10 January 2022

Australian Government Attorney-General's Department
By email: PrivacyActReview@ag.gov.au

Submission on the Privacy Act Review Discussion Paper (October 2021)

About us

The UNSW Allens Hub for Technology, Law and Innovation ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the 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 UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

The Deakin University Centre for Cyber Security Research and Innovation ('CSRI') is a Strategic Research Centre that brings together a multi-disciplinary team of researchers drawn from Deakin's four Faculties. CSRI's research program is focussed on the technology, systems, human, business, legal and policy aspects of Cyber Security, and is committed to achieving translational and transformational research outcomes for industry, business and society. CSRI's research program is advised by senior industry and thought leaders through its Executive Advisory Board for Cyber (EABC) and is funded through national competitive grants and industry. More information about Deakin CSRI can be found at https://www.deakin.edu.au/csri.

The IEEE Society on Social Implications of Technology ('SSIT') explores the ethics and social implications of technology, ensuring that IEEE fulfils its mission of advancing technology for humanity. With more than 400,000 members in 160 countries, IEEE is the world's largest technical professional association. SSIT is a community that engages some of the world's experts on technology and its impact, but also philosophers, lawyers, ethicists, policy makers, professors — in general people who take an active interest in where humanity and emerging technologies are headed and can interact. The Australia Chapter ('SSIT Australia') pursues a wide range of activities in the Australia region, including technical meetings, international conferences, and development of public policy through workshops and submission papers. SSIT Australia has members from a wide range of industries and academic backgrounds joining an ongoing dialogue on the social implications of technology. More information about SSIT Australia can be found at https://technologyandsociety.org/member-resources/find-a-local-ssit-group/australia-chapter/.

About this Submission

We are grateful for the opportunity to make a submission on the Discussion Paper. Our submission reflects our views as researchers; they are not an institutional position. This submission can be made public.

Our main points relate to:

- the existence of policy issues remain beyond the scope of the Privacy Act Review;
- the fact that information cannot be cleanly divided into 'personal' and 'non-personal', but that much data that has undergone a de-identification process is re-identifiable with some measure of risk (proposal 2);
- our support for proposal 2.4;
- our suggestions in relation to proposal 3;
- concerns about the relationship between the small business exemption and the Consumer Data Right;
- the importance of removing or narrowing the employee records exemption in order to ensure cyber security requirements apply in this context;
- a requirement for privacy notices to be accompanied by code that can be automatically processed by computers (so that privacy settings can be used to control what an individual agrees to) (proposal 8);
- the limitations of relying on consent as a solution to consumer issues with privacy (proposal 9);
- the importance of transparency about research uses (proposal 10.4);
- how proposal 11 could be strengthened;
- our support for proposals 15.1-3;
- our suggestion for extending proposal 17;
- our response to some of the questions in chapter 27 (data breach notification);
- the ability to use a range of existing security standards to reduce compliance costs in proposal 19.2;
- support and further suggestions for strengthening enforcement powers (proposal 24);
- suggestions for a direct right of action (proposal 25);
- specific issues around biometric identifiers.

Larger questions

While reform of the *Privacy Act 1988* (Cth) is to be encouraged, there are more questions raised by the increasing use of information about individuals and populations to generate predictions, make decisions and manipulate people than can be answered by a statute that prescribes principles for processing personal information. Even if Australia were to tighten up its legislation in line with Europe's General Data Protection Regulation, as many jurisdictions are doing, the issues cannot be properly analysed without a broader mandate than that given to the Privacy Act Review. For example, discrimination law, consumer protection law, human rights law and competition law would need to be included if our goal is to ensure data practices protect the rights and interests of Australians. However, the Discussion Paper does move us forward, if not all the way to the destination, and we have therefore focussed our comments on its proposals.

Personal information (proposal 2)

More than two categories of information

While these changes are steps in the right direction, it does not resolve the dilemma that there is no neat line between personal and non-personal information. In particular, the following problems remain:

- individuated targeting where there is no "identification";
- identification at household level, where there is no ability to identify the individual within a household (eg electricity use), where the privacy impacted is not of an individual but of a family;
- the fact that no information about people can be fully anonymised given the possibility of access to other datasets.

To give an example of the third problem, consider very high level statistics (such as the number of women, men and non-binary adults in Australia. That is "anonymised" in most ordinary senses of the term. But, if I know the gender of every Australian adult bar one, then I can determine the gender of that individual from the aggregated statistic. This example is, of course, far-fetched, but the fundamental point remains - there is no clear dividing line between personal information and anonymised information, only a scale of risk. Aggregated data on the gender of Australian adults would be at the low risk end of the scale, but it is potentially re-identifiable.

This means that the idea of information "under the Act" versus information "not under the Act" ought not be treated as a simple binary. One can distinguish among:

1. Information that is personal, in that it is clearly about an individual
2. Information that can be re-identified, albeit with varying levels of difficulty
3. Information that was never about an individual (for example, historical weather patterns).

Information in the first category should be "under the Act" and information in the third category should not be "under the Act" but information in the second category can only be managed on the basis of a risk assessment, which ought to depend on the sensitivity of the information and the probability of re-identification given planned release protocols. The challenge is also cumulative – the more such datasets are available, the increased risk of identifying further datasets.

Inferred information (proposal 2.4)

We welcome this proposal to expressly recognise inferred information as personal information and include inferring of information in the definition of information collection. It is appropriate to make it clear that inferred information may not be recorded in any material form, yet still be used for purposes of data-driven decision-making, as we noted in our submission to the Issues Paper in 2020.[1]

We recognise this may pose some challenges to entities that use AI/ML models in their operations to infer information about individuals with the purpose of informing their decisions, for example in commercial context, as to personalised advertising or other personalised products, including financial

[1] The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers & Law, 'Joint submission to Attorney General's Department: Privacy Act Review 2020' (6 December 2020) 7 <https://www.ag.gov.au/sites/default/files/2021-01/the-allens-hub-for-technology-law-and--innovation.PDF>.

services.[2] Indeed, a number of submissions to the Issues Paper in 2020, notably from Facebook, Microsoft and DIGI, have indicated concerns regarding a possible increased protection of inferences.[3] Those submissions seem to indicate that inferencing is mainly used in relation to de-identified information, and therefore the current practice of companies using inferences is not to provide notice or ask consumers for consent in respect of inferred information.

However, it needs to be recognised that de-identification will not always prevent privacy and other harms.[4] Furthermore, there is a significant risk of privacy harms when inferences are used, as they may make it possible to uncover facts about people that they might prefer to keep private, such as a person's sexual orientation from their face photos,[5] a person's suicidal tendencies from their posts on Twitter,[6] or the fact that they are expecting a baby.[7]

These are privacy risks that are best addressed in the Privacy Act.[8] However, mere recognising of inferences as personal information may not be sufficient to prevent harms we have mentioned. First, as noted, de-identification will not always protect individuals from harms related to processes such as profiling. Second, the harms will be a consequence of a decision-making process based on inferences in relation to individuals' current and future behaviours, opinions, commercial worth, and other predictions. Such inferences may be unexpected, incorrect, or irrelevant.[9] Furthermore, where ML models are used for decision-making and inferences only appear in the form of numerical vectors, protection through treating inferences as personal information will achieve little.

The regulatory focus needs to be placed on the purpose of the use of data, and the resulting decision-making process.[10] The role of privacy law is to ensure sufficient transparency, not only as to the use of inferencing models (proposal 17), but also regarding their commercial or other purpose and outcomes they produce.

[2] For a detailed analysis regarding the use of AI/ML models in the context of consumer insurance and its implications for consumers, see Zofia Bednarz and Kayleen Manwaring, 'Keeping the (Good) Faith: Implications of Emerging Technologies for Consumer Insurance Contracts' (2021) 43(4) *Sydney Law Review* (forthcoming). Please let us know if you would like access to an advance copy.

[3] See Microsoft Australia, 'Microsoft submission to review of the Privacy Act 1988' 2-3 <https://www.ag.gov.au/sites/default/files/2021-02/microsoft-australia.PDF>, Facebook, 'Submission to the Australian Privacy Act Review Issues Paper' (6 December 2020) 25 <https://www.ag.gov.au/sites/default/files/2021-02/facebook.PDF> and Digital Industry Group Inc ('DIGI'), 'Submission to Attorney General's Department: Privacy Act Review 2020' (4 December 2020) 6-7 <https://www.ag.gov.au/sites/default/files/2021-02/digi.PDF>.

[4] See above. Also Mireille Hildebrandt, 'Profiling and the Identity of the European Citizen' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 305-309, see also Sandra Wachter, 'Data Protection in the Age of Big Data' (2019) 2 *Nature Electronics* 6, 7.

[5] Yilun Wang and Michal Kosinski, 'Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images' (OSF Research Project, updated 26 May 2020) <https://osf.io/zn79k/>.

[6] Bridianne O'Dea et al, 'Detecting Suicidality on Twitter' (2015) 2 *Internet Interventions* 183.

[7] Brigid Richmond, 'A Day in the Life of Data: Removing the Opacity Surrounding the Data Collection, Sharing and Use Environment in Australia' (Report, Consumer Policy Research Centre 2019) 34 describes how US store Target would infer customer's pregnancy based on their shopping history and send them pregnancy- and baby-related advertising and products.

[8] Contrary to what was submitted by DIGI 'Submission to Attorney General's Department: Privacy Act Review 2020' (4 December 2020) 6.

[9] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' [2019]2 *Columbia Business Law Review* 1, 9—22.

[10] As we argue in The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers & Law, 'Joint submission to Attorney General's Department: Privacy Act Review 2020' (6 December 2020) 7.

Flexibility of the APPs (proposal 3)

We welcome proposals 3.1 and 3.2 to allow the IC additional flexibility to impose permanent and temporary code requirements in the public interest, particularly in urgent situations. These go some way to addressing the significant existing power imbalance in the legislation between regulated industries and those supposedly the beneficiaries of the regulation. However, this proposal should be strengthened by allowing a formal role for recognised consumer advocacy groups (eg Australian Privacy Foundation, Australian Communications Consumer Action Network, CHOICE) to make an application for a code to be made in the public interest. In addition, as mentioned in our submission on the Online Privacy Code Bill of 9 December 2021, codes should focus on issues specific to the regulated sectors rather than attempting a narrow version of general privacy law reform (which needlessly increases regulatory complexity).

Exemptions

Small business exemption and the CDR

The Discussion Paper considers a number of possible options in relation to the small business exemption, from complete abolition to proscribing acts or practices that pose a higher risk to privacy and therefore should be covered by the Act regardless of annual turnover. Among other things, the Discussion Paper notes that the small business exemption does not apply to a number of entities by virtue of a special designation in the Act and raises the question whether there are 'further high privacy risk acts and practices that should be prescribed as exceptions to the small business exemption'. This part of the submission responds to this question in the context of the recent revisions to the Consumer Data Right (CDR) framework.

Accredited persons under the CDR Rules are not eligible for the small business exemption pursuant to section 6E(1D) of the Act. We appreciate that accredited persons who act as recipients of CDR data are not exempted but wish to stress that the recent expansion of the CDR framework via the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021* has introduced a significant change to the CDR data sharing model. More specifically, the revised CDR Rules have introduced a new concept of 'trusted advisers' and authorised disclosure of CDR data to trusted advisers *without requiring them to obtain CDR accreditation*. According to the revised CDR Rules, trusted advisers include providers of certain specialist services, in particular:

- qualified accountants within the meaning of the *Corporations Act 2001* (Cth);
- persons who are admitted to the legal profession;
- registered tax agents, BAS agents and tax (financial) advisers within the meaning of the *Tax Agent Services Act 2009* (Cth);
- financial counselling agencies within the meaning of the *ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792*;
- 'relevant providers' within the meaning of the *Corporations Act 2001* (Cth) (ie individuals authorised to provide personal advice to retail clients in relation to relevant financial products), with certain exceptions; and
- mortgage brokers within the meaning of the *National Consumer Credit Protection Act 2009* (Cth).

The above professionals are not subject to bespoke information security controls envisaged by the CDR framework, which targets mainly accredited data recipients (ADRs). In short, in a relationship between the disclosing entity (an ADR) and the recipient of disclosed CDR data, the relevant protections apply to the former – but not to the latter. The Explanatory Statement to the relevant amendments states that 'disclosure of the CDR data from an accredited data recipient to a trusted adviser is covered by the information security controls in Schedule 2 to the CDR Rules' – however in practice the only relevant control implied in this case is the obligation of the ADR to protect CDR data in transit e*n route to the trusted adviser*. In other words, these protections – in the context of CDR data transfers from ADRs to trusted advisers apply to data *in transit*, rather than data *at rest* (once such data have reached the recipient).

Furthermore, the CDR framework rules concerning trusted advisers do not establish an unequal relationship (as observed, for example, in the case of sponsored accreditation): ADRs are not responsible for the actions or information systems of trusted advisers. Trusted advisers only act as CDR data recipients and are subject to their own information security rules (which may or may not be as strict as those found in Schedule 2 of the CDR Rules). In other words, instead of establishing a single information security framework for different recipients of CDR data, the reforms have made possible co-existence of two parallel regimes (with different requirements for data protection): one for ADRs and one for trusted advisers.

Under the revised CDR framework, trusted advisers may end up being the 'weakest link' in the chain of transfers of valuable CDR data. Whether this risk will materialise will depend on the relevant duties applicable to different classes of trusted advisers outside the CDR framework (since the latter is carefully drafted to avoid direct regulation of trusted advisers). In this context, the application or non-application of the Act to trusted advisers – and, in particular, the scope of the small business exemption – becomes particularly important.

In 2018, a survey by Accenture identified security and privacy of financial data as 'Australian consumers' biggest concern with Open Banking', with 64% of respondents citing it 'as the main obstacle to sharing their financial data with third parties'. In the context of sharing of CDR data with non-accredited entities, these issues become more pronounced. On the one hand, the CDR privacy safeguards do not apply to such entities. On the other hand, some of the non-accredited recipients of CDR data may not even be captured by the Act due to the small business exemption. This can potentially undermine consumer trust in the CDR framework. In fact, the potential for degraded privacy protections has been identified as one of the key objections to allowing non-accredited entities access to CDR data:

> 'Any decision to allow non-accredited third parties to access sensitive CDR data is *incredibly dangerous*. It is dangerous because consumers are being led to assume their data will be protected under a "Consumer Data Right" but in fact it is facilitating the movement of this data to *lower privacy protections*.'

In the view of the Office of the Australian Information Commissioner, 'any … expansion of the CDR system should also maintain the strong privacy protections and safeguards that currently exist within the system'. This view was supported by a number of other submissions during the consultation phase preceding the recent CDR amendments.

Considering that trusted advisers are not subject to the accreditation requirements of the CDR framework, the Act may serve as one of the very few controls safeguarding CDR data disclosed to this group of professional service providers. Because of this, we believe that the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021* should *serve as a catalyst for the immediate adjustment or complete elimination of the small business exemption*.

We appreciate the Consultation's emphasis on the problem of additional costs that small businesses may need to bear as a result of implementing privacy law. However, with the amended CDR Rules already in place, we stress that the floodgates have been opened for the CDR data to be channelled from the highly regulated CDR environment to entities that are not subject to CDR information security controls. The Act should therefore be amended to remove the exemption. If a complete abolition of the small business exemption is not feasible, we suggest that all classes of trusted advisers, as defined by the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021*, should not enjoy any exemptions from the application of the Act. This is particularly important if one accepts the argument of some commentators, like the Australian Privacy Foundation, that '[d]ata breaches are a near certainty' and the proper question 'is not if but when'.

Employee records exemption

For the reasons given in our earlier submission, we believe this exemption should be removed. While we note the counter-points made in the Discussion Paper, we observe that there are many provisions in the *Privacy Act* where employer-related regulation does not provide a sufficient substitute. Examples include APP 11 (relating to security) and the data breach notification requirements. Some of the most high profile data breaches internationally relate to employee data in part because this provides a useful vector for broader cyber attacks. None of the arguments raised in the Discussion Paper against repealing the exemption would justify excluding employee records from security-related requirements. If it were felt necessary to retain the exemption to avoid conflict with other legal requirements, the exemption could be re-worded to apply only to those principles and requirements where there is a direct conflict or to provide exemptions that facilitate particular kinds of data processing.

Privacy notices (proposal 8)

The recommendations on privacy notices assume that the best mechanism is a notice written in a natural language (usually English), albeit potentially simplified. However, a better mechanism is to require that such notices be accompanied by a machine-consumable version that answers the questions with which people are most concerned. This might not be *everything* with all the nuance of a privacy notice, but by virtue of being able to be processed by computer systems (including search engines, app stores and the like), it will be more useful to individuals seeking to manage their own privacy. SSIT, of which the SSIT Australian Chapter is part, is the sponsor of a global standard development working group on Machine Readable Privacy Terms Working Group (https://standards.ieee.org/project/7012.html).

Consider, by way of simplified example, a rule that requires the following to be encoded digitally as yes or no responses in a standard format accompanying every privacy notice:

- Might information be used (by the organisation or by those with whom it shares data) in profiling individuals?
- Might information be used (by the organisation or by those with whom it shares data) for marketing purposes?
- Might information be used (by the organisation or by those with whom it shares data) for research purposes without approval by a human ethics governance process, including under the *Data Availability and Transparency Act*?
- Might information be sold or given to a data broker?

- Might information be stored (by the organisation or by those with whom it shares data) outside the jurisdiction?

The restricted practices referred to in proposal 11 could also be the basis of a series of questions that must be answered in the required form.

While privacy notices can still have a natural language nuanced version, encoding answers to these and other simple questions that are important to people means they can automatically limit the organisations with whom they share information through device, software or platform settings. While simplistic, this is likely to have a greater impact on the ability of individuals to control their own privacy than nuanced policies that very few people read.

If the Act will, contrary to the above suggestion, continue to rely on non-digital natural language privacy notices exclusively, there should be a conciseness requirement in addition to a "plain English" requirement that assumes a reading level based on the literacy of at least 95% of the targeted population.

Consent (proposal 9)

Allens Hub researchers have recently published an open access report (funded by the International Association of Privacy Professionals Australia-New Zealand Chapter Legacy Grant scheme) (the 'Consent Report') discussing in detail:

- legal and practical problems with concepts of consent under the *Privacy Act 1998* (Cth) and associated consumer laws; and
- some suggested solutions to these problems. [footnote: Kayleen Manwaring, Katharine Kemp and Rob Nicholls, *(mis)Informed Consent in Australia* (Report for iappANZ, 31 March 2021) <http://handle.unsw.edu.au/1959.4/unsworks_75600>]

We direct the Attorney-General's attention to the Consent Report, in particular sections 2.10, 3.4, 5.5.3, and 6.4.

We would particularly emphasise that consent, even a stronger version of consent than is currently required in the Privacy Act, cannot be a solution to all consumer issues with privacy (as set out in the Consent Report). This problem must be addressed particularly in the light of persistent information asymmetry and other power imbalances and the impossibility of consumers having the time and capability to understand all of the privacy documents presented to them, even with the amendments suggested by the Discussion Paper.

Impact on research (proposal 10.4)

The Discussion Paper asks whether the proposal in 10.4 is likely to have a negative impact on research. That depends in part whether the *Data Availability and Transparency Bill*, which provides an avenue for data to be used for research, is passed. But leaving that aside, data collected for research purposes should flag such purposes as a *primary purpose* and disclose that purpose at the time the data is collected. Surreptitious collection of personal information would be unlikely to pass ethics review in a university context except in narrow circumstances.

Restricted and prohibited acts and practices (proposal 11)

Neither option 1 or 2 in this proposal in their current form are sufficient to protect consumers from harm from these practices.

Option 1 could be strengthened by enforced disclosure to the OAIC (commercial-in-confidence if necessary) of restricted practices undertaken by APP entities, the purposes of those practices, the harms identified, and the steps taken to mitigate those harms.[11]

For Option 2, the efficacy of the consent and notice options suffer from the usual issues set out in our comments on Proposal 9. In contrast, opt-out rights for particular practices are to be encouraged, as long as this does not have the additional consequence that consumers are effectively 'locked out' of receiving the relevant service (unless such information is actually necessary for provision of the relevant service rather than merely a convenient add-on for the provider).

We support the introduction of prohibited practices into the privacy framework, including profiling, behavioural advertising and other forms of 'digital consumer manipulation'[12] knowingly, recklessly or negligently directed at children and other vulnerable people (such as those with disabilities, addictions, mental health problems or the elderly), the scraping of personal information from online platforms, the tracking and sharing of mental health information other than by the individual's own health service providers, or the use of information about an individual's emotional stress, mental or physical health or financial vulnerability to manipulate them for a commercial purpose or is otherwise shown to cause harm or discrimination.[13]

We also suggest that the IC should be granted rule-making power to issue and update an enforceable 'blacklist' for general data collection, use and disclosure practices that are likely to breach the 'fair and reasonable test' (Proposal 10), with a sunset clause to allow time for such practices to be confirmed by the legislature.

Right to erasure (proposals 15.1-15.3)

It is good to see the more detailed thinking about the possibility of introducing a right to erasure in Australia. In our view, there is no need to excessively limit an individual's ability to request erasure, rather the focus should be on the obligations to comply with that request. We particularly support the ability to refuse a request based on "serious threat to the life, health or safety of any individual, or to public health and safety" - this will help prevent the use of the right to preserve the reputation of those who, for example, have a history of family violence.

Automated decision-making (proposal 17)

It is not clear why this proposal would be limited to "automated" decision-making. The concern that people generally have is that it will be used for data-driven decision-making, whether that is through machine learning or through reliance on statistical methods performed by humans. The automation itself is rarely what raises concerns. More discussion of this issue, and whether technology-specific regulation of automation in decision-making is appropriate, is discussed in chapter 5 of Michael Guihot and Lyria Bennett Moses, *Artificial Intelligence, Robots and the Law* (LexisNexis 2020). We are happy to arrange a copy to be sent if that is useful.

[11] Kayleen Manwaring, *Surfing the third wave of computing: Consumer Contracting with eObjects in Australia* (PhD Thesis, UNSW, 2019) http://handle.unsw.edu.au/1959.4/64921 318

[12] Kayleen Manwaring, 'Will emerging information technologies outpace consumer protection law? The case of digital consumer manipulation' (2018) 26(2) *Competition and Consumer Law Journal* 141.

[13] Ibid.

Potential problems in relation to privacy that arise in the context of automated decision-making result from the fact that AI, and in particular machine learning models, encourage greater data collection, sharing and combining. We discuss some of the issues that the use of AI/ML models may cause in sections above.[14] These problems will not be adequately addressed through increased transparency regarding the use of ADM as proposed in 17.1.

Data breach notification (questions in ch 27)

We believe the "serious harm" test should be modified. There are four reasons for this suggestion:

1. an entity deciding whether the "serious harm" test is met may not be aware of the particular situation of the individual (for example, whether they are concerned about violence from a former intimate relationship) and thus may reach inaccurate conclusions;
2. it is possible that, in making the assessment, the entity will not be aware of other available data which might compound the risk to individuals (for example, by facilitating re-identification of publicly available de-identified information about individuals or by forming a crucial part of a mosaic of information about an individual);
3. such high threshold does not reflect the expectation of the public who are concerned with breaches of privacy (and not only 'serious harm');
4. such a high threshold is not in line with international standards such as those under the *General Data Protection Regulation* ('*GDPR*').

Thus, we suggest that the threshold be replaced with something analogous to a reversed onus, where notification is required unless the entity can demonstrate that the risk of harm to an individual and their rights is low.

Security (proposal 19.2)

The proposal here is that the Act include "a list of factors that indicate what reasonable steps may be required". Rather than creating such a list purely for the purposes of the *Privacy Act* (leaving most organisations that operate across jurisdictions complying with multiple such standards), it may be more useful to allow compliance with any of a list of existing standards. The below is adapted from an earlier submission to the Department of Home Affairs on a related point:

> *The use of standards (technical, governance, management) has a number of advantages in the highly technical and rapidly evolving context of cyber security. However, there are also limitations, including the lack of free public availability of many standards instruments, the fact that Australia is too small a market to set its own standards, the fact that standards may be based on patented products and processes, the fact that standards come with a compliance cost, and the fact that some standards are only relevant to part of the challenges (or part of the markets) identified in the Call for Views.*
>
> *We believe the best way forward is (1) for Australia to be involved in standards development for relevant international standards (eg through Standards Australia, the International Organization for Standardization, the IEEE Standards Association, or other professional-based standards bodies) and for this to be appropriately resourced, (2) for requirements, recommendations or labelling to be based on compliance with a suite of standards with*

[14] And also in Zofia Bednarz and Kayleen Manwaring, 'Hidden depths: the effects of extrinsic data collection on consumer insurance contracts', Working Paper 2022, copy held by authors. We are happy to arrange for a copy to be sent if this is useful.

alternatives specified where more than one acceptable standard exists, and (3) for the government to subsidise access to standards to ensure their availability to those (such as consumers, consumer bodies and smaller enterprises) that may not be able to pay the required access fees. The government can also be proactive in supporting the development of an evidence base that can be used by those doing standards development work to better understand Australian industry and consumer needs and expectations. Incorporation of industry-driven technical standards into legal requirements may send a co-regulatory message to the industry, creating a risk of regulatory capture (as industry is involved in standards development). This risk needs to be managed, including by supporting diverse actors (including consumer organisations) to participate in standards development.

Ideally standards will be sufficiently clear and well-aligned with Australian expectations so that they can be followed by businesses and understood by consumers. Legal requirements that reference standards should be specific about which standards (which can involve a choice) constitute compliance. Standards can also be cross-referenced to terminology that can be used in advertising so that "safe" or "secure" is given specific meanings (like "free range" in the context of eggs).

There is no one-size fits all with cyber security standards. Standards adoption needs to be based on risk profiles, industry segment, budget, organisational maturity and likelihood of implementation. While cyber security professionals are well aware of ISO 27001 and NIST standards, these are largely unknown in industry. There are 2,065,523 small businesses in Australia employing less than 19 people, accounting for 97 per cent of all Australian businesses by employee size. Many of these businesses play critical roles in Australia and are often part of supply chains for larger businesses. On the whole, most have no understanding of cyber security, let alone adopting a recognised international framework. The government needs to give options and implementation guidance to small and medium businesses on fit-for-purpose standards and frameworks.

Enforcement (proposal 24)

We welcome the strengthening of the IC's enforcement powers, and the introduction of the industry-funded levies to support the IC's enforcement work. The introduction of the mid-tier civil penalties regime, where the 'serious and repeated interference' threshold is not required to be met, has the potential to assist the development of the OAIC into a true enforcement regulator and the consequent acceptance by industry that privacy compliance is not optional.

The infringement notice scheme suggested in 24.1 should have a place, but processes should be put in place to ensure that it is used only in appropriate circumstances. Considering the OAIC's substantial history as a conciliator rather than an enforcer, and its chronic under-resourcing, actions must be taken to avoid overuse of this scheme in circumstances where the mid- and high-tier civil penalty provisions are more appropriate to promote the public interest. This action is important to avoid issues of regulatory capture and the perception of a 'regulator without teeth', similar to those identified in the Hayne Royal Commission's[15] relating to the over-reliance by ASIC on enforceable undertakings and compensation payments and the consequent poor enforcement of financial services legislation contributing to persistent and serious misconduct by the financial services industry.

[15] *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* ('*RCMBSFS*') (Final Report, 2019).

Additionally, we would support Option 3 in Proposal 24.9, the appointment of a Deputy Information Commissioner - Enforcement, along with an appropriately resourced and skilled team, to concentrate on enforcement issues. This will provide a less complex enforcement regime than a fragmented EDR scheme, and will signal to industry players the importance of compliance with the Privacy Act. We would also encourage the introduction of a knowledge and skills exchange program between Australia's major regulators, particularly the ACCC, ASIC and the OAIC, to promote the efficient and quick creation and maintenance of enforcement regulator competencies.

A direct right of action (proposal 25)

Proposal 25 creates a direct right of action which may be exercised by individuals or groups whose privacy has been interfered with by an APP entity. The proposal requires that the complaint be assessed, first, for conciliation by the OAIC (or a recognised EDR scheme). Following this initial assessment procedure, the complainant could then elect to initiate action in the Federal Court or the Federal Circuit Court 'where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation' (proposal 25.1). In any of these cases, the complainant would need to seek leave of the court to make the application. Finally, the proposed model grants the OAIC the power to appear as amicus curiae to provide expert evidence at the request of the court.

This proposed model suffers from several flaws in its current form:

First, as noted in the discussion paper itself, there are several reasons to avoid the unnecessary hurdle of the initial assessment, including causing unnecessary delays, increasing procedural complexity, and limiting individuals' access to justice. This problem is particularly pronounced in the proposed model, as it is suggested that the application is conditioned upon the granting of leave from the court, creating a double barrier. Where advisable, a conciliation or mediation process can be initiated by the court itself, in suitable cases. Conditioning the application to the court with a preliminary assessment process can therefore limit individuals' access to justice without an appropriate justification. An effective privacy regime requires an unconditional and easily accessible right of action, which can provide affected individuals and groups with a low cost and easy way to exercise their rights. The GDPR provides a good example for such a model. It allows those affected to choose their preferred course of action and does not condition the right of action upon a prior administrative assessment process. While affected individuals have a right to lodge a complaint with the supervisory authority (GDPR Article 79), and if they choose to do so, they have a right to an effective judicial remedy against the supervisory authority (GDPR article 78), this route does not bar them from exercising their right to an effective judicial remedy against a controller or processor (GDPR article 79). Therefore, individuals who consider that their rights under the GDPR have been infringed have a direct and unconditional right to an effective judicial remedy at a state court 'where the controller or processor has an establishment' or 'where the data subject has his or her habitual residence' (unless the controller or processor is a public authority acting in the exercise of its public powers).

Second, while we agree that granting the OAIC the power to provide, where appropriate, expert evidence is a useful component of the proposed model, this feature highlights the inequalities between parties that are embedded in the proposed model. Affected individuals would typically lack the expertise or resources that the data entities and government bodies entail, and only a small portion of affected individuals are expected to have the resources required for a complex and prolonged legal process. This problem can be mitigated by allowing NGOs with expertise in this area to intervene and represent affected individuals. The GDPR can serve as a good example for such a model. To make it easier and more accessible for individuals to exercise their right to effective judicial remedy, the GDPR provides individuals the right to mandate a not-for-profit organisation to lodge the complaint or to exercise the rights on their behalf. This delegation of the right to action to a designated NGO enhances individuals' right of action significantly and mitigates inequality in both resources and expertise required for litigation.

Third, even if affected individuals would be allowed to designate an NGO to represent them, litigation in Federal courts can be costly and inaccessible to many Australians. The discussion paper notes that there may be a possibility to create a 'small claims procedure' for privacy claims, but warns that this may not be feasible in light of the existing caseload and resourcing of the Federal courts. Therefore, we submit that any effective judicial remedy for privacy harms must be designed to provide a rapid no- (or low-) cost judicial process, whether as a special procedure within the Federal courts (mandating the necessary resources), or through establishing or delegating to a tribunal.

Issues with biometric identifiers (see question at p35 of Discussion Paper)

Biometric identifiers raise particular concerns, and may require increased protections. Alternatively, protections for sensitive information, defined to include biometric information, could be enhanced more broadly.

Biometric information is collected by specific technical methods and processing to represent physical, physiological and/or behavioural characteristics of a natural person that allow and confirm unique identification of that natural person. These types of biometric identification are sensitive due to being biologically distinct to each individual like facial images or voice-prints. Unlike other personal information, in any situation where the biometric information may be compromised, an individual is exposed to risk and with no recourse to replacement.

In some jurisdictions, biometric identifiers are defined and then subjected to specific additional requirements. For example, "biometric identifiers" defined in Illinois' *Biometric Information Privacy Act 2008* (or BIPA) 740 ILCS 14/15[16] are subject to specific requirements and enforcement. [17]

Biometrics are a growing market. For example, voice biometrics market size is predicted to expand from $984 million in 2019 to up to $2.8 billion by 2024.[18] It is used in Australia, including by the Australian Tax Office.[19] Opting in to the Australian Tax Office voice biometrics system simply requires the user to repeat a phrase three times; there is no detailed information provided on risks of participation and no opportunity to replace the voiceprint. Even with consent, there are privacy

[16] Biometric Information Privacy Act. (740 ILCS 14/5). Sec. 5. BIPA requires any private entity in possession of biometric data develop a public, written policy "establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information." Accessed 10 January 2022 https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

[17] See, Lazxarotti and Atrakchi 'As Voice Recognition Technology Market Surges, Organizations Face Privacy and Cybersecurity Concerns.' October 2020. Accessed: https://www.workplaceprivacyreport.com/2020/12/articles/biometric-information/as-voice-recognition-technology-market-surges-organizations-face-privacy-and-cybersecurity-concerns/ or class action cases, such as, https://www.classaction.org/media/mcgovern-et-al-v-amazon-web-services-inc.pdf

[18] Market research indicates growth in this market driven by law enforcement and banking, financial and insurance sectors see — https://www.researchandmarkets.com/reports/5146201/global-voice-recognition-biometrics-market-2020

[19] https://www.csoonline.com/article/3546188/voiceprint-authentication-starts-to-go-mainstream-in-australia.html. Voice biometrics were added to the ATO app in 2016, making it the first deployment across call centre and app in Australia.

issues in the use of voiceprint data,[20] particularly given the fact that most people do not know how such data is processed and used[21] and voice prints may reveal sensitive information.

There are measures that could be introduced into the *Privacy Act* to better protect individuals in the context of biometric information, drawing on examples such as BIPA. This could strengthen proposals 11.1 and 11.2 and 14.1. In particular:

- drawing on BIPA, the Privacy Act could introduce a definition of biometric identifiers;
- there could be a requirement that the use of biometric identifiers is *necessary* in the context of a particular purpose (in other words, that less risky alternatives would be insufficient to achieve the purpose);
- mandatory PIA risk assessment for the use of biometric identifiers;[22]
- a requirement be introduced that identified risks be mitigated,[23] including through *destruction* rather than de-identification or anonymisation of biometric information, reduced maximum retention periods, and an ability to withdraw consent (see proposal 14.1).

Alternatively, it may be appropriate to extend such requirements to *all* sensitive information, defined to include biometrics.

Yours sincerely,

Lyria Bennett Moses (UNSW Allens Hub and IEEE SSIT)

Greg Adamson (IEEE SSIT)

Zofia Bednarz (UNSW Allens Hub)

[20] A stored voiceprint captures more than 140 unique physical and behavioural characteristics of a person and enables other information to be inferred such as gender, demographics, ethnicity or education level — see Privacy Commissioner of New Zealand ‘Taking the measure of biometrics‘, https://www.privacy.org.nz/blog/taking-the-measure-of-biometrics/. In such cases, government collection, retention, and use of biometrics must be necessary as well as proportionate to user privacy needs and a legitimate security goal.

[21] In 2019, voice biometric data from roughly five million people collected by UK's HMRC tax authority was deemed in violation of the EU's General Data Protection Regulation, despite informed consent, and the Information Commissioners Office (ICO) said the HMRC taxation office failed to give customers sufficient information about how their voiceprint data would be processed and ordered to be deleted, despite consent. https://www.biometricupdate.com/201905/biggest-ever-deletion-of-biometric-ids-from-a-state-held-database-to-be-carried-out-by-uk-tax-authority.

[22] This would be preferrable over the proposed OAIC and CSIRO's Data61 De-Identification Decision-Making Framework which is non-binding and the PIA as overall risk management and planning processes of APP entities set a mandate threshold set when requiring collection of biometric data, even with consent. https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment

[23] These could also include use of regulatory sand-boxes as noted in the AGD Discussion Paper and stated in the UK 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.

Anton Didenko (UNSW Allens Hub)[24]

Shiri Krebs (Deakin CSRI)

Kayleen Manwaring (UNSW Allens Hub and IEEE SSIT)

Simon Taylor (UNSW Allens Hub)

[24] The research conducted by Anton N Didenko was funded by the Australian Government through the Australian Research Council (project FL200100007 'The Financial Data Revolution: Seizing the Benefits, Controlling the Risks'). The views expressed are those of the author and are not necessarily those of the Australian Government or Australian Research Council.