DIGITAL
LAW
ASSOCIATION

SUBMISSION

Review of Privacy Act 1988

24 January 2022

Disclaimer and Copyright

While the DLA endeavours to ensure the quality of this publication, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this publication.

© The Digital Law Association (DLA)

ABOUT THIS SUBMISSION

The Digital Law Association is an organisation dedicated to the promotion of a fairer, more inclusive, and democratic voice at the intersection of law, policy and technology.

Our mission is to encourage leadership, innovation, and diversity in the areas of technology and law by:

- bringing together the brightest legal minds in the profession and in academia to collaborate; and
- developing a network that promotes digital law, and particularly female leaders in digital law.

This document was created by the Digital Law Association in consultation with its members. In particular, the compilation of this submission was led by:

- Angelina Gomez
- Susannah Wilkinson

This submission has been contributed to by the following Digital Law Association members:

- Caden Atzeni
- Natasha Blycha
- Eleanor Brooker
- Heather Delfs
- Amiinah Dulull
- Darren Hart
- Anna Jaffe
- Erin Kanygin
- Joni Pirovich
- Eloise L’Estrange
- Dr Jenny Ng
- Emily Price
- L Rich
- Sean Tran
- Emiko Watanabe

Submission Process

In developing this submission, our members have engaged through email correspondence, video calls, and worked in teams to conduct research and prepare briefing papers about the issues dealt with in the third issues paper.

Recommendation #1	***In order to better understand and conceptualise future amendments to the Act, that personal information be characterised as property owned by the individual to whom the information relates, which the DLA recommends is included as an Australian Privacy Principle.***
Recommendation #2	***That review and consideration of amendments to the Privacy Act take into account the principles relating to Control, Notice/Consent, Organisational Accountability, International Consistency, National Consistency and Education, in addition to the Australian Privacy Principles.***
Recommendation #3	***That the definition of personal information be amended by replacing the word 'about' with 'relates to' in order to extend the application of the definition to a wider range of information and for international consistency.***
Recommendation #4	***That the definition of personal information be amended to include a non-exhaustive list of the types of information capable of being covered by the definition of personal information using the equivalent list from the GDPR with the further addition to the definition of the words 'racial, ethnic and gender'.***
Recommendation #5	***That the definition of personal information be amended by adding the words "directly or indirectly" after the words "reasonably identifiable".***
Recommendation #6	***That the definition of 'collection' be amended to expressly cover information obtained from any source and by any means, including inferred or generated information.***
Recommendation #7	***That the Privacy Act be amended to require personal information to be anonymous before it is no longer protected by the Act.***
Recommendation #8	***Digital identity is the cornerstone of the digital economy and any legislation enabling a digital identity system should be broad enough to safely unlock the benefits of the digital economy but with rights and freedoms protected in a bill of digital rights and freedoms.***
Recommendation #9	***That processes or system in which personal information is collected, used and disclosed are designed in a way that assures a person's privacy is protected and safeguarded. These systems should be designed with data stewardship principles in mind, and with the benefit of latest review process on identification of ethical issues with technology design.***
Recommendation #10	***That collection, use or disclosure of personal information under APP 3 and APP 6 must be fair, reasonable, lawful and transparent in the circumstances.***
Recommendation #11	***That Option 1 from the Discussion Paper be adopted to provide a list of restricted practices that require reasonable steps to identify privacy risks and implement measures to mitigate those risks, but that the proposal be scrutinised to ensure it is adequately robust to accommodate impacts of emerging technologies such as AI and quantum.***

Recommendation #12	***That this recommendation be reconsidered in light of the Principles noted in section 3.1 of this submission. That education is provided to consumers in respect of how individuals can avail themselves of this right.***
Recommendation #13	***That the right to erasure of personal information be reconsidered in light of the Principles noted in section 3.1 of this submission and Article 17 of the GDPR.***
Recommendation #14	***That the Privacy Act be amended to include protections with regards to automated individual decision-making, including profiling in line with Article 22 of the GDPR.***
Recommendation #15	***That proposal 18 be reconsidered in light of the Principles noted in section 3.1 of this submission, and that education is provided to individuals in respect of how they can avail themselves of this right.***
Recommendation #16	***That proposal 20 be implemented so that organisational accountability of APP entities extend to both primary and secondary purposes for which personal information is collected.***
Recommendation #17	***That the role of Federal Privacy Ombudsman be created that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR schemes, with appropriate funding to act proactively in pursuing enforcement.***
Recommendation #18	***That proposal 25 be adopted to create a direct right of action for an individual to litigate a claim for breach of their privacy under the Act.***
Recommendation #19	***That Option 1 of proposal 26.1 be adopted to introduce a statutory tort for invasion of privacy specifically allowing for claims of damages for emotional distress and loss of control over an individual's data (and corresponding statutory guidance on formulation and quantum of such claims).***

1. Review of Privacy Act 1988 (Cth)

1.1. Summary

The Digital Law Association's (**DLA**) submission focusses on the question of, 'What is personal information?'. This question is critically important because the answer provides the lens through which the DLA considers all amendments to the Act should be analysed and provides a unifying objective for the Act. The DLA considers that personal information should properly be characterised as the property of the individual. The DLA uses this characterisation to analyse proposed amendments to the Privacy Act and identify key principles that must be addressed in any amendments to the Act namely: Control, Notice/Consent, Organisational Accountability, International Consistency, National Consistency and Education.

1.2. Introduction

Data flow is complex, and its complexity is increasing exponentially as Australia moves towards becoming a leading digital nation. The DLA welcomes this important and timely review of the *Privacy Act 1988* (Cth) (the **Privacy Act** or the **Act**) and acknowledges that it seeks to bring together a number of initiatives over the past 15 years to modernise our privacy regulatory landscape to ensure that Australia is ready to take advantage of the opportunities in the growing digital economy while safeguarding the rights of individuals to privacy.

The digital economy allows individuals to benefit from, and interact with, a range of products and services across the globe that would have been unheard of not that long ago. The data from these interactions can be used and aggregated from different data sources[1] and can create issues for privacy protection. Essentially, the aggregation of data from various sources can create a 'mosaic effect' and 'shadow profiles' that can identify, or relate to, an individual with or without the individual's knowledge or consent, and these have the potential to infringe on the right to privacy.

This data ecosystem is being shaped by the rise of companies that collate, process/analyse and trade in consumer data to advertise, influence, target, profile, determine resource allocation and measure policy effectiveness. Enterprise data and the Internet of Things (IoT) are increasingly being added to this data landscape, as well as technical information which can create inferred personal data. This ecosystem creates both opportunity for the abundance of data to be used to better the lives of individuals (e.g. AI learning tools) and risk that individuals will lose privacy protections with the collection and use of this data.

New ways of analysing and using data together with the application of emerging technologies means that the complexity of this data ecosystem will likely increase exponentially in the coming years. This is an opportune time to lay the foundations of a legal framework for privacy that will be agile and robust enough to safely and sustainably encourage wide scale adoption of new technologies – e.g. Artificial Intelligence (**AI**),[2] machine learning (given the intent under Australia's AI Action Plan to be a global leader in developing and adopting trusted, secure and responsible AI) and quantum computing

[1] Data sources may differ by the entity collecting the data, geography, time, purpose etc.

[2] Australia's Artificial Intelligence Action Plan https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-action-plan/strategic-vision.

(given Australia's positioning to take advantage of $4 billion revenue),[3] without undermining the current approach to and concepts of privacy – and address the questions that will arise, such as: Who should control data obtained from smart machines, smart vehicles or smart cities? How do we protect privacy when interacting with web 3.0/the metaverse?[4] Are we able to protect our personal information stored in our digital twin?[5] Should your digital twin be entitled to privacy considerations (e.g. after an individual's death)? While protecting an individual's privacy is not the answer to all these questions, it is an important starting point.

While the future is impossible to predict with clarity, what is obvious is that there will be an increasing number of touch points where individuals will leave a data trail from their interactions in the digital realm with an ever increasing number of companies, government agencies, organisations, service providers, and other individuals. These increasing touch points will result in data aggregation and the inevitable situation where data is used in ways that may well be different to the purpose for which collection was intended or 'consented to'.

These developments only increase the difficulty an individual faces when protecting their privacy – in controlling their personal data, in understanding the potential implications of sharing that data and in providing meaningful consent. Any amendments to the Privacy Act to address these difficulties must be considered from the perspective of how entities will effectively be able to provide these protections. As supply chains become complex and more global, it is important to acknowledge the complexity faced by entities navigating relevant regulations and implementing solutions for their customers. Effective privacy protection laws must as far as possible offer consistency both nationally (Commonwealth and the States) and internationally (e.g. by aligning with the most universally adopted privacy regulations, the EU's General Data Protection Regulation (**GDPR**)). Responsible use of personal information will only be effective if the organisations have a common understanding of what is responsible, reasonable, fair and lawful.

The GDPR is widely accepted as the benchmark in privacy protection. Recognition by key players in the data economy further signals acceptance of this regulation. By way of example, Google CEO Sundar Pichai in a BBC Interview,[6] praised the GDPR, stating it provided companies with a framework to comply with, and that it gave users guarantees.

[3] CSIRO, 'Growing Australia's Quantum Technology Industry' https://www.csiro.au/en/work-with-us/services/consultancy-strategic-advice-services/csiro-futures/futures-reports/quantum; Lane Campbell, 'Worse Than Y2K: Quantum Computing And The End Of Privacy', *Forbes* (18 April 2018) https://www.forbes.com/sites/forbestechcouncil/2018/04/18/worse-than-y2k-quantum-computing-and-the-end-of-privacy/?sh=62ca963d4829; Cameron Kerry, 'Protecting privacy in an AI-driven world', *Brookings* (10 February 2020) https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/.

[4] Jonathan Vanian, 'Mark Zuckerberg's metaverse may be as privacy flawed as Facebook', *Fortune* (30 October 2021) https://fortune.com/2021/10/29/mark-zuckerberg-metaverse-privacy-facebook-meta/; The University of Sydney, 'Facebook and the Metaverse: should we be worried about privacy?' (29 October 2021) https://www.sydney.edu.au/news-opinion/news/2021/10/29/facebook-and-the-metaverse-should-we-be-worried-about-privacy.html; SBS, 'Facebook's 'metaverse' triggers data mining, privacy concerns from experts,' *SBS News* (29 October 2021) https://www.sbs.com.au/news/facebook-s-metaverse-triggers-data-mining-privacy-concerns-from-experts/3a302b6e-664d-4096-b7b9-fef8d057b632; Kate O'Flaherty, 'Why Facebook's Metaverse Is A Privacy Nightmare', *Forbes* (13 November 2021) https://www.forbes.com/sites/kateoflahertyuk/2021/11/13/why-facebooks-metaverse-is-a-privacy-nightmare/?sh=40c7aa856db8.

[5] Andrzej Kawalec, 'How To Protect Your Digital Twin', *Forbes* (21 October 2019) https://www.forbes.com/sites/forbestechcouncil/2019/10/21/how-to-protect-your-digital-twin/?sh=6b90f4316253; National Law Review, 'Digital Twins and Your Health' (18 January 2022) https://www.natlawreview.com/article/digital-twins-and-your-health; Mireille van Hilten, Elsje Oosterkamp & Marc-Jeroen Bogaardt, 'The use of digital twins in healthcare: socio-ethical benefits and socio-ethical risks' (2021) 17(6) *Life Sciences, Society and Policy* https://lsspjournal.biomedcentral.com/articles/10.1186/s40504-021-00113-x.

[6] Aaron Hurst, 'Global frameworks the way forward for AI and data privacy — Google CEO', *Information Age* (14 July 2021) https://www.information-age.com/global-frameworks-way-forward-for-ai-and-data-privacy-google-ceo-123496121/.

Mr Pichai said that more of this kind of regulation would be needed over time, for example in relation to managing AI.

The proposed amendments to the Privacy Act need to be able to address the salient legal issues arising from our rapidly evolving digital world. The DLA believes that the review should seek to understand and answer fundamental questions about the nature and objectives of privacy laws in our fast-digitising and rapidly changing world. We are concerned that the Discussion Paper does not address these fundamental questions, which we expand on in the below sections of the DLA's submission.

2. Characterisation of Personal Information

Before any considerations as to what amendments are required to better empower individuals to protect their data and serve the Australian economy, a fundamental question needs to be answered: What does the Act seek to protect? That is, what is the proper characterisation of *"personal information"*? We believe that this question is fundamental because the answer provides a clear overarching lens through which to consider this review, the amendments proposed as part of the review, and ultimately the Act itself.

2.1. What is personal information?

Recommendation 1

> ***In order to better understand and conceptualise future amendments to the Act, that personal information be characterised as property owned by the individual to whom the information relates, which the DLA recommends is included as an Australian Privacy Principle.***

Personal information is characterised as property for the purposes of protecting it, but it is also in some cases intrinsic to a person's identity (including in the case of sensitive information).

Professor Alan Westin, a significant figure in privacy scholarship in his classic, *Privacy and Freedom* identified privacy as, *"the claim of individuals…to determine for themselves when, how and to what extent information about them is communicated."*[7] Simply, if individuals can protect and decide on and control access to their personal information in order to exercise commercial and privacy rights, the power dynamic shifts back to the individual from organisations (e.g. some tech service providers/digital platforms provide 'free' services in exchange for collecting and amassing huge quantities of marketable data from which they are able to create a mosaic of personal information that identifies individuals and user preferences).

Personal information is the *"new oil"*[8], although not a finite resource, with value generated through data analytics. The DLA considers that appropriate treatment of personal information (i.e., information that relates to an individual who is reasonably identifiable), is so significant against this backdrop of data consumption, that personal information must be accorded property rights in order to afford adequate remedies and enforcement and the protection of the fundamental human right to privacy. Simply, an

[7] Alan Westin, *Privacy and Freedom* (Ig Publishing, 2015).

[8] Meglena Kuneva, 'Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling' (Speech, European Consumer Commissioner, 31 March 2009); World Economic Forum, '*Personal Data: The Emergence of a New Asset Class*' (January 2011).

individual must be recognised as the owner of their own information. This characterisation empowers an individual and guards against arbitrary interference from the State or any other actors.

This characterisation aligns with the conceptualisation of *"personal data"* as property by the EU in its GDPR – a key piece of regulation with substantial international acceptance and case law guidance. *"Personal information"* in the California Consumer Privacy Act and in Canadian Privacy regulations (Privacy Act and the Personal Information Protection and Electronic Documents Act), is also conceptualised as property – see Schedule 2 for the DLA's review of personal information/data in these regulations and other overseas jurisdictions.

3. Principles to Guide Protection of Privacy

3.1. Principles

Recommendation 2

> ***That review and consideration of amendments to the Privacy Act take into account the principles relating to Control, Notice/Consent, Organisational Accountability, International Consistency, National Consistency and Education, in addition to the Australian Privacy Principles.***

Using the lens of personal information as property, these are the key principles that the DLA considers should be a guide to privacy protection (in addition to the Australian Privacy Principles) – when analysing and deciding on any amendments to the Privacy Act:

(a) **Control** **–** Individuals should have control over their personal information. They should be allowed to licence (permit) use (by consent), cancel that licence (withdraw consent), request the erasure, correction or alteration of personal information and to seek redress for interferences with their privacy (e.g. misuse of their personal information). However, individuals should not be allowed to permanently divest themselves of all their personal information (i.e., to sell their identity), as some personal information is intrinsic to an individual's identity.

(b) **Notice/Consent** **–** There should not be an overreliance on notice and consent mechanisms.[9] It is the DLA's view that focussing on notice/consent unfairly shifts onus/responsibility away from organisations that collect and process data to individual consumers. Digital devices are interconnected and personal data is routinely collected without much awareness or consent, especially as permissions are often buried in fine print. Given the complexity of data use, it is not realistic for an individual to always be in a position to understand the often lengthy terms and conditions to be able to give genuine informed consent or be able to predict the long term consequences of giving that consent. In many cases, individuals may not be aware that they are sharing their personal information or if they are, how to protect their privacy when they do.[10]

[9] Consent should not be the only line of defense when it comes to protecting personal information: Dawn Lo, 'Should you know (or care) how your data is being used before you consent?', *UNSW Sydney* (27 August 2020) https://newsroom.unsw.edu.au/news/business-law/should-you-know-or-care-how-your-data-being-used-you-consent; Leon Trakman, Robert Walters and Bruno Zeller, 'Digital Consent and Data Protection Law – Europe and Asia-Pacific Experience' (Law Research Paper No 20-10, UNSW, 7 February 2020) http://dx.doi.org/10.2139/ssrn.3538860.

[10] In a 2020 Australian survey, 85% of respondents consider that they understand that they should protect their personal information but are less sure how they can do this (49% agree). 59% care about data privacy, but don't know what to do about

There is often a disconnect and lack of transparency between what consumers think is being collected and what is actually being collected, and also between how consumers think information will be used and how that information is actually used.[11] Essentially, while notice and consent are fundamental to many privacy and data protection regimes, practically, they can only be effective when used judiciously and combined with the other principles (such as control and accountability) to avoid consent fatigue, and to prevent the burden resting too heavily on the individual.

(c) **Organisational accountability** – Entities that collect and process personal information should be accountable to individuals and regulators. The Act should treat these entities as 'trusted custodians of that information' and provide the mechanisms for those entities to establish, maintain and demonstrate that trust.

Put another way, these entities should collect and process personal information in a fair, reasonable, lawful and transparent manner in relation to the individual[12] and must be able to demonstrate compliance.[13] Consequently, privacy law should regulate the collection and processing (i.e., use and disclosure) of personal information. Laws that affect privacy, that allow organisations to collect, process and use personal information should provide proper safeguards against interference. They should be precise, and not give decision-makers too much discretion in authorising interferences with privacy. This includes having in place enhanced mechanisms to enforce compliance with the Act. There must be effective mechanisms to encourage compliance and remedy noncompliance. The relevant regulators should be well-resourced, be able to resolve complaints in a timely and efficient matter and should have sufficient powers to take a proactive role in enforcement and in monitoring industry compliance.

(d) **International consistency** – Given that the digital world does not pay particular heed to national boundaries, to ensure interoperability and to better facilitate cross-border transfers of information, the Privacy Act should align with overseas regimes, in particular the GDPR. This would result in consistent and predictable standards for industry, and would also make it more likely that individuals would understand how their information was being used/protected (and therefore also help to reduce the reliance on, for example, individual notices or consent mechanisms to explain the jurisdictional differences). The DLA has prepared a schedule comparing international regulations on privacy covering issues that we consider important to review and ensure alignment – with regards to the proposed amendments to the Privacy Act (see Schedule 2).

it. See OAIC, 'Australian Community Attitudes to Privacy Survey 2020', 43 https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page.

[11] In a Eurobarometer several years ago, only 18% of respondents reported reading privacy policies fully and 49% partially, length and complexity being typical reasons for not reading them. In fact, many habitually accept consent dialogues without even glancing the provided information. See Tuukka Lehtiniemi and Yki Kortesniemi, 'Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach' (2017) 4(2) *Big Data & Society* https://doi.org/10.1177/2053951717721935.

[12] Pricewaterhousecoopers Business Solutions SA was fined €150,000 for failing to ensure of lawful, fair and transparent processing of its employees' personal data, see EDPB, 'Company fined 150,000 euros for infringements of the GDPR' (31 July 2019) https://edpb.europa.eu/news/national-news/2019/company-fined-150000-euros-infringements-gdpr_en; and in Sweden, the Data Inspectorate fined a school in the town of Skellefteå, for processing sensitive personal data unlawfully (re the use of facial recognition technology to monitor student attendance), see EDPB, 'Facial recognition in school renders Sweden's first GDPR fine' (22 August 2019) https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv; BBC News, 'Facial recognition: School ID checks lead to GDPR fine' (27 August 2019) https://www.bbc.com/news/technology-49489154.

[13] The GDPR's *"legitimate interest"* test is a useful guide here and will assist in aligning Australia with international standards.

(e) **National consistency – **The privacy issues and potential harms faced by Australians are the same regardless of geographical location and the DLA is concerned at the lack of uniformity between State and Commonwealth regulations – as there are numerous regulations in Australia that deal with personal information and privacy. These need to be reviewed for consistency and harmonised. The DLA illustrates this point through a schedule comparing State/Commonwealth regulations that control aspects of personal information (e.g. health records) and privacy that we consider important with regards to the proposed amendments to the Privacy Act (see Schedule 1).

The DLA considers that all State and Commonwealth regimes that have the potential to impact privacy should be consistent. Consequently, the DLA is of the strong view that all States and the Commonwealth (with regards to other regulations) should harmonise with the Privacy Act (as amended). For example, the definition of personal information, how fair and reasonable data collection and use is expressed and what rights an individual has to correct, alter or delete their personal information require harmonisation across the various regulations.

The DLA further considers that regular reviews should be carried out to ensure continued consistency, and that the Commissioner be approached for comment on any new legislation (or amendments) that has the potential to be inconsistent with the Privacy Act's protection of personal information.

(f) **Education –** It is important that there is continued focus on educating society of the potential harm from unregulated use of personal information, their rights and of how the law will protect them from harm and their personal information from misuse. Successful data protection concerns a wide range of stakeholders and requires a whole-of economy approach.

4. Proposed amendments in the Privacy Act Review October 2021

4.1. Proposal 2 – Definition of Personal Information

Proposal 2.1 – Recommendation 3

> ***That the definition of personal information be amended by replacing the word ‘about’ with ‘relates to’ in order to extend the application of the definition to a wider range of information and for international consistency.***

The DLA agrees with the proposal for the reasons stated in the Discussion Paper. The DLA agrees that this is an important amendment as it widens the application of the Privacy Act to not just information about an identified individual, or an individual who is reasonably identifiable but leaves open the possibility of compounding information that relates to an individual that can lead to identification.

Proposal 2.2 – Recommendation 4

> ***That the definition of personal information be amended to include a non-exhaustive list of the types of information capable of being covered by the definition of personal information using the equivalent list from the GDPR with the further addition to the definition of the words ‘racial, ethnic and gender’.***

The corresponding GDPR definition states (Article 4(1)):

> *… an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, racial, ethnic, gender or social identity of that natural person;* (underlined addition by the DLA)

The words underlined have been added to address the importance of issues of race and ethnicity (*Privacy Act 1985* (Canada), section 3) and gender (in 2017, the United Nations Human Rights Committee reiterated that the right to privacy covers gender identity).[14]

Proposal 2.3 – Recommendation 5

> ***That the definition of personal information be amended by adding the words "directly or indirectly" after the words "reasonably identifiable".***

The DLA agrees with the proposal for the reasons stated in the Discussion Paper.

Proposal 2.4 – Recommendation 6

> ***That the definition of 'collection' be amended to expressly cover information obtained from any source and by any means, including inferred or generated information.***

The DLA agrees with the proposal for the reasons stated in the Discussion Paper.

Proposal 2.5 – Recommendation 7

> ***That the Privacy Act be amended to require personal information to be anonymous before it is no longer protected by the Act.***

The DLA agrees that the Privacy Act should be amended to require information to be anonymous rather than de-identified for the Act to no longer apply. In light of the danger of data obtained from various sources forming a pattern that is able to identify an individual, requiring information to be anonymous would force entities to meet this higher, irreversible standard and increase consumer protection. The GDPR in Recital 26 recognises that personal data which has undergone pseudonymisation should be considered to be information on an identifiable natural person, if it could still be attributed to a natural person by the use of additional information.

This continued protection is important as the risk profile of de-identification is high – it has the potential to render the protections of the Privacy Act moot. This is because if re-identification of an individual is possible, then it opens up the possibility of breaches of privacy that could have significant impact on an individual but for which the individual has no protection. This continued protection will need to be monitored by the Regulator (for potential further amendments to the Act) as industry gets more sophisticated in combining data sets, and the difficulty for any data set to be *"truly, robustly anonymous – given how the risk of re-identification demonstrably steps up with even just a few attributes available"*.[15]

[14] Human Rights Committee, *Views: Communication No. 2172/2012,* 119th sess, UN Doc CCPR/C119/D/2172/2012 (2 December 2011).

[15] Natasha Lomas, 'Researchers spotlight the lie of 'anonymous' data', 24 July 2019 https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/: *"Researchers from two universities in Europe have published a method they say is able to correctly re-identify 99.98% of individuals in anonymized data sets with just 15 demographic attributes."*

4.2. The role of self-sovereign identity as a solution to privacy & protection of personal information[16]

Recommendation 8

> ***Digital identity is the cornerstone of the digital economy and any legislation enabling a digital identity system should be broad enough to safely unlock the benefits of the digital economy but with rights and freedoms protected in a bill of digital rights and freedoms.***

Recommendation 9

> ***That processes or system in which personal information is collected, used and disclosed are designed in a way that assures a person's privacy is protected and safeguarded. These systems should be designed with data stewardship principles in mind, and with the benefit of latest review process on identification of ethical issues with technology design.***

Digital identity is the cornerstone of the digital economy and due to the complex interactions in the digital world, personal information, privacy and the digital rights and freedoms of Australians are inextricably linked. Consequently, the DLA encourages consideration by the Attorney-General of implementing a digital identity management system to better facilitate its goals of better empowering consumers, protecting their data and serving the Australian economy. Simply, what the DLA supports is a shift both in mindset and reflected in regulation from the collection of 'as much as possible' personal information as a requirement for access to services, to the collection of minimal data to provide the service. The collection of data should be limited to what is required by law (KYC) and necessary to provide the service. For example, where a post code will suffice instead of an individual's home/work address or where one method of contacting an individual will suffice (email or mobile) as opposed to providing multiple points of contact.

There are various types of identity management systems in the digital world, consisting of centralised identities, user-oriented identities, federated identities, and self-sovereign identities (**SSI**).[17] Available digital identity management systems are evolving from completely centralised to more decentralised approaches in the pursuit of guaranteeing data protection, portability, and interoperability.[18] SSI is considered the next evolutionary stage of digital identities.[19]

Under an SSI system, distributed ledger technology can serve to create a permission-less, interoperable, and decentralised digital identity framework.[20] The user is the administrator of their identity and has much more control over their data and information than others have, know, or share about them. Unlike centralised, third-party, and federative models (i.e., Australia's Digital Identity Framework), the SSI approach does

[16] This section draws on submission made by the Digital Law Association on Digital Identity available at Digital Law Association, 'Australia's Draft Digital Identity Legislation', https://storage.googleapis.com/production-domaincom-v1-0-2/012/433012/QL37nvIy/b1eb894493c7488d9b8da7c643359987?fileName=211027%20-%20Digital%20Law%20Association%20submission%20to%20Australias%20Digital%20Identity%20Legislation.pdf.

[17] Fraunhofer Institute, 'Self-Sovereign Identity Foundations, Applications, and Potentials of Portable Digital Identities Project Group Business & Information Systems Engineering', *Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT* (2021) 9.

[18] Marco Lopez, 'The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain Interamerican', *InterAmerican Development Bank* (Publication, September 2020) 14 https://publications.iadb.org/publications/english/document/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignity-Digital-Wallets-and-Blockchain.pdf

[19] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya and Christoph Meinel, 'A survey on essential components of a self-sovereign identity' (2018) 30 *Computer Science Review*, 80–86.

[20] Jonathan Lim, 'Self-sovereign identity: the harmonising of digital identity solutions through distributed ledger technology' (2020) 1(2) *ANU Journal of Law and Technology* 97.

not require an entity for managing people's identity. Neither an identity provider nor a service provider, such as the accredited identity service provider envisioned in the Australian Digital Identity Framework,[21] is needed to manage one's credentials and authenticators on their behalf. With SSI, an identity provider effectively becomes an identity issuer.[22]

The main benefit of the SSI system includes the facility to enable interoperability between different solutions.[23] As the cryptographic proofs of ownership are found on a decentralised network, the adoption of SSI protocols and standards would allow for private and public entities to store proofs of information within the same accessible decentralised networks.[24] With respect to Australia's Framework, it appears that onboarding entities may have to comply with any technical standards issued by the Oversight Authority,[25] and to date the TDIF requirements have not permitted SSI technology to be 'accredited'.

SSI models hold the potential to be highly scalable; however, this is also dependant on the implementation of proper trust frameworks, mature and robust decentralised ledgers, and proper regulations.[26] In a federated identity management system, such as Australia's existing (although not enough entities became accredited to fulfil the federated identity system) or proposed system, the low number of identity providers, and their burden to maintain large infrastructures and assume high costs to provide security can render them less reliable and scalable than an SSI system.[27]

The Federal Republic of Germany, the Kingdom of Spain and Finland have recently partnered with one another to pursue opportunities for collaborating on cross-border digital identity based on SSI, to ensure that all solutions and components of digital identity will meet European standards and reflect European ethical values on digital sovereignty.[28] Through their partnership, they aim to ensure the sharing of best practices and knowledge (technical, regulatory, operational) in the sphere of digital identity and SSI, and are designing and conceptualising a cross-border pilot to be implemented in 2022.[29] There have also been other regional efforts to develop public-permissioned regional networks, such as European Blockchain Services Infrastructure in Europe and LACChain in Latin America.[30] This is the sort of effort and partnerships that the DLA encourages the Attorney-General to initiate in conjunction with efforts by the Digital Transformation Agency and the Australian Human Rights Commission.

[21] Exposure Draft: Trusted Digital Identity Bill 2021 (Cth) s 7.3.3 ('*Trusted Digital Identity Bill*').
[22] Lopez (n 18) 21.
[23] Ibid 98.
[24] Ibid 46.
[25] *Trusted Digital Identity Bill* (n 21) s 36.
[26] Lopez (n 18) 46.
[27] Ibid 18.
[28] See *Declaration for cooperation and exchange of best practices in the field of self- sovereign identity between the Federal Republic of Germany and the Republic of Finland*, signed in duplicate 22 September 2021.
[29] See *Joint Declaration on cooperation and exchange of best practices in the field of self-sovereign identity between the Federal Republic of Germany and the Kingdom of Spain*, signed in duplicate 29 July 2021.
[30] Lopez (n 17) 46.

4.3. Proposal 10.1 – Additional protections for collection, use and disclosure of personal information

Recommendation 10

> ***That collection, use or disclosure of personal information under APP 3 and APP 6 must be fair, reasonable, lawful and transparent in the circumstances.***

With regards to 10.1, the DLA propose the addition of the words 'lawful and transparent'. The DLA considers that the addition of these words is required to emphasise the need for data collection and processing to be in accordance with the law and transparent, and to align with the GDPR, to ensure international consistency, pursuant to Article 5:

> *1(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*

This also aligns with other overseas jurisdictions, namely the California Consumer Privacy Act, the New Zealand Privacy Act, Hong Kong's Personal Data (Privacy) Ordinance and Singapore's Personal Data Protection Act (see Schedule 2).

4.4. Proposal 11 – Restricted and prohibited acts and practices

Recommendation 11

> ***That Option 1 from the Discussion Paper be adopted to provide a list of restricted practices that require reasonable steps to identify privacy risks and implement measures to mitigate those risks, but that the proposal be scrutinised to ensure it is adequately robust to accommodate impacts of emerging technologies such as AI and quantum.***

The DLA supports self-sovereign identity as a way to increase an individual's capacity to self-manage their privacy (see section 4.2 above), however, in the interim, there is value in Option 1, as it clearly identifies the restricted practices and this will assist in industry compliance. However, further guidance will still need to be provided to explain in simple terms the meaning of each restricted practice, for example, what is meant by *"on a large scale"*. The DLA looks forward to reviewing and commenting on the final draft of an Option 1 section prior to its inclusion in the Privacy Act.

The DLA is also concerned that the list of practices is limited and does not adequately future proof the Privacy Act in light of emerging technology (where it creates a new threat to privacy). We anticipate that if Option 1 is used as is, there will be a need to include further restricted practices with proper definitions, in the near future. For example, see discussion on AI in automated decision-making in section 4.7 below.

4.5. Proposal 14 – Right to object and portability

Recommendation 12

> ***That this recommendation be reconsidered in light of the Principles noted in section 3.1 of this submission. That education is provided to consumers in respect of how individuals can avail themselves of this right.***

The DLA supports this proposal in principle but does not support this proposed amendment as currently drafted, as practically, in most cases, an individual will not know what their personal information is being used for and whether or not their consent extends to that use. These rights if included need to be supported with sufficient education and access to clear and simple to follow guidelines on how an individual can avail themselves of their rights.

4.6. Proposal 15 – Right to erasure of personal information

Recommendation 13

> ***That the right to erasure of personal information be reconsidered in light of the Principles noted in section 3.1 of this submission and Articles 17 and 19 of the GDPR.***

The DLA supports this proposal in principle and recognises that the right to erasure should not be an absolute right, and often requires a balancing exercise among the different interests at stake.

However, the DLA is not able to take a final view on this proposal as it is not clear how the grounds in Proposal 15.1 will be drafted in the final version of the Act, how they will interact with other parts of the Act (e.g. how an individual will be notified of their rights in line with Article 19 of the GDPR) and that they appear to be more restrictive than those in the GDPR (which includes in Article 17(2), the right to be forgotten).[31] Also, the proposal does not provide a list of the exceptions to an individual's right to erasure of personal information, and the DLA recommends that any such list take into account Article 17, paragraphs 2 and 3 of the GDPR, to provide broader protections to an individual and to ensure international consistency.[32]

Based on the characterisation of personal information as property, and the principle of ownership it confers on an individual, it is important that grounds under which an individual can request erasure should be as wide as possible balancing the interests of industry and society (e.g. where necessary to comply with legal obligations, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or for the defence of legal claims) and the exceptions under which an individual may not exercise their rights to erasure should not be overly restrictive.

Further, any inclusion of this right in the Act, requires education (as in most cases an individual will not know what their personal information is being used for and whether or not their consent extends to that use) and simple to follow guidelines as to how an individual can avail themselves of this right (e.g. Who to send their request to? How to draft their request? What to do if their request is refused?); and on how businesses are to comply and demonstrate compliance.

[31] See *Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González*, Judgment of the Court (Grand Chamber), 13 May 2014 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 – recognising the right to be forgotten. See also two judgments of the Court of Justice of the European Union further defining the scope of the right to be forgotten in the context of search engines, *GC and Others* (C-136/17): ECLI:EU:C:2019:773 https://curia.europa.eu/juris/document/document.jsf?text=&docid=218106&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=325980 and *Google v CNIL* (C-507/17): ECLI:EU:C:2019:772 https://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=326493.

[32] See European Data Protection Board, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR', adopted on 2 December 2019 https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf; Haya Yaish, 'Forget Me, Forget Me Not: Elements of Erasure to Determine the Sufficiency of a GDPR Article 17 Request' (2019) 10(1) Journal of Law, Technology & the Internet https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1115&context=jolti.

4.7. Proposal 17 – Automated decision-making

Recommendation 14

> ***That the Privacy Act be amended to include protections with regards to automated individual decision-making, including profiling in line with Article 22 of the GDPR.***

The DLA agrees in principle with Proposal 17 but considers that it needs to be expanded to include profiling in line with Article 22 of the GDPR (e.g. whether for sentencing, provisions of services or other grounds of classifying individuals).

Further, the DLA considers that an individual should be accorded the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, as described in Article 22 of the GDPR.

The DLA supports the recommendations put forward in the AHRC's Human Rights and Technology Final Report 2021. Issues associated with impact on individuals of automated decision-making cannot be adequately addressed through notice alone.

The DLA considers that there needs to be enhanced systems in place (e.g. more robust oversight by the Regulator and access to remedies) to ensure due process when personal information is used in automated decision-making (**ADM**), especially in light of the Robodebt class action (*Prygodicz v Commonwealth of Australia (No 2)* [2021] FCA 634.[33] The DLA is of the opinion that this is a requirement of any adoption of Article 22 of the GDPR, that its safeguards are strengthened, namely, the ability to contest decisions, for decisions to be explained (which while not explicitly stated in Article 22 is found in Recital 71 of the Preamble to the GDPR) and to access meaningful human intervention.

There is some urgency to implement further safeguards to protect an individual subject to ADM as there is no specific protection under the Privacy Act for individuals related to the use of personal information by ADMs (e.g. relating to the use of ADMs to make determinations related to individuals) unlike in other jurisdictions.[34] There is also no specific legislation authorising the use of ADMs.[35]

This is especially pressing as ADM is already used in Australia across a wide range of government functions, and uses personal information to significantly impact the lives of individuals. This includes in areas of visa eligibility, right to welfare, taxation liability and infringement notices.[36] Further, an algorithm of sorts is already utilised to impose sanctions on 90% of criminal offences, such as speeding fines.[37] Using AI could potentially lessen transparency[38] and studies have shown though that despite the

[33] *Prygodicz v Commonwealth of Australia (No 2)* [2021] FCA 634; Kobi Leins, 'What Is The Law When Ai Makes The 'Decisions'?', *University of Melbourne* (4 December 2019) https://pursuit.unimelb.edu.au/articles/what-is-the-law-when-ai-makes-the-decisions.

[34] Attorney-General's Department, *Privacy Act Review* (Discussion Paper) 137.

[35] Commonwealth Ombudsman, 'Automated decision-making better practice guide', (2019) 9 https://www.ombudsman.gov.au/__data/assets/pdf_file/0030/109596/OMB1188-Automated-Decision-Making-Report_Final-A1898885.pdf ('*Better practice guide*').

[36] Mirko Bagaric, 'Instant Justice? The Desirability of Expanding the Range of Criminal Offences Dealt with on the Spot' (1998) 24(2) Monash University Law Review 231, 234; Nigel Stobbs, Dan Hunter and Mirko Bagaric, 'Can Sentencing Be Enhanced by the Use of Artificial Intelligence?' (2017) 41(5) *Criminal Law Journal* 261-277, 261.

[37] Stobbs, Hunter and Bagaric (n 33) 262-263.

[38] Raffaele Piccolo, 'AI in Criminal Sentencing: A Risk to our Human Rights?' (2018) 40(11) *Bulletin (Law Society of South Australia)* 15-17, 16.

promises of AI being led only by its guiding principles, it is also susceptible to bias.[39] For example, some, *"data analytics techniques that support automatic decision-making such as automatic algorithms have the potential to create personal information with an inherent bias, that is discriminatory or that leads to inaccurate or unjustified results."*[40]

As noted above, ADMs are complicated and come in many forms. Consequently, just notifying individuals that an ADM is being used may not be sufficient. In the Discussion Paper, the AHRC preferred the terminology, *"AI informed decision-making"* when providing a notice but this is quite a vague definition. This is because even people in the AI space cannot agree on what does and does not constitute AI.[41]

Any notice (although the DLA considers that any notice by itself is not sufficient) must at the very least clearly define what is included in the ADM. For example, 'automated processing' and 'AI', if not properly defined could mean explicit coding of rules that govern the decision making or where the black box learns and adapts when making decisions.

The DLA considers that significant work needs to be undertaken to clarify and provide guidance on what is included in the definition of ADM and how it is to be regulated. Further, issues in relation to ADM may potentially justify the need for the Australian equivalent of the EU Artificial Intelligence Act (which we refer to in Schedule 2 – to key aspects as they relate to personal information and privacy).

4.8. Proposal 18 – Accessing and correcting personal information

Recommendation 15

> ***That proposal 18 be reconsidered in light of the Principles noted in section 3.1 of this submission, and that education is provided to individuals in respect of how they can avail themselves of this right.***

The DLA does not agree with this proposal as currently drafted. The issue with this proposal is that it does not deal with the reality that in most cases an individual will not know what their personal information is being used for and whether or not their consent extends to that use. Further, with any inclusion in the Privacy Act, there must be education on how an individual can avail themselves of this right.

[39] Lyria Bennett Moses, 'Artificial Intelligence in the Courts, Legal Academia and Legal Practice' (2017) 97(7) Australian Law Journal 561, 571; Alyssa Carlson, 'The Need for Transparency in the Age of Predictive Sentencing Algorithms' (2017) 103(1) *University of Iowa Law Review* 303-329, 311-312; Joo-Wha Hong and Dmitri Williams, 'Racism, Responsibility and Autonomy in HCI: Testing Perceptions of an AI Agent' (2019) 100 *Computers in Human Behavior* 79, 80.

[40] *Better practice guide* (n 32) 15.

[41] Kevin Ashley, *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age* (Cambridge University Press, 2017) 4; Lyria Moses, 'Artificial Intelligence in the Courts, Legal Academia and Legal Practice' (2017) 97(7) *Australian Law Journal* 561, 562-563; Raffaele Piccolo, 'AI in Criminal Sentencing: A Risk to our Human Rights?' (2018) 40(11) *Bulletin (Law Society of South Australia)* 15-17; Michael Mills and Julian Uebergang, 'Artificial Intelligence in Law: An Overview' (2017) (139) *Precedent* 35-38, 35. See also, Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', revised and adopted on 6 February 2018 file:///C:/Users/922983/Downloads/wp251rev_01_en_A754F3E1-FB46-9E76-C0A919864E4B6641_49826.pdf.

4.9. Proposal 20 – Organisational accountability

Recommendation 16

> ***That proposal 20 be implemented so that organisational accountability of APP entities extend to both primary and secondary purposes for which personal information is collected.***

The DLA agrees with the proposal for the reasons stated in the Discussion Paper.

4.10. Proposal 24.9 – Enforcement: Alternative regulatory models

Recommendation 17

> ***That the role of Federal Privacy Ombudsman be created that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR schemes, with appropriate funding to act proactively in pursuing enforcement.***

For Proposal 24.9, the DLA considers Option 2 to be the best approach for the reasons described in the Discussion Paper. It will be important that any such role be supported with appropriate funding for the Federal Privacy Ombudsman (**FPO**) to act proactively in order to achieve required enforcement objectives. Of course, to avoid duplication and inconsistency, the Freedom of Information functions currently undertaken by the Information Commissioner would need to be considered.

Having a separate FPO responsible for triaging and conciliating privacy complaints, (regardless of whether or not external dispute resolution processes are available), will allow the OAIC (again, with sufficient funding) to focus on building requisite institutional capacity and to take on a proactive enforcement-focused regulator role by directing its attention to taking regulatory action including conducting systemic industry reviews (to ensure compliance). This will assist in creating agility to keep pace with emerging technologies to protect individuals from privacy risks we are not aware of yet.

4.11. Proposal 25 – A direct right of action

Recommendation 18

> ***That proposal 25 be adopted to create a direct right of action for an individual to litigate a claim for breach of their privacy under the Act.***

The DLA agrees in principle with the proposed design elements as set out in proposal 25.1. However, we note that it is not clear how this right will interact with Proposal 26, and the DLA looks forward to considering and commenting on the final drafts of Proposal 25 and 26.

4.12. Proposal 26 – A statutory tort of privacy

Recommendation 19

> ***That Option 1 of proposal 26.1 be adopted to introduce a statutory tort for invasion of privacy specifically allowing for claims of damages for emotional distress and loss of control over an individual's data (and corresponding statutory guidance on formulation and quantum of such claims).***

It has been 20 years since *Australian Broadcasting Corporation v Lenah Game Meats Pty Limited* (2001) 208 CLR 199, 258 where Gummow and Hayne JJ left open the possibility of recognising an Australian tort of privacy, and the DLA considers that Australia is now ready for this tort to be introduced. It is needed to give an individual greater control of their personal information, their right to control their property:

> *Whatever development may take place in that field will be to the benefit of natural, not artificial, persons. It may be that development is best achieved by looking across the range of already established legal and equitable wrongs. On the other hand, in some respects these may be seen as representing species of a genus, being a principle protecting the interests of the individual in leading, to some reasonable extent, a secluded and private life, in the words of the Restatement, "free from the prying eyes, ears and publications of others". Nothing said in these reasons should be understood as foreclosing any such debate or as indicating any particular outcome. Nor, as already has been pointed out, should the decision in Victoria Park.* (Footnote omitted.)

There is also a need to include statutory guidance on claims for damages, including emotional distress and loss of control over an individual's data. This is because left to judicial discretion, there is no guarantee that the common law will be interpreted to allow for such a claim. By way of example, in *Bellingham Alex v Reed Michael* [2021] SGHC 125, an individual sought damages for emotional distress and loss of control over his data pursuant to section 32(1) of Singapore's Personal Data Protection Act. The High Court adopted a narrow interpretation of *"loss and damage"*, finding that the term referred to the heads of loss under common law and not more widely to include emotional harm and loss of control over personal data. This result is opposite to the decision reached by the Hong Kong District Court (in *Tsang Po Mann v Tsang Ka Kit and Anor.* [2021] HKCU 665), where the plaintiff received damages for injury to her feelings for misuse of CCTV camera footage pursuant to section 66 of the Personal Data (Privacy) Ordinance (Cap. 486).

5. Conclusion

Once again, the DLA appreciates this opportunity to contribute to this Discussion Paper. The breadth of proposals set forth in the Discussion Paper is a useful first step towards much-needed reform to be able to address issues that are arising in the digital economy and emerging technology. The DLA welcomes further consultation on these proposals and the overarching aims, guidance and principles for the Act and the related Australian Privacy Principles, as these proposals are further refined and draft legislation is prepared.

FIND US AT

@digitallawassociation

@DigitalLawAssoc

@digitallawassociation

@DigitalLawAssoc

CONTACT US

✉ info@digitallawassociation.com