national security agencies to actively assess and destroy data no longer required, or provide justification on why it should be kept. This obligation should be contained in the *Privacy Act* and apply to specified agencies and data categories, within the broader context of *Privacy Act* obligations.

The mandated data retention scheme should also be captured by *Privacy Act* obligations. Currently, the mandated data retention scheme has no compulsory deletion period following the retention of metadata by telecommunications providers for two years, resulting in the possibility that customer metadata could be retained for far longer periods.[48] In 2015, some telecommunications providers flagged that they were developing programmes for their own retention of data for business purposes,

---

[42] An extended report by the Data to Decisions Cooperative Research Centre on the legal challenges in creation of the National Criminal Intelligence System is available on request.

[43] Lyria Bennett Moses, 'Who Owns Information? Law Enforcement Information Sharing as a Case Study in Conceptual Confusion' (2020) 42(2) *University of New South Wales Law Journal* 615.

[44] Peter Leonard, 'Lost in the Landscape of Australian Privacy Regulation' (2013) 32(3) *Communications Law Bulletin* 6 at p 7.

[45] Commonwealth of Australia, Parliamentary Joint Committee on Intelligence and Security, Review of the mandatory data retention regime, October 2020, 51-54, 106.

[46] Commonwealth of Australia, Official Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, 7 February 2020, 29-30; see also Churches and Zalnieriute (n 3); Genna Churches and Monika Zalnieriute, 'Unlawful metadata access is easy when we're flogging a dead law', The Conversation (10 December 2019) <https://theconversation.com/unlawful-metadata-access-is-easy-when-were-flogging-a-dead-law-127621>.

[47] Commonwealth of Australia, Parliamentary Joint Committee on Intelligence and Security, Review of the mandatory data retention regime, October 2020, Recommendation 9 (subject to a period of retention for the Commonwealth Ombudsperson to conduct audit processes).

[48] Churches and Zalnieriute (n 3); See also, Monika Zalnieriute and Genna Churches, Submission #4 to the Review of the mandatory data retention regime, Parliamentary Joint Committee on Intelligence and Security, 28 June 2019, 18-19.

including the retention of 'web browsing'.[49] However, consumers may not be comfortable with such sensitive data being held indefinitely by a business, whether for commercial or law enforcement purposes. Also, the longer retention period provides extended opportunity for law enforcement access, potentially skewing privacy considerations under the mandatory data retention regime. Thus, the *Privacy Act* should ensure that the data retention scheme operates consistently with privacy principles, subject to the specific obligations in the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* and other relevant laws.

The advantage of having all obligations in a single, coherent *Privacy Act* is that, except where specifically provided for, data protection requirements apply. Further, differential treatment based on agency or data type would be captured in a single place and linked to a clear scope and justification.

Yours sincerely,

Lyria Bennett Moses, Zofia Bednarz, Genna Churches, Julia Cooper, Samuel Hartridge, Daniel Joyce, Monika Zalnieriute (listed in alphabetical order) – Allens Hub

Marina Yastreboff, on behalf of the Australian Society for Computers and the Law

[49] Commonwealth of Australia, Parliamentary Joint Committee on Intelligence and Security, Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, February 2015, 106 [3.127].