Privacy Act Review Discussion Paper

Submission from elevenM

10 February 2022

Contents

Introduction

Over the last decade, digital innovation has resulted in a wholesale transformation of economies around the world. This has driven an explosion in the collection and handling of data and led to activities, including profiling and targeting of individuals and the derivation of behavioural predictions and inferred personal information, many of which were not contemplated when the *Privacy Act 1988* (Cth) (**the Act**) was established.

Continued digital innovation is integral to Australia's growth and prosperity, and trust is a critical dependency.

Trust in the digital world rests on the ability of an organisation, agency or other entity to manage the privacy and security of their customers' information such that customers feel they are in control and that their engagement with the entity is safe and reliable.

Across an economy, digital trust depends on structuring markets and creating incentives to align government and corporate behaviour with community expectations. It requires giving consumers choice and control without requiring constant vigilance to defend against harms. It requires the maintenance of effective protections and penalties for the misuse of Australians' personal information and a well-resourced regulator, empowered to take effective action.

In its current form, the Privacy Act falls short of these goals. The Act does not adequately support consumers to understand how their information is to be handled or give them assurance that they have any control over such handling. It does not aid them to make informed and impactful decisions. This is because the Act's cornerstones of consent and notice are no longer effective. The idea that individuals continue to safeguard their own privacy in this data driven world is a fiction.

Reform of our current framework would also benefit the economy by building trust and enabling international trade. Privacy compliance has become a hurdle for Australian businesses, who must currently navigate the requirements of overseas jurisdictions (most notably, the EU's General Data Protection Regulation (**GDPR**)) to be considered a trustworthy recipient of personal information. Without Australia being regarded as 'adequate', businesses are left to their own capabilities and resources to navigate these complex laws.

elevenM welcomes this opportunity to contribute to the review.

About elevenM

elevenM is a specialist privacy and cyber security consultancy. Our mission is to build trust in an online world.

As one of Australia's leading privacy consultancies, our team comprises experts in complementary disciplines such as privacy compliance, operations and technology, risk and compliance, IT risk, supplier risk, data governance and cyber security.

Members of our team combine technical and legal qualifications with extensive experience in the field. We work hand in hand with our clients to understand their businesses and identify effective and efficient solutions which are suitable for them — not only for today but for the constant changes coming over the horizon.

We work closely with various entities (public and private sector) to implement privacy and security programs, including improving transparency, delivering training and awareness initiatives, managing risks, remediating after breaches, conducting privacy impact assessments, assessing vendors and third-party supplier frameworks, embedding privacy by design and more.

In 2020, elevenM and Monash Law School conducted a major research project examining the privacy risks and harms that can arise for children and for other vulnerable groups online. Our research was commissioned by the OAIC and conducted in partnership with two leading academics from Monash Law School, Normann Witzleb and Moira Paterson. A summary of that research can be found on the elevenM website,[1] and our full report is available from the OAIC.[2] We have reproduced sections from our report below where relevant.

[1] elevenM Consulting, *Towards a safer online world for children and the vulnerable* (Blog Post, 27 October 2021) <https://elevenm.com/2021/10/27/towards-a-safer-online-world-for-children-and-the-vulnerable/>.

[2] Monash University and elevenM Consulting, 'Privacy risks and harms for children and other vulnerable groups in the online environment: Research paper commissioned by the Office of the Australian Information Commissioner' (December 2020) <https://www.oaic.gov.au/__data/assets/pdf_file/0012/11136/Report-Privacy-risks-and-harms-for-children-and-other-vulnerable-groups-online.pdf> ('Monash-elevenM research').

Submission

1. Objects of the Act

Objects clauses signal the purpose of an Act and guide in its interpretation. In interpreting a provision of an Act, the interpretation that would best achieve the purpose or object of the Act is to be preferred to each other interpretation.[3] The objects clause is particularly important for the Privacy Act and in today's rapidly moving technological environment, as our principles-based regulatory regime requires constant interpretation and application to new technologies and contexts.

Proposal 1.1	*Amend the objects in section 2A, to clarify the Act's scope and introduce the concept of public interest, as follows:* *a) to promote the protection of the privacy of individuals with regard to their personal information; and* *b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities undertaken in the public interest.*
elevenM position	We support proposal 1.1 to amend the objects in section 2A to clarify the Act's scope and introduce the concept of public interest. However, in our view the proposal does not go far enough. For the reasons that follow, the objects in section 2A should also be amended to: • recognise information privacy as a human right; and • recognise that strong privacy protections serve the public interest.

Section 2A should recognise information privacy as a human right

The protection of privacy is a human rights issue. Human rights jurisprudence provides a well-tested and globally accepted framework for balancing competing rights and interests,

[3] *Acts Interpretation Act 1901* (Cth), s 15AA.

including the right to data protection or information privacy as part of the broader human right to privacy.[4]

Amending section 2A to recognise the role of the Privacy Act in protecting information privacy as a human right would provide interpretive clarity for the Act and the application of the Australian Privacy Principles (**APPs**), reflect community expectations and support global interoperability.

We do not agree with the statement in the Discussion Paper that:

> *It is not appropriate for the objects to refer to a 'right to privacy' because, despite common parlance, Art 17 does not confer such a right, nor does it amount to absolute protection.*

Privacy is a fundamental human right recognised in Article 12 of the UN Declaration of Human Rights, in Article 17 of the *International Covenant on Civil and Political Rights* (**ICCPR**), and in many other international and regional agreements. Article 17 of the ICCPR protects individual privacy as a human right by conferring on individuals, a right to the protection of the law against arbitrary or unlawful interference with their privacy and imposing on state parties, an obligation to protect everyone against such interference. As a signatory to the ICCPR, Australia has an obligation to enact such protection within our domestic law.

Data protection or information privacy is widely acknowledged as a human right in itself, and a key component of the broader right to privacy.[5]

Although Australia does not give human rights explicit protection at the federal level through domestic human rights legislation or a bill of rights, protection of the broader right to privacy exists at the state and territory level in Victoria, the ACT and Queensland. Australian courts have also recognised the status of the individual right to privacy within modern human rights jurisprudence.[6]

Section 2A should be amended to acknowledge the status of data protection and/or information privacy as a human right.

---

[4] Such as the test of 'proportionality', assessing whether limits on rights are necessary, suitable and in pursuit of a legitimate objective.

[5] For example, the first recital of the GDPR recognises that "The protection of natural persons in relation to the processing of personal data is a fundamental right".

[6] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285, [62]-[72].

Section 2A should recognise that strong privacy protections serve the public interest

Although the right to privacy is an individual right, there is a strong public interest in protecting that right.[7] Section 2A (as currently drafted, and if proposal 1.1 is enacted) provides insufficient recognition of the public and communal interests in strong privacy protections.

In many cases, privacy rights are consistent with and support economic, security and other important public interests. For example, strong privacy protections support Australia's economic growth and prosperity by building digital trust, which in turn unlocks digital innovation. Trust in the ability of organisations, agencies and others to manage the privacy and security of our personal information is a critical foundation for almost all aspects of modern life, from everyday online transactions to critical governmental programs such as COVID responses, healthcare, tax administration and the census. Innovative new industries and solutions can only be developed where sufficient public trust and social license exists.

It is also increasingly clear that certain handling of one person's personal information may give rise to privacy harms for other people, or for the community at large. In its submission to the Issues Paper, the Office of the Australian Information Commissioner (**OAIC**) noted several practical examples, including:

- The development of predictive analytics tools to make decisions about an individual, regardless of whether that individual's personal information was used to develop the decision-making model.
- The increased political polarisation as a result of personalisation and targeting driven by personal information online.[8]

Section 2A should be amended to acknowledge the public interest in protecting privacy rights.

[7] Australian Law Reform Commission, *For your information: Australian Privacy Law and Practice* (Report no 108, May 2008), vol 1, 290 [5.123].

[8] Office of the Australian Information Commissioner, Submission to the Attorney-General's Department, *Privacy Act Review – Issues Paper* (11 December 2020) 25 [1.20].

2. Personal information, de-identification and sensitive information

The definition of these terms sets the scope of the Privacy Act and determines the level of protection to be applied. So far as possible, these definitions should:

- provide certainty and a clear means of determining what obligations apply with respect to a given piece of information;
- set the scope of the Act to capture the appropriate information — that information that must be controlled in order to achieve the objectives of the Act; and
- be technologically neutral and able to evolve over time, to provide flexibility to encompass future technologies.

Replacing 'about' with 'relates to

Proposal 2.1	*Change the word 'about' in the definition of personal information to 'relates to'.*
elevenM position	We support proposal 2.1.

In our view, the proposal will provide greater certainty and better focus consideration on whether the information is connected to or reveals information about an identifiable individual. We consider that any increased compliance costs arising from a broader scope of application of the Act will be offset by its clearer scope.

Following the decision of the Full Federal Court of Australia (**FCA**) in *Privacy Commissioner v Telstra Corporation Ltd*[9] ('the Grubb case'), substantial uncertainty has persisted within government and industry as to the proper scope of the Act.

This uncertainty increases costs and makes compliance difficult for APP entities. If organisations cannot determine with confidence, which of their information assets are subject to the Privacy Act, assessing privacy risk and allocating resources appropriately is difficult. At best, uncertainty leads to an unnecessarily high cost of compliance, as APP entities err on the side of caution by applying privacy governance and controls to data that need not be protected. At worst, uncertainty leads to interferences with privacy and harm to individuals when APP entities fail to apply privacy controls to data they erroneously

[9] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFA 4 (19 January 2017).

considered beyond the scope of the Act. Examples of both best and worst scenarios are common in our experience.[10]

The proposal would help to resolve this uncertainty by providing a clearer and simpler test, which is better aligned with international standards.

In addition to generating uncertainty, by drawing attention to 'about' as a separate test, the Grubb case has led to an unfortunate focus on how information is generated and its proximity to an individual when the key concern of privacy should always be what is revealed or conveyed about a person. The proposal would better focus consideration on whether the information is connected to or reveals anything about an identifiable individual.

We note that the proposal is likely to broaden the scope of the Act, particularly in the telecommunications sector.[11] We anticipate any additional compliance costs associated with this expansion to be modest, as the scope of personal information remains bounded by the primary requirement that personal information be linked back to an identifiable individual. Further, we note that similar obligations are (or will soon be) in place with respect to information that 'relates to' an individual under the Consumer Data Right (**CDR**) regime and the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**), both of which use 'relates to' in defining personal information. Any additional compliance costs will also be offset by greater clarity and alignment between the regimes.

Finally, and significantly for any businesses with operations outside of Australia, the proposal would bring Australia back into alignment with comparable jurisdictions (eg: Canada) and international standards (eg: GDPR), which do not apply a separate 'about' test.

Including a non-exhaustive list of the types of information capable of being covered

Proposal 2.2	*Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information.*
elevenM position	We support proposal 2.2.

[10] High profile examples of the latter scenario include the Office of the Victorian Information Commissioner, 'Disclosure of mkyi travel information – investigation under section 8C(2)(e) of the Privacy and Data Protection Act 2014 Vic' (Report, 15 August 2019) <https://ovic.vic.gov.au/wp-content/uploads/2019/08/Report-of-investigation_disclosure-of-myki-travel-information.pdf>. Office of the Australian Information Commissioner, 'Publication of MBS/PBS data' (Report, 23 March 2018) < https://www.oaic.gov.au/__data/assets/pdf_file/0015/2094/publication-of-mbs-pbs-data.pdf>.

[11] For example, where organisations may hold technical information that 'relates to' an individual's use of a service but is 'about' a device on or connected to the organisation's network.

A non-exhaustive list of the types of information capable of falling within the definition of personal information would add further clarity and context to the definition of personal information.

In order to remain technologically neutral and avoid falling out of date too quickly, the list should comprise categories of information (eg: 'an identifier or logical address of an individual or device'), rather than instances of those types (such as a MAC address or an IP address).

Not all technical data carry privacy risks. Some responses to the issues paper appeared to interpret this proposal as for a list of technical information types that would *in all circumstances* amount to personal information. It should be clear that any type of information included in the proposed list does not *necessarily* amount to personal information and must still satisfy the primary elements of the definition to amount to personal information.

Defining 'reasonably identifiable'

Proposal 2.3	*Define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment.*
elevenM position	We support proposal 2.3. Further work and consultation is required to clarify the threshold at which an individual is said to be 'identified'. We would support a broad definition, as foreshadowed in the Discussion Paper, that an individual is ''identified' when they are distinguished from others or have a profile associated with a pseudonym or identifier, whether or not they are named.

Further guidance, by means of a definition and list of factors to support assessment of when an individual is 'reasonably identifiable', would be welcome.

In our view, clarification is also required with respect to when, for the purposes of the Privacy Act, an individual is 'identified'. In our view, the definition should clearly include:

- Information that would enable the individual to be distinguished from others or recognised within a certain context (for example, a photograph of a person's face that allows that individual to be distinguished from others, or an IP address, location or device identifier that allows a user to be distinguished from others).
- Information that enables an APP entity to 'single out' or reach and affect a person, for example, in the context of behavioural targeting or direct marketing.

The Discussion Paper states that the definition 'would cover circumstances in which an individual is distinguished from others or has a profile associated with a pseudonym or

identifier, despite not being named.'[12] This standard reflects the OAIC's current guidance and has been applied recently by the OAIC in relation to facial images.[13] As the Discussion Paper notes, it is also aligned to international standards, including the GDPR.

Clearly defining personal information as including information that enables an individual to be 'distinguished from others', or to be 'singled out' aligns with community expectations by extending privacy protections to cover commonplace online tracking and advertising practices which are of significant concern to the community, but which have, to date, been considered beyond the scope of the Act.

Because the definition of personal information sets the scope of the Act, it should include any information that *may*, if not appropriately governed, lead to privacy harms. To the extent that flexibility is required, or a lower standard of protection is appropriate for information that presents a lower risk, this is better provided for through the provisions of the APPs and standards such as fairness and reasonableness, rather than by excluding lower-risk information from regulation entirely.

Clarifying coverage of households

elevenM position	Clarify that information that relates to a household also amounts to personal information.

The definition should also clarify whether information relating to a small cohort of identified individuals (such as a household) amounts to personal information of any one of those individuals. In our experience, it is common practice in many areas to treat data at a household level as beyond the scope of the Privacy Act. For example, many commercially available data products package detailed preference, demographic or other data at the household level in order to avoid the application of the Privacy Act.

Information about a household (for example, demographics, financial status, family/relationship type, racial or ethnic origin, movements, buying habits etc) are equally privacy invasive as the same information about any one individual within the household. This is particularly so considering that contact details and identifying information are commercially available for most Australian households.

[12] Attorney-General's Department, *Privacy Act Review – Discussion Paper* (October 2021) 27.

[13] See Office of the Australian Information Commissioner, *What is personal information* (Web Page, 5 May 2017) <https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information> and *Commissioner initiated investigation into 7- Eleven Stores Pty Ltd (Privacy)* (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021) [31]-[39].

Other jurisdictions (most notably California) have adopted a definition of personal information that includes information linked to a consumer *or household.*

Defining 'collection' to clearly cover inferred information

Proposal 2.4	*Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.*
elevenM position	We support proposal 2.4. The definition of 'collection' should be inclusively, rather than exhaustively, defined to remain open to new technological development.

As noted in the Discussion Paper, this proposal reflects current OAIC guidelines.

The language used in the Discussion Paper suggests that collection could be defined exhaustively to mean 'gathering, acquiring, inferring or obtaining personal information from any source and by any means'.[14] We recommend that the definition be framed inclusively (i.e. to *include*, rather than be limited to gathering, acquiring, inferring or obtaining) to avoid any risk that it may be interpreted more narrowly than intended. For example, we note it is unclear whether the proposed definition would cover information that was 'created'. An inclusive definition also has the best chance of remaining open to new and unforeseen technological developments.

Requiring information to be anonymous before the Act no longer applies

Proposal 2.5	*Require personal information to be anonymous before it is no longer protected by the Act.*
elevenM position	We support proposal 2.5.

We prefer the more restrictive requirement that information be anonymous, meaning that re-identification be no longer possible or that any risk of re-identification, extremely remote or hypothetical. The potential for privacy harms to arise from the collection, use and sharing of

[14] Attorney-General's Department (n 12) 28.

these rich, 'de-identified' datasets is well documented.[15] We agree that this reform would not impose an unworkably high standard.

Because these definitions set the Act's scope, it should include any information that *may*, if not appropriately governed, lead to privacy harms. To the extent that flexibility is required, or a lower standard of protection is appropriate for information that presents a lower risk, this is better provided for through the provisions of the APPs and standards such as fairness and reasonableness, rather than by excluding lower-risk information from regulation entirely.

Introducing penalties for malicious re-identification of information

Proposal 2.6	*Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments.*
elevenM position	We strongly oppose proposal 2.6.

In our view, the Privacy Amendment (Re-identification) Offence Bill 2016 presents an ineffective and unnecessarily punitive approach to the problem of government agencies publishing poorly de-identified information. The Bill would have a destructive and chilling effect on legitimate information security and data analytics research, without materially altering the incentives for government agencies or for malicious actors.

The issue of malicious re-identification and onwards disclosure of re-identified information may be partially addressed by introducing a statutory tort.

Rather than general civil and criminal offences contemplated by the Bill, we support the OAIC's recommendation to introduce a prohibition on APP entities taking steps to re-identify information that they collected in an anonymised state, except in order to conduct testing of the effectiveness of security safeguards that have been put in place to protect the information.[16]

[15] See, eg, Justin Sherman, 'Big data may not know your name. But it knows everything else', *Wired* (Web Page, 19 December 2021) <https://www.wired.com/story/big-data-may-not-know-your-name-but-it-knows-everything-else/>; Salinger Privacy, 'The definition of personal information – Research paper for the office of the Australian Information Commissioner' (Research Paper, 17 February 2020).<https://www.oaic.gov.au/__data/assets/pdf_file/0012/1308/definition-of-pi.pdf.pdf>.

[16] See OAIC (n 5) 35.

Definition of sensitive information

elevenM position	Precise geolocation information should be included in the definition of Sensitive Information.

According to the OAIC's Community Attitudes to Privacy Survey 2020, half (48%) of Australians consider location information to be one of the biggest privacy risks today, and only a quarter (24%) feel that their location information is well protected by law and regulations.[17]

Precise geolocation data can be extremely invasive, and is often collected without individuals' knowledge, by default or even after a user believes they have turned it off.[18] In many cases, location data is used as a tool for surveillance, control and abuse.[19]

Including precise geolocation information as a new category of sensitive information would require applications and services to obtain specific consent for the collection of precise location data, ensuring that users are aware and are able to opt out.

We acknowledge that a definition of 'precise' would have to be settled upon in order to implement this recommendation. Any such definition would have to be contextual, as for example, geolocation information at a resolution of 1km in an inner city environment may not reveal much meaningful information about an individual's movements, but may be much more revealing in a rural or regional environment.

elevenM position	The definition of sensitive information should include information or an opinion that is collected for use as, or used or disclosed as a proxy for, any of the attributes listed in the definition of sensitive information.

[17] Office of the Australian Information Commissioner, 'Australian Community Attitudes to Privacy Survey 2020' (report prepared by Lonergan Research, 2020) 79 <https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf>.

[18] Australian Competition and Consumer Commission, 'Google misled consumers about the collection and use of location data' (Media release,16 April 2021) <https://www.accc.gov.au/media-release/google-misled-consumers-about-the-collection-and-use-of-location-data>.

[19] See, eg, Kristian Silva, 'GPS trackers, hidden cameras on the rise as domestic violence increases during pandemic', *ABC News* (online, 24 November 2020) <https://www.abc.net.au/news/2020-11-24/domestic-violence-report-shows-increase-in-online-abuse/12911926>.

We support the recommendation of the Castan Centre for Human Rights Law in its submission to the Issues Paper, that the definition of sensitive information should include proxies for sensitive personal information.[20]

The inclusion of proxies is important in this age of advanced data analytics and algorithmic decision making, where proxy indicators can easily be identified and used in place of the defined sensitive attributes to avoid heightened protections. For example, an organisation wishing to target online advertising based on an individual's sexual orientation or practices may, instead of seeking to collect this sensitive information (requiring consent etc), identify proxy indicators such as browsing history and purchasing patterns that strongly indicate the protected attribute — thereby targeting or discriminating based on that attribute without attracting the higher standard of protection intended to be afforded under the Act.

3. Flexibility of the APPs

More flexible code-making powers

Proposal 3.1	*Amend the Act to allow the IC to make an APP code on the direction or approval of the Attorney-General:* • *where it is in the public interest to do so without first having to seek an industry code developer; and* • *where there is unlikely to be an appropriate industry representative to develop the code.*
Proposal 3.2	*Amend the Act to allow the IC to issue a temporary APP code on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.*
elevenM position	We support proposal 3.1, except consider that the requirements should be alternative, rather than cumulative. We support proposal 3.2. We support the information Commissioner's recommendation for inclusion of a power for the Information Commissioner to intervene at any point in the code-development process, where an APP code is being developed by a code developer, if satisfied it would be preferable for the Commissioner to develop the Code.

[20] Castan Centre for Human Rights Law, Submission to the Attorney-General's Department, *Privacy Act Review – Issues Paper* (29 November 2020) 19.

In order to better facilitate adaptation of the Privacy Act regime to specific or emerging needs, a more flexible code-making power is necessary.

We note the growing fragmentation of privacy rules and regulations (for example contained in the CDR scheme and under the Data Availability and Transparency Bill 2020), which leads to increased complexity and compliance costs for business. We recognise that there is a need in many industries for greater prescription and clarity as to how the APPs apply, or for higher standards of protection. Wherever possible, this should be provided within the framework of the Privacy Act, either by guidance or a Code, rather than through a separate, case-specific legislative framework.

Proposals 3.1 and 3.2 are essential to facilitate this outcome. As outlined in the Discussion Paper and the Information Commissioner's submission to the Issues Paper, the OAIC's current code-making powers are of limited effectiveness, largely as a result of the inevitable complexity, delay and difficulty of finding an appropriate industry code developer.[21]

The proposed double requirement, that development of the code by the Information Commissioner must be both in the public interest and there must not be an appropriate industry representative, is unnecessary.

Circumstances may arise in which there is an appropriate industry body, but the Attorney-General and the Information Commissioner consider it to be in the public interest that the Code be developed by the Commissioner directly. This could be, for example, because the Commissioner and the Attorney-General do not have confidence in the industry code developer to participate in the process in good faith. Either condition should suffice alone.

We also support the inclusion of a power for the Information Commissioner to intervene at any point in the code development process where an APP code is being developed by a code developer if satisfied it would be preferable for the Commissioner to develop the Code, as proposed by the Information Commissioner in her submission to the Issues Paper.[22]

Elevate the status of the Commissioner's APP guidelines

elevenM position	We support the Information Commissioner's recommendation to elevate the status of the Commissioner's APP guidelines through a new provision that would require entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

[21] See OAIC (n 8) 38-41.

[22] See OAIC (n 8) 41.

In the absence of substantial judicial consideration of the provisions of the Privacy Act, the only interpretive guidance available to APP entities and individuals is contained in the Guidelines issued by the Information Commissioner. The Commissioner's guidelines are widely relied on by industry, despite the fact that they are not legally binding, nor is an entity required to have regard to them when considering how to comply with the Act.

The absence of any such requirements limits the utility of the APP guidelines from the perspective of an individual seeking to understand their privacy rights and contributes to uncertainty for APP entities as to how the Act will apply if tested. Elevating the status of the Guidelines as recommended by the Information Commissioner would help resolve these issues.

4. Small business exemption

elevenM position Remove the small business exemption.

No comparable jurisdiction exempts small businesses from the general privacy law. It is contrary to community expectations and deprives individuals of a right to complain about many of the most serious interferences with their privacy. It adds unnecessary complexity and provides limited benefit to small business at significant cost to the broader economy. Further, with the growth of data-driven, technology start-ups, there are a significant number of small businesses that fit within the small business exemption but nevertheless may hold significant volumes of personal information and may present significant privacy risk to their users.

The effect of the exemption is that affected individuals, rather than small businesses, bear the costs of handling or mishandling personal information. When a small business causes harm to an individual, the cost of that harm should be borne by the business, not by the individual. Many small businesses handle significant amounts of personal information, and many of the most significant and damaging interferences with privacy occur at small, local and personal scales. The OAIC outlines some examples of this kind of harm, such as the disclosure of an individual's personal and/or sensitive information in response to a negative review of a business, or the disclosure of personal information about an individual involved in a family violence dispute to the offender. While the costs for small business to comply with the Act should not be ignored, there is no justification for these costs to be borne by the affected individuals instead. This is consistent with community expectations — 71% of Australians agree that small businesses should be covered by the Privacy Act.[23]

The exemption is also complex and difficult to navigate. There are 12 categories of business that are not covered by the exemption (and therefore covered by the Privacy Act), as well as

[23] OAIC (n 17) 60.

various categories of information (such as CDR data, or information retained under the TIA Act) that must be managed in compliance with the APPs. Further, there are exceptions to the exceptions to the exemption — for example, where a small business has individuals' consent to trade their personal information. It is difficult for small businesses to understand their obligations and even harder for individuals to understand when their privacy will be legally protected.

The cost to small business of the current system is not insubstantial. It includes the need to constantly assess whether the Act will apply and to consider whether future contracts and plans may bring them within the scope of the Act. The current cost of the exemption is also significant for larger enterprise, who require assurance that their small business suppliers are complaint with the APPs and must obtain that assurance through contractual measures and ongoing audits. It also stands as a barrier to international trade by preventing GDPR adequacy, and substantially increases the costs associated with overseas contracting and international data flows.

Should the exemption be removed, the cost of compliance is unlikely to be significant. The OAIC is well placed to provide appropriate guidance, tool kits and templates. Most responsible small businesses' processes are shaped by the reasonable expectations of their customers (which include appropriate management of personal information). Small business also typically rely on digital systems provided by larger entities such as banks and software vendors, which are designed with privacy and security in mind. Small businesses providing services to larger APP entities are typically already required by contract (or under the Privacy Act for Commonwealth contractors) to comply with the APPs. Noting also that obligations under the APPs are designed to scale with risk and resources, in our view, for most small businesses, changes to IT systems and business processes in order to comply with the Act are likely to be limited.

Finally, as we have argued above in the context of the definition of personal information, the scope of the Act should be set to include any information that may, if not appropriately governed, lead to privacy harms. To the extent that flexibility is required, or a lower standard of protection is appropriate for information that presents a lower risk, this is better provided for through the provisions of the APPs and standards such as fairness and reasonableness, rather than by excluding lower-risk information from regulation entirely.

elevenM position	We do not support requiring small businesses to comply with a simplified set of rules, or some but not all of the APPs, or prescribing further acts or practices to be covered by the Act.

Applying different rules for different businesses is not consumer friendly. It requires consumers to have a higher privacy literacy than businesses themselves.

These approaches simply add further complexity and cost to an already confusing regime. The APPs are designed to operate as a whole, protecting personal information throughout the information lifecycle, and already include provision to scale up or down based on risk and resources available.

elevenM position	It is not appropriate to permit individuals to opt out of the application of the Privacy Act as a whole.

The Discussion Paper seeks stakeholder views on whether proposal 9.1, to require consent to be voluntary, informed, current, specific and unambiguous, would address concerns about the privacy risks associated with the consent provisions of the small business exemption.

In our view, regardless of the standard of consent applied, it is not appropriate to permit organisations to rely on consent as a basis for being exempt from the Act. If the small business exemption is retained, the consent exception should be removed.

5. Employee records exemption

elevenM position	Remove the employee records exemption. Replace the employee records exemption with a limited exception to APPs 12 and 13 (Access and Correction) covering information handled for the purpose of assessing suitability for employment or progression, discipline and performance management. No other amendment to consent requirements or APPs is required for employers/employees.

Employees are uniquely vulnerable to privacy harms arising from the mishandling of their personal information by employers because of the volume and sensitivity of personal information that is collected by employers and the power differential inherent in most employment relationships.

There is no justification for excluding private sector employees from privacy protections. As the Discussion Paper correctly observes, employee privacy is not adequately dealt with under workplace relations laws.

The effect of the exemption is that employees, rather than their employers, bear the costs of handling or mishandling personal information. When an employer mishandles their employees' personal information in a way that causes them harm, the cost of that harm should be borne by the employer, not by the employee. As the Discussion Paper and many submissions note, employers often collect a wide range of high risk personal and sensitive information about their employees. It is anomalous and inappropriate that employers do not have obligations to protect or appropriately handle this information, and that any costs of mishandling are borne by employees themselves. It is also inconsistent with community expectations — 73% of individuals surveyed by the OAIC in 2020 considered that

businesses collecting work-related information about employees should be covered by the Privacy Act.[24]

The modern workforce is not limited to employees — it includes a range of internal and external contributors, including contractors, service providers, gig economy workers, external app developers and more.[25] Larger enterprises, which manage other types of contributors alongside their employee workforce must choose whether to apply the same level of protection to personal information collected about all contributors, or to artificially distinguish between information about employees and other contributors, so as to apply a lower standard of protection for their employees. In our experience, most large enterprises simply elect to apply the same level of privacy protection for all contributors. Removing the exemption would establish a universal standard of protection for employees, contractors and customers, simplifying information management requirements for organisations.

If the employee records exception is abolished, we would support the introduction of a limited exception to APPs 12 and 13 (Access and Correction) covering information handled for the purpose of assessing suitability for employment or progression, discipline and performance management. This could cover reference checks and assessments at the time of recruitment, as well as ongoing performance management and disciplinary investigations.

We do not consider that any other amendment to the APPs is required in order for employers to effectively manage their workplaces. We agree with Salinger Privacy's submission to the Issues Paper on this point:

> *Other obligations, such as the need to ensure only relevant and non-intrusive personal information is collected, that personal information is securely stored, and that the accuracy of personal information is checked prior to making a decision, should all apply in employment scenarios just as they would when dealing with customers' personal information.*[26]

We do not consider that any amendment to consent requirements is required in light of *Lee v Superior Wood*[27], or if the employee records exemption is abolished. We support the OAIC's

---

[24] OAIC (n 17) 60.

[25] A recent global management survey found that 87% of respondents consider that their workforce includes more than just their employees: MIT Sloan Management Review and Deloitte, 'Workforce ecosystems' (Research Report, 13 April 2021) <https://www2.deloitte.com/us/en/insights/focus/technology-and-the-future-of-work/workforce-ecosystems-practical-guidance-for-leaders.html>.

[26] Salinger Privacy, Submission to the Attorney-General's Department, *Privacy Act Review – Issues Paper* (20 November 2020) 12.

[27] *Lee v Superior Wood* [2019] FWCFB 2946.

submission to the Issues Paper on this point.[28] Power asymmetries in any relationship affect the validity of consent, whether that is between employers and employees, business and consumers, or agencies and individuals. Appropriate exceptions already exist under APPs 3 and 6 so that even with a limited ability to rely on consent, employers will be able to collect, use or disclose an employee's personal or sensitive information, where there is a genuine business need to do so.

6. Political exemption

elevenM position Remove the political exemption.

In our view, the political exemption damages, rather that supports, Australia's system of representative democracy. There is no coherent policy justification for exempting political parties from the Act and there is no reason that political parties cannot act within the bounds of the Privacy Act. A critical aspect of trust in public institutions is the willingness to submit to the same levels of accountability as everyone else.[29]

The role of data in political campaigning has changed significantly since the introduction of the exemption in 2000. Even in 2010, it was becoming increasingly clear that 'data driven' election campaigns pose a real threat to public trust in democratic processes. This led to the recognition by the Australian Law Reform Commission (**ALRC**) that abolishing the exemption would promote, rather than impede, public confidence in the democratic process.[30] The following submission from the Public Interest Advocacy Centre, quoted in the ALRC report is even more true today:

> *The unregulated operation of [electoral] databases can diminish public confidence in the democratic process, discourage constituents from contacting their local Member of Parliament about issues of concern, and distort the political process by skewing it in favour of swinging voters. The proposal to remove the exemption should result in greater transparency and accountability in the way that political parties and their representatives handle personal information.*

In the last decade, the need to apply privacy laws to political campaigning has become even more urgent. The Facebook-Cambridge Analytica scandal brought greater public attention to the ways in which advanced marketing and data analytics techniques can be used to profile

[28] OAIC (n 8) [4.27].

[29] Former Victorian Privacy Commissioner Paul Chadwick, quoted in ALRC (n 7) 108 [41.33].

[30] Ibid [41.57].

voters and micro-target political messages to exploit individual beliefs and fears. These practices harm public debate, rather than enhance it.

Though beyond the scope of review, we would also advocate for related amendments to the *Do Not Call Register Act 2006* and the *Spam Act 2013*.

7. Journalism exemption

elevenM position	We recommend that the journalism exemption be abolished and replaced with limited exemptions to the APPs as necessary to facilitate the conduct of journalism in the public interest. We anticipate this may require amendment to the collection, use and disclosure of personal information (APPs 3, 5 and 6), access and correction (APPs 12 and 13) and breach notification obligations.

We recognise the important public interest that journalism serves, however the current exception does not strike an appropriate balance between the relevant interests.

Public interest journalism may require some limited exemptions with respect to:

- APPs 3, 5 and 6 to permit collection, use and disclosure of personal information.
- APPs 12 and 13 to permit refusal of an access or correction request by a media organisation where access or correction would prejudice the conduct of journalism in a way or to an extent that is on balance, contrary to the public interest.
- Breach notification obligations to allow a journalist to delay notification to affected individuals in the event of a data breach where notification would prejudice the conduct of journalism in a way or to an extent that is on balance, contrary to the public interest. For example, if a media organisation were to suffer a data breach affecting information collected in the conduct of public interest investigative journalism, it is possible that the public interest in preserving the secrecy of the investigation pending its completion may outweigh the interest of affected individuals in being notified.

However, we do not see any policy justification for exemptions from other APPs. We do not consider that the public interest is served by media organisations failing to take reasonable steps to ensure the quality of personal information (APP 10), or the security of personal information (APP 11).

Further, by omitting any kind of public interest requirement, the exemption allows for no balancing of interests between the public interest in protecting privacy and the public interest in freedom of expression and information. The exemption should only apply in circumstances where on balance, journalism is in the public interest.

As we noted in our submission to the Issues Paper, the definition of ‘media organisation’ is overly broad. Any organisation that maintains a website or a blog could be characterised as a media organisation for the purposes of the Privacy Act, which is defined as ‘an

organisation whose activities include the collection, preparation for dissemination or dissemination of material having the character of information, for the purpose of making it available to the public.[31] This definition could be amended to require that the qualifying activities be the main or primary activities of the organisation.

The exemption falls short of the objectives of the Act and of Australia's international obligations by leaving individuals without meaningful redress or recourse to law when their privacy has been interfered with.

8. Notice of collection of personal information

Strengthening and streamlining APP 5

Proposal 8.1	*Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.*
Proposal 8.2	*APP 5 notices limited to the following matters under APP 5.2:* • *the identity and contact details of the entity collecting the personal information* • *the types of personal information collected* • *the purpose(s) for which the entity is collecting and may use or disclose the personal information* • *the types of third parties to whom the entity may disclose the personal information* • *if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection* • *the fact that the individual may complain or lodge a privacy request (access, correction, objection or erasure), and* • *the location of the entity's privacy policy which sets out further information.*
Proposal 8.3	*Standardised privacy notices could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised notices.*
Proposal 8.4	*Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of*

[31] *Privacy Act 1988* (Cth) s 6 (definition of 'media organisation').

	collection, or if that is not practicable, as soon as possible after collection, unless: • *the individual has already been made aware of the APP 5 matters; or* • *notification would be impossible or would involve disproportionate effort.*
elevenM position	We strongly support proposals 8.1–8.4. We recommend a further addition to proposal 8.1, that privacy notices must be clear, current, understandable *and accessible, taking into account the needs, capabilities and behaviours of the reader.*

Including accessibility as a requirement and drawing attention to the need to take the audience into account would recognise the wide variety of ways in which readers may be hindered in their ability to access, consume and understand a notice. This could be, for example, because of a physical or cognitive disability, because of a language barrier, lack of background knowledge or literacy, or because they are a child. It would make it clear that clarity and understandability are not objective standards, but depend on the needs, capabilities, and behaviours of each audience member.

The standard for compliance with APP 5 should require organisations to design the content, style, mode of delivery and timing of privacy notifications to ensure that they are accessible and appropriate for all users (and their supporters or representatives, if any) across the spectrum of ability.

To take a specific example, we repeat Vision Australia's submission to the ACCC Digital Platforms Inquiry Issues Paper:

> *… it is wrong to assume that general measures aimed at protecting the privacy of consumers will automatically provide the same protections to consumers who are blind or have low vision. For example, many privacy policies are not provided in formats that are accessible to people who are blind or have low vision, and we have no reason to believe that this situation will change unless organisations and companies are required by legislation to make their privacy policies accessible. Similarly, it can be difficult or impossible to find privacy policies if the websites, apps and other digital platforms where they are located do not comply with accessibility guidelines.*[32]

[32] Vision Australia, Submission to the Australian Competition and Consumer Commission, *The Digital Platforms Inquiry Issues Paper* (29 March 2018) 4 <https://www.accc.gov.au/system/files/Vision%20Australia%20%28April%202018%29.pdf>.

A general transparency obligation

elevenM position	We recommend that in addition to enhanced obligations to provide privacy information in the form of a collection notice (APP 5) and a privacy policy (APP 1), a further, general obligation to take reasonable steps to ensure that any collection, use or disclosure of personal information be transparent to the individuals affected be adopted.

There is broad agreement on the limitations of existing consent requirements and transparency mechanisms under the Privacy Act. Some of the limitations of current requirements are outlined in the Discussion Paper, in the ACCC's Digital Platforms Inquiry Final Report, and the Online Privacy Bill consultation materials.

Research from the Consumer Policy Research Centre recently found that privacy policies do not aid informed choices and do not provide consumers with genuine choice or control:

- In 2020, 94% of Australian consumers reported not reading all the privacy policies or T&Cs that applied to them in the past 12 months.
- Of consumers who had read privacy policies, 69% reported accepting terms even though they weren't comfortable with them – the main reason for doing so was it was the only way to access the product or service (75%).[33]

Making privacy policies and notices easier to consume may have some beneficial impact. However, focusing privacy notice requirements on the point of first collection, when users are usually focused on gaining access to the product or service, rather than on reviewing privacy risks, is ineffective. It is not clear to us that the proposed enhancements to APP 5, or *any* enhancements that maintain the paradigm of a single notice on first collection of personal information will have any significant impact on individuals' engagement with privacy information or their ability to exercise genuine choice and control.

We recommend that in addition to enhanced obligations to provide privacy information in the form of a collection notice (APP 5) and a privacy policy (APP 1), a further, general obligation to take reasonable steps to ensure that any collection, use or disclosure of personal information be transparent to the individuals affected be adopted. This would be analogous to the transparency principle under the GDPR.

Such an obligation would require organisations to take steps beyond the initial provision of notice to communicate to individuals how and why their personal information is being collected, used or disclosed, and any relevant rights or options they might have. This could be through design features, just in time notifications, occasional reminders/renewal of consent, privacy dashboards or availability of retrospective summaries of collections, uses

[33] Consumer Policy Research Centre, 'CPRC 2020 Data and Technology Customer Survey' (Web Page, 7 December 2020), <https://cprc.org.au/publications/cprc-2020-data-and-technology-consumer-survey/>.

and disclosures. A good example of how this may look in practice can be seen in IKEA's app design, implementing their new 'Data Promise'.[34]

Guidance could give content to this new obligation without being prescriptive as to specific measures that an organisation must implement. Emphasis should be on encouraging inclusive and evidence-based design processes that produce notices and design features for privacy transparency that are effective for all users, regardless of their specific needs, vulnerabilities and behaviours. The ICO Age Appropriate Design Code provides detailed guidance, drawing on a wide evidence base, on the key considerations with respect to the evolving interests, needs and capacity of children.[35] The Consumer Experience work stream for the CDR Consumer Data Standards provides a good example of how a program of consumer experience research can be deployed from exploratory research through to prototype testing to understand consumer expectations, needs and behaviours in a given field.[36]

9. Consent to collection, use and disclosure of personal information

Proposal 9.1	*Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.*
elevenM position	We strongly support proposal 9.1.

We agree with the statements made by other submitters, as cited in the Discussion Paper, about the shortcomings of consent — particularly with respect to the burden it places on individuals to understand and consider complex data handling practices and foresee unknown privacy harms.[37]

In most cases, individuals are not well placed to make privacy choices the reflect their interests. OAIC guidance should reflect this by requiring that APP entities seeking to rely on consent should take the following factors into account:

- Most people don't read or understand privacy disclosures. The OAIC's Australian Community Attitudes to Privacy 2020 survey found that just 1 in 5 Australians (20%)

[34] IKEA, 'The New IKEA Data Promise Gives Privacy and Transparency to Customers' (Youtube, 30 January 2020) <https://www.youtube.com/watch?v=j1MsEl9cTRc>.
[35] Information Commissioner's Office UK, *Age appropriate design: a code of practice for online services* (Web Page, August 2020) <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/>.
[36] Data61, 'Consumer Experience Reports', *Consumer Data Standards* <https://consumerdatastandards.gov.au/engagement/reports/reports-cx/>.

[37] Attorney-General's Department (n 12) 75.

both read privacy policies and are confident that they understand them.[38] The Consumer Policy Research Centre similarly found that 94% of Australian consumers reported not reading all the privacy policies or T&Cs that applied to them in the past 12 months.[39]

- Most people have difficulty understanding and making rational decisions about the risk of future informational harms. Not only are digital information ecosystems often complex, but when we are well informed, individuals have a range of psychological and cognitive biases that get in the way of rational decision making, such as availability bias (the tendency to make judgements about the likelihood of an event based on how easily examples come to mind), or a tendency to value immediate gratification or convenience over future benefits. For example, 50% of people surveyed by Deloitte stated that they had given consent (when they had previously refused) because they were tired of being asked continuously by the same service.[40]
- Consent should not be considered valid where available options are not presented honestly and equally, or where it has been secured through use of 'dark patterns'. Dark patterns, the use of user interface or interaction design to lead users to make a particular selection, are now widely recognised as significantly compromising user autonomy and choice online.[41]

A stronger standard of consent is particularly necessary in order to reign in practices of some data brokers who continue to rely on dubious historical consents, which may be several years old and achieved without clear action from the individual (for example, through a statement in a linked privacy policy that the participant consents to specified uses and disclosures, usually for direct marketing). Proposal 9.1 would send a clear message that this approach to consent is unacceptable. If the proposal is adopted, we submit that these legacy practices should be addressed though OAIC education and enforcement as a matter of priority.

We note our position above that precise geolocation information should be included in the definition of sensitive information. Including precise geolocation information as a new category of sensitive information would require apps and services to obtain specific consent

---

[38] OAIC (n 17) 69.

[39] Consumer Policy Research Centre (n 33).

[40] Deloitte, 'Opting-in to meaningful consent — Deloitte Australian Privacy Index 2020' (2020) 7 <https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-australian-privacy-index-2020.pdf>.

[41] See generally, this 2018 report from the Consumer Council of Norway presents a detailed explanation of some of the ways Google, Facebook and Microsoft use default settings, 'dark patterns' and features of interface design to nudge users towards privacy intrusive options: Forbrukerådet [Norwegian Consumer Council], *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy* (2018) <https://www.forbrukerradet.no/dark-patterns/>.

for the collection of precise location data, ensuring that users are aware and are able to opt out. This is warranted based on the extremely invasive nature of such information and its particular scope for abuse.

The Discussion Paper asks whether entities should be required to refresh or renew an individual's consent on a periodic basis where such consent is obtained for the collection, use or disclosure of sensitive information. If proposal 10.1, for a 'fair and reasonable' requirement is adopted, a separate requirement to periodically refresh or renew consent is unnecessary, as the more flexible reasonableness requirement will operate to prevent inappropriate ongoing reliance on old consents.

Proposal 9.2	*Standardised consents could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consents.*
elevenM position	We support proposal 9.2.

As noted above, the Consumer Experience work stream for the CDR Consumer Data Standards provides a good example of how a program of consumer experience research can be deployed from exploratory research through to prototype testing to understand consumer expectations, needs and behaviours in a particular field.[42]

10. Additional protections for collection, use and disclosure

A general 'fair and reasonable' handling obligation

Proposal 10.1	*A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.*
Proposal 10.2	*Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances could include:* • *Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances* • *The sensitivity and amount of personal information being collected, used or disclosed*

[42] Data61 (n 36).

- *Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information*
- *Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity*
- *Whether the individual's loss of privacy is proportionate to the benefits*
- *The transparency of the collection, use or disclosure of the personal information, and*
- *If the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child.*

elevenM position We strongly support proposals 10.1 and 10.2.

Organisations, not individuals, should be primarily responsible for preventing privacy harms. Proposals 10.1 and 10.2 present an important step towards a regulatory framework centred on organisational accountability and harm prevention, rather than on individual self-management. This shift aligns with consumer expectations, and with the regulatory approach adopted in similar contexts — such as product safety, consumer protection, occupational health and safety, and the regulation of financial services — where it is recognised that 'buyer beware' is neither effective nor economically efficient.

Strengthening mechanisms for consent and transparency may be of some benefit, but no matter how streamlined or simplified privacy policies and notices become, most Australians will still not have the time, inclination or expertise to make informed decisions about future privacy risks. As the ANU Humanising Machine Intelligence Project submitted to the Issues Paper, self-management mechanisms must be scaffolded by robust institutional assurances, so that consumers can trust that their digital safety does not depend on their unfailing vigilance and the vigilance of their fellow Australians'.[43]

Rather than requiring individuals to understand how a product or service may be harmful to them and to take steps to avoid that harm, it is preferable to prevent the harm itself.[44] This is consistent with principles of Australian Consumer Law with respect to product safety and unfair business practices, and is overwhelmingly the expectation of consumers:

[43] ANU Humanising Machine Intelligence Project, Submission to the Australian Attorney-General's Department, *Privacy Act Review Issues Paper* (2020) 2 <https://www.ag.gov.au/sites/default/files/2021-01/humanising-machine-intelligence-project-australian-national-university.PDF>.

[44] CHOICE, Submission to the Australian Attorney-General's Department, *Privacy Act Review – Issues Paper* (December 2020) 2 < https://www.ag.gov.au/sites/default/files/2021-01/choice.PDF>.

- 94% of consumers expect government to protect them against the collection and sharing of their personal information, and
- 94% of consumers expect government to protect them from having their information being used in a way that makes them worse off.[45]

The proposed 'fair and reasonable' requirement should apply to all collection, use or disclosure of personal information by all APP entities, regardless of the legal basis for processing — be it consent, authorised by law or under another exemption. It would be anomalous if the presence of consent or a legal authorisation excused an APP entity from acting fairly or reasonably, or permitted opaque information handling, excessive collection/disclosure, or unjustified risks to individuals. The standard offers sufficient flexibility to take the presence of consent or a legal authorisation into account.

We do not expect the fair and reasonable test to have a significant impact on the business operations of most entities. Most standard Privacy Impact Assessment (**PIA**) processes already take many of the proposed factors into account, including community expectations, data minimisation and risks. As the Discussion Paper notes, the new requirement would only impose regulatory burden on those entities that handle personal information in a manner that is inconsistent with community expectations.

The Discussion Paper seeks stakeholders' views on how the new fair and reasonable requirement should interact with existing obligations within APPs 3 and 6. We recommend the new requirement should be applied in an overarching way, as a new positive obligation applying to all handling of personal information. Other more focused requirements that draw on standards of reasonableness or that overlap with the proposed factors (such as transparency or reasonable expectations) should be retained. Focused requirements (eg: that the manner of collection not be unreasonably intrusive, or that a particular disclosure accord with an individual's reasonable expectations) are not equivalent or interchangeable with a wholistic requirement that collection, use or disclosure be reasonable in the circumstances.

Due diligence for third party collections

Proposal 10.3	*Include an additional requirement in APP 3.6 to the effect that that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3.* *Commissioner-issued guidelines could provide examples of reasonable steps that could be taken, including making reasonable enquiries regarding the collecting entities' notice and consent*

[45] Consumer Policy Research Centre (n 33).

	procedures or seeking contractual warranties that the information was collected in accordance with APP 3.
elevenM position	We support proposal 10.3.

In our experience, most APP entities acquiring data from third party sources already conduct some level of due diligence to ensure the legality and appropriateness of the information source. As such, we expect the cost of compliance with this additional requirement to be low. However, clear guidance from the OAIC on what steps are considered reasonable will be essential, particularly for smaller APP entities.

Defining primary and secondary purpose

Proposal 10.4	*Define a 'primary purpose' as the purpose for the original collection, as notified to the individual.* *Define a 'secondary purpose' as a purpose that is directly related to, and reasonably necessary to support the primary purpose.*
elevenM position	We do not support proposal 10.4.

We would welcome further legislative clarity on the definition of 'primary purpose', however we submit that any definition should retain the current features of the concept, being that it refers to the specific function or activity for which the information is collected, narrowly defined and objectively determined.

Proposal 10.4 risks turning the determination of the primary purpose of a collection from an objective test to something that is wholly determined by the APP entity. That is, the proposed definition would elevate an APP entity's statement of the primary purpose of collection over any analysis of the true or actual purpose based on context or circumstances.

The proposal would have the effect of broadening APP entities' discretion to use and disclose personal information for self-defined 'primary purposes' that are neither necessary nor beneficial to consumers, provided only that those additional purposes are notified to the individual. The proposal could therefore undermine the current protections in APP 6.2 that the restrict use and disclosure of personal information for any purpose other than the (narrowly defined) primary purpose of collection, unless related and reasonably expected, or consent is obtained.

Consider, for example, a mobile phone service provider wishing to use or sell subscriber location or usage data for advertising purposes. As a secondary purpose, this would require the service provider to obtain consent or establish that such use/disclosure is related to the primary purpose of collection and reasonably expected. Under proposal 10.4, provided this further use was notified as a 'primary purpose', nothing further would be required.

Further, APP entities would be incentivised to provide long lists of 'primary purposes' in collection notices, covering the range of activities presently permitted under APP 6.2(a) (use/disclosure for a reasonably expected secondary purpose).

Finally, we are concerned that the proposed limitation of 'secondary purpose' to purposes 'directly related to and reasonably necessary to support the primary purpose' may not permit certain secondary uses that are generally accepted by the community — such as strategic business planning or improving internal processes. It is artificial and divergent from ordinary usage to include such purposes as 'primary'.

Research exemptions

elevenM position	We support Salinger Privacy's proposal for the inclusion of a public interest research exemption in APP 6.2 in place of the current tests in sections 16B, 95 and 95A.

We support the submissions made by Salinger Privacy with respect to the unnecessary restrictions on public interest research as a result of the drafting of sections 16B, 95 and 95A. We support Salinger Privacy's proposal for the inclusion of a public interest research exemption in APP 6.2 in place of the current tests.[46]

11. Restricted and prohibited practices

Restricted practices

Proposal 11.1	***Option 1*** *APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:* • *Direct marketing, including online targeted advertising on a large scale* • *The collection, use or disclosure of sensitive information on a large scale* • *The collection, use or disclosure of children's personal information on a large scale* • *The collection, use or disclosure of location data on a large scale*

[46] Salinger Privacy (n 26).

	• *The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software* • *The sale of personal information on a large scale* • *The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale* • *The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects, or* • *Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.* ***Option 2*** *In relation to the specified restricted practices, increase an individual's capacity to self-manage their privacy in relation to that practice.* *Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted practices (see Chapter 14), or by ensuring that explicit notice for restricted practices is mandatory.*
elevenM position	We support option 1 of proposal 11.1, subject to further refinement of the listed categories. We recommend that the restricted practices include 'Any collection, use or disclosure that **may** result in a high privacy risk or risk of harm to an individual'. We do not support option 2 of proposal 11.1. If option 1 is enacted, care should be taken to make it clear that the requirement does not limit an organisation's more general obligations under APP 1.2 and under the proposed 'fair and reasonable' requirement (if adopted).

As we have noted above in relation to proposals 10.1 and 10.2, we submit that the review should seek to shift the focus of the regulatory framework for privacy towards organisational accountability and harm prevention, and away from individual self-management. Option 2 effectively places responsibility for identifying and avoiding foreseeable privacy harms arising from high-risk practices on the individuals that they effect, rather than the organisations that profit from those practices. We do not support this approach. Organisations, not individuals, should be primarily responsible for preventing privacy harms.

We support the approach outlined in option 1, to introduce a two-part obligation with respect to the specified restricted practices:

i. to take reasonable steps to identify privacy risks;
ii. to take reasonable steps or implement measures to mitigate those risks.

The first obligation is at least partially covered by APP entities' obligations under APP 1.2. An organisation that fails to take reasonable steps to identify privacy risks of a high risk

privacy activity is likely to be lacking the practices, procedures and systems required under APP 1.2. For example, the Commissioner recently found Clearview AI breached APP 1.2 by failing to conduct 'a systematic assessment of measures and controls that should be implemented to identify and mitigate the risks' of its facial recognition tool.[47]

Including this first obligation as part of a separate and explicit requirement attached to higher risk activities would have the benefit of clarifying and codifying the expectation that a PIA be done in those circumstances.

The second obligation is well aligned to proposal 10.1 in that it focuses APP entities' attention on the management of risk and the prevention of harm, rather than on tick-box compliance. In this way, option 1 supports the regulatory objectives of encouraging flexibility, Privacy by Design and organisational accountability. The option would help to keep compliance costs to a minimum by giving organisations the flexibility to choose how to manage privacy risks and by requiring only those measures that meaningfully drive down risk.

One potential downside of option 1 is that it may support an interpretation that privacy risk assessment and mitigation is required only with respect to the specified high risk activities, and is not otherwise required. If option 1 is enacted, care should be taken to make it clear that the requirement does not limit an organisation's more general obligations under APP 1.2 and under the proposed 'fair and reasonable' requirement (if adopted).

We are also concerned that the catch-all in the final dot point in the list of restricted practices may set the bar too high by requiring a likelihood of 'high privacy risk or risk of harm'. This may be interpreted by APP entities as requiring a likelihood (i.e. greater than 50% chance) of interfering with individuals' privacy or causing harm, thus excluding practices that may have a lower chance of more significant impacts. We recommend that either the list of categories be amended or that it be accompanied by guidance that qualifies practices that may carry a lesser chance of a more serious interference with privacy or more serious harm.

Prohibited practices

elevenM position	Rather than seeking to enshrine specific no-go zones in legislation, we recommend that proposal 10.1 be adopted and that the OAIC publish guidance identifying practices generally considered to be unreasonable, supported by a requirement that APP entities have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

[47] *Commissioner initiated investigation into Clearview AI, Inc. (Privacy)* [2021] AICmr 54 (14 October 2021) [219]–[234].

While we support the introduction of no-go zones, we share the Review's concern that any prohibited practice would need to be carefully calibrated and appropriately targeted. We support the approach taken by the Office of the Privacy Commissioner of Canada, which has effectively established no-go zones through guidance on the application of a general 'appropriateness' standard, similar to proposal 10.1 in the Discussion Paper for a 'fair and reasonable' requirement. Rather than seeking to enshrine specific no-go zones in legislation, we recommend that proposal 10.1 be adopted and that the OAIC publish guidance identifying practices generally considered to be unreasonable. Guidance could be informed by the OAIC's experience as the regulator, consultation with industry and the community, and the OAIC's research work, including the Australian Community Attitudes to Privacy Survey.

To further support this approach, we repeat our recommendation (in section 3 above) that the status of the Commissioner's APP guidelines be elevated through a new provision that would require entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

12. Pro-privacy default settings

Proposal 12.1	***Option 1 — Pro-privacy settings enabled by default*** *Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.* ***Option 2 – Require easily accessible privacy settings*** *Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.*
elevenM position	We strongly support option 1. We support option 2, but only in addition to option 1 and not as an alternative.

Research in behavioural economics shows that when people are presented with a pre-selected option, they are significantly more likely to select that option – particularly in consumer contexts where the default choice is conveyed as either a recommendation or the

status quo.[48] This is often referred to as the 'default effect'. The default effect is particularly powerful for settings and defaults that remain 'under the hood' and are not presented to users as choices to be made.[49] An investigation by the Norwegian Consumer Council in 2018 found that Facebook, Google and Microsoft all employed privacy intrusive default settings, many of which were obscured or difficult to find and change.[50]

High-privacy default settings may be less convenient for some users and businesses, but would better protect individuals at greater risk of harm from misuse or unintended disclosure of personal information (such as survivors of family violence). High-privacy default settings would also support individuals with more limited technical, critical and social skills to start from a safer base and exercise greater control and autonomy over their settings.

We anticipate that requiring high-privacy default settings would drive better design practices around privacy settings and contribute to user awareness and control. As a practical matter, the requirement would likely result in services presenting users with a range of choices as to basic privacy settings and defaults as part of their account creation or customer onboarding process. In combination with strengthened transparency and consent requirements, pro-privacy defaults would contribute significantly to individuals' awareness and agency in how their data are used and shared.

13. Children and vulnerable individuals

Parent or guardian consent

Proposal 13.1	*Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16. The review is seeking additional feedback on whether APP entities should be permitted to assess capacity on an individualised basis where it is practical to do so.* *Feedback is also sought on the circumstances in which parent or guardian consent must be obtained:* ***Option 1 – All collections of personal information***

[48] Jon M Jachimowicz et al, 'When and Why Defaults Influence Decisions: A Meta-Analysis of Default Effects' (2019) 3(2) *Behavioural Public Policy* 159.
[49] For example, an analysis of Microsoft Word users showed less than 5% of users changed any settings at all: Jared Spool, 'Do Users Change Their Settings?' (Web Page, 14 September 2011), <https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/>.
[50] Forbrukerrådet, *Deceived by Design* (n 41).

	Parent or guardian consent to be required before collecting, using or disclosing personal information of the child under the age of 16. ***Option 2 – Where consent is currently required under the Act*** *Parent or guardian consent to be required in respect of a child under the age of 16 in situations where the Act currently requires consent, including before the collection of sensitive information or as an available mechanism to undertake a secondary use or disclosure of personal information.* *The assumed age of capacity would also determine when a child may exercise privacy requests independently of their parents, including access, correction or erasure requests.*
elevenM position	We do not support option 1. We support option 2.

We do not support option 1. Children's privacy is better protected by stronger mechanisms for organisational accountability and privacy by default, such as those outlined in proposals 10.1 and 10.2 (fair and reasonableness requirements), 11.1 (restricted and prohibited practices) and 12.1 (pro privacy default settings). These proposals, based on standards of reasonableness, scale effectively to afford higher standards of protection towards younger children and more vulnerable individuals. If enacted, it will be safe (and indeed preferable) to place less emphasis on consent as a basis for processing personal information.

Option 1 would elevate the role of consent and push more of the burden of protecting children's privacy (and the cost of getting it wrong) onto parents. Relying on parental consent is not an effective way of protecting the privacy of children at any age. Expecting all parents to understand and evaluate privacy risks associated with the complex data and advertising ecosystems underlying every app, game or online service that their child may use is unrealistic and puts unfair pressure on parents to be the safety net against poor privacy practices. As we (and others) have argued in relation to proposal 10.1, rather than requiring individuals to understand how a product or service may be harmful to them and to take steps to avoid that harm, it is preferable to prevent the harm itself.

Further, for older children, a blanket requirement for parental consent would be impracticable and would negatively impact a child's autonomy and development. Virtually every service or product in the modern digital economy involves the processing of some amount of personal information. The effect of a blanket parental consent requirement would be that children under 16 would be entirely unable to operate in the world without parental supervision.

Option 2 preserves children's rights to autonomy and participation, while maintaining a parental safety net with respect to higher-risk practices.

Age of consent

Proposal 13.1	*Proposal 13.1 would set the assumed age of capacity at 16.*
elevenM position	Subject to the results of further consultation with stakeholders, the existing standard under the Privacy Act and OAIC guidance should be maintained. That would apply: • a cut-off age of 15 for a rebuttable presumption with respect to capacity, and • the ordinary standard for the quality of consent, which requires that the individual must have capacity, and that consent must be informed, voluntary, current and specific.

In our research on privacy risks and harms for children and other vulnerable groups in the online environment conducted for the OAIC, we observed that despite a growing body of empirical evidence into the capacities of children and adolescents to make their own privacy decisions, there is no consensus as to the most appropriate age of consent.[51] Approaches in overseas jurisdictions are not evidence-based and range from 13 to 18 years of age.

We recommended that future Australian regulation should therefore aim to stipulate an age limit at which it can be assumed that a child of ordinary capacities and development will have capacity to make their own privacy decisions.

Any such threshold-setting necessarily involves a balancing of a range of factors and interests, including risk to children, children's autonomy and participatory rights, the impracticability of individual capacity assessment in most contexts and the desirability for industry of bright-line rules. There is no single number that will strike this balance appropriately for all people across all contexts to which the Privacy Act applies. On this basis, we support maintaining the status quo, pending further research and engagement leading to sector-specific age thresholds being set.

APP 5 notices for children

Proposal 13.2	*Require APP 5 notices to be clear, current and understandable, in particular for any information addressed specifically to a child.*
elevenM position	We strongly support proposal 13.2. We also recommend that the review adopt a further, general obligation to take reasonable steps to ensure that any collection, use

[51] Monash-elevenM research (n 2) 82–95.

	or disclosure of personal information be transparent to the individuals affected be adopted (discussed in section 8 above).

In our research on privacy risks and harms for children and other vulnerable groups in the online environment conducted for the OAIC, we examined in detail, the challenges and strategies for delivering effective notification for children.[52] We observed that the length and complexity of privacy policies and notices are a barrier to children just as they are to adults, and that children need specific modes of communication to ensure they understand and engage with the information that is being given to them.

Research has shown that although they struggle with 'standard' social media platform privacy policies, older children and teens are easily able to understand simplified privacy policies that have specifically been drafted for children. For example, a study conducted by the UK Children's Commissioner in 2017 showed how Instagram's Terms and Conditions could be redrafted as a one-page, child friendly document that could be easily understood by a test group of children aged 13–17.[53]

Privacy transparency for children should aim for more than mere disclosure of material facts. It should aim to educate, empower, and enable privacy self-management, accounting for a child's developing needs and capabilities. Children are not equipped to bear responsibility for reading and understanding collection notices or privacy policies (however simply drafted), nor is it reasonable to expect them to have the cognitive ability and background knowledge to understand how a disclosed act or practice is likely to impact them.

The onus should be on platforms to help children to understand and contextualise privacy disclosures by:

- using the most effective tools and strategies for clear communication,
- taking into account children's specific needs, vulnerabilities and contexts, and
- adopting design practices for privacy disclosures that involve children and ensure their effectiveness.

14. Right to object and portability

Proposal 14	*An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information. On receiving notice of an objection, an entity must take reasonable steps*

[52] Monash-elevenM research (n 2) 102–119.
[53] Children's Commissioner, *Growing up Digital – A Report of the Growing Up Digital Taskforce* (Report, January 2017) <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf> 8–12 ('Growing Up Digital').

	to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection
elevenM position	We support a right to object or withdraw consent under the Privacy Act.

We support the model for a right to object or withdraw consent as outlined in the Discussion Paper. We note our above support for proposals 9.1 (consent), and 10.1 and 10.2 (fair and reasonable requirements) and consider that if both proposals are implemented, a right to object or withdraw consent would be useful in providing additional certainty about the extent and application of those provisions.

Such a right would provide individuals with enhanced ongoing control over how their personal information is used or disclosed once it has been collected. We note there are two distinct elements of the proposal that have not been fully explored or distinguished in the Discussion Paper:

1. the right to withdraw consent (which would be limited to the situations under the APPs where consent is required), and
2. the right to object to the collection, use or disclosure of personal information.

We support the inclusion of both elements of the proposal and consider they would be particularly useful to data subjects in circumstances, including where:

1. a data subject has already actively provided personal information (for example, in an online form), but then wishes to withdraw consent or 'undo' that provision of information and prevent the information from being used by the entity, and
2. a data subject is monitored, for example through online tracking or by CCTV camera, and later receives an APP 5 notice advising of the collection, at which point a right to object would enable the data subject to make a choice.

A right to withdraw consent would codify the OAIC's current APP guidance on consent, which establishes the principle that consent must be current and specific (this necessarily includes enabling an individual to withdraw their consent at any time, which should be an easy and accessible process). A right to object would be broader and would apply to information handling by entities generally (without being limited to situations requiring consent), providing individuals with a level of choice not presently available.

We support the position put forward in the Discussion Paper, that a right to object not necessarily become grounds for an entity to refuse access to a service. Instead, we agree that a fair and reasonable test would require consideration of 'the amount and sensitivity of the personal information collected and whether its use was reasonably necessary to achieve the functions and activities of the entity such that the individual could not be offered the service without it' and 'whether the individual's loss of privacy as a result of the collection,

use or disclosure is proportionate to the benefit of the service'.[54] We suggest OAIC guidance should be developed to help entities understand such considerations. Guidance should also be developed to assist entities understand what might constitute a 'reasonable steps' requirement (see our comments on proposal 19 below).

15. Right to erasure of personal information

Proposal 15.1	*An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions at 15.2, below:* • *the personal information must be destroyed or de-identified under APP 11.2* • *the personal information is sensitive information* • *an individual has successfully objected to personal information handling through the right to object (see Chapter 14)* • *the personal information has been collected, used or disclosed unlawfully* • *the entity is required by or under an Australian law, or a court/tribunal order, to destroy the information, and* • *the personal information relates to a child and erasure is requested by a child, parent or authorised guardian.*
Proposal 15.2	*Provide for exceptions to an individual's right to erasure of personal information. An APP entity could refuse a request to erase personal information to the extent that an exception applied to either all or some of the personal information held by an APP entity.*
Proposal 15.3	*An APP entity must respond to an erasure request within a reasonable period. If an APP entity refuses to erase the personal information because an exception applies, the APP entity must give the individual a written notice that sets out the reasons for refusal and mechanisms available to complain about the refusal, unless unreasonable to do so.*
elevenM position	We strongly support the introduction of a right to erasure under the Privacy Act.

[54] Attorney-General's Department (n 12) 113.

	We suggest the right be carefully crafted to ensure its accessibility to data subjects. Relevant exceptions to this right should be limited to those included in Article 17 of the GDPR.

We strongly support the introduction of a right to erasure under the Privacy Act. The risks posed by the sharing of personal information online are becoming increasingly apparent (risks that may not have been generally understood a decade ago), while consumer concerns about personal protections in the digital age continue to increase. A right to erasure would empower individuals to assert a level of control over their personal information and address the lag in individual privacy literacy which, for many individuals, has resulted in the unwitting sharing of huge amounts of personal information either voluntarily (e.g. via social media) or because such sharing was necessary to access a product or service. As this Review considers mechanisms to enhance individual privacy protections, and limit the purposes for, and situations in which, personal information can be collected in future, it is appropriate to acknowledge and provide a mechanism to address the very real risks posed by the past excessive sharing of information (including by children).

We recognise that in creating any such right, there is a need to ensure the appropriate balancing of competing interests, including those of business in not being overburdened by excessive requests or compliance costs. In practice, we query the likelihood of the excessive uptake of this right however. In our experience, data subject rights currently available under the Act, while important, are not heavily used. For example, large enterprises with millions of customers often receive only a handful of access or correction requests under the Act every year. We suggest that the concerns about an influx of erasure requests, as outlined in the Discussion Paper, are largely unfounded.

We do, however, acknowledge that there may be initial costs associated with IT works to make erasure possible, although we note this would be mitigated by the proposed exception where erasure is technically impractical. Implementation costs could be further eased by including a transition period to allow APP entities sufficient time to prepare.

List of exceptions

The Discussion Paper's proposed model is based on Article 17 of the GDPR and is fairly restrictive in nature. It would confer a fettered right on an individual to request erasure of their personal information under certain prescribed circumstances, subject to any overriding exceptions. Under the proposal, an APP entity would need to respond to an erasure request 'within a reasonable period' (not defined), and if it refuses to erase the personal information because an exception applies, it would need to give the individual written reasons.[55]We support the premise that a person should have a right to seek the erasure of their personal information where there is no need for, or no countervailing interest in, its retention. To

[55] Attorney-General's Department (n 12) 123.

provide any meaningful benefit to an individual, careful formulation is required to ensure that the list of circumstances within which erasure would be available, together with any prescribed exceptions, do not unnecessarily restrict access to this right.

At the least, we suggest limiting the list of exceptions to correspond with the exceptions included in Article 17 of the GDPR, with necessary modifications for the Australian context.

Public interest exception

We recognise there may be legitimate public interest grounds for retaining personal information in some circumstances, including for reasons such as freedom of speech and the media, and we acknowledge the difficulty of adapting the GDPR's freedom of expression exception to an Australian context. While we support a limited exception of this nature, we suggest that without clear parameters and guidance, such an exception could be used to prioritise trivial matters perceived to be 'in the public interest' at the expense of individual privacy interests. We draw the Department's attention, as an example, to the 'barbecue man' incident in NSW in May 2021, during which the Australian Financial Review defended its decision to publish sensitive health information about an individual without his consent, because the individual was a 'prominent businessman involved in a number of key business transactions and it was newsworthy and in the public interest to explain his movements given the ongoing reporting around the visits.'[56] Such a defence has been widely criticised, including by NSW Ministers, members of the public and other media organisations, as contrary to public health outcomes.

Even if the exception is modelled on the FOI Act test as the Discussion Paper proposes, we foresee risks with its application, noting that it would be available to all APP entities, including private sector organisations, many of which would have no experience making decisions of this nature. Use of this exception would rely on APP entities independently weighing up, and making a judgment call about, whether and to what extent the public interest outweighs an individual's interest.

We perceive a real risk of entities' overreliance on a discretionary exception of this kind. If such an exception is included, it should be very clearly constrained and be accompanied by detailed OAIC guidance as to its limits and appropriate application. Such guidance should clarify the extent to which particular types of information (for example, information about

---

[56] Amanda Meade, 'NSW health minister condemns media for naming Sydney 'barbecue man' at centre of Covid outbreak', *The Guardian* (online, 10 May 2021) < https://www.theguardian.com/australia-news/2021/may/10/nsw-health-minister-condemns-media-for-naming-sydney-barbecue-man-at-centre-of-covid-outbreak>.

For completeness, we note that under section 15 of the *Health Records and Information Privacy Act 2002* (NSW), there is a broad exemption available to media organisations for the disclosure of health information 'in connection with its news activities'.

children or sensitive information) are to be afforded greater weight in an entity's balancing exercise. A statutory presumption in favour of erasure as an overarching guiding principle should be included.

We also suggest a right to an OAIC review of an erasure decision should be enlivened following an entity's written response to the request. Inclusion of a limit of 30 days for an entity's erasure decision should be included, in line with the period in which agencies must currently respond to access or correction requests, and the period that the OAIC views as 'reasonable' for organisations.

16. Direct marketing, targeted advertising and profiling

An unqualified right to object to direct marketing

Proposal 16.1	*The right to object, discussed at Chapter 14, would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. An individual could still request not to receive direct marketing communications from an organisation. If an organisation provides marketing materials to an individual, it must notify the individual of their right to object in relation to each marketing product provided.* *On receiving notice of an objection, an entity must stop collecting, using or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.*
elevenM position	We support proposal 16.1. We also support additional protections being attached to profiling.

The main privacy harms (and community concerns) associated with direct marketing flow from the activities that precede, support or even follow the actual marketing communication, for example:

- Pervasive digital tracking and surveillance to collect behavioural data for use in profiling and targeting of direct marketing.
- The creation of detailed behavioural, demographic or interest-based profiles.
- The tailoring of offers or services to these profiles in ways that might be unfair or adversely impact the individual (such as denial of service or preferential pricing).

By providing an unqualified right to opt-out of all handling of their personal information for the purposes of direct marketing, proposal 16.1 better targets protections and user control towards the sources of privacy harm.

Notification of use or disclosure for the purpose of influencing behaviour or decisions

Proposal 16.2	*The use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected.*
elevenM position	We do not support proposal 16.2. We would support the proposal in a different form, namely if: • The use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions may be as a primary or a secondary purpose but must be notified to the individual when their personal information is collected. • The term 'influencing an individual's behaviour or decisions' is clarified to narrowly target activities that adversely impact individual privacy or autonomy.

We support the objective of increasing transparency with respect to the collection, use and disclosure of personal information for direct marketing purposes, and would support a requirement that an individual be notified of such use on collection. However, for most businesses, personal information is not collected for direct marketing as a primary purpose — rather it is collected to support the sale of a product or provision of a service. We are concerned that requiring collection notices to frame direct marketing as a primary purpose in all circumstances may be distorting and misleading. We believe the same transparency objective can be met without requiring that direct marketing be described as a primary purpose.

As we have argued in relation to proposal 10.4 above, we consider that an important feature of the current operation of the Act is that the 'primary purpose' of collection is objectively determined and constrained with respect to the primary function or activity for which personal information is being collected. Like proposal 10.4, proposal 16.2 risks establishing an overly broad concept of 'primary purpose', which is entirely at the discretion of the collecting APP entity.

We are also concerned that the phrase '*influencing an individual's behaviour or decisions'* may be unintentionally and unreasonably broad. Virtually any business activity can be described as intended to influence an individual's behaviour or decisions — a non-personalised mail-out catalogue is intended to influence an individual's behaviour or decisions towards a purchase, for example. Internal cybersecurity training for personnel within an organisation is similarly intended to influence behaviour or decisions. If this phrase is to be adopted, it will require further clarification within the Act and through guidance.

An alternative approach would be to frame protections around specific activities aimed at influencing an individual's behaviour or decisions, such as profiling or algorithmic variation of content served to an individual (eg: via search, recommendations, or a news feed).

Privacy policy to cover use or disclosure for the purpose of influencing behaviour or decisions

Proposal 16.3	*APP entities would be required to include the following additional information in their privacy policy:* • *whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual, and* • *whether the entity uses third parties in the provision of online marketing materials and if so, the details of those parties and information regarding the appropriate method of opting-out of those materials.*
elevenM position	We do not support proposal 16.3. We would support the proposal in a different form, namely if the term 'influencing an individual's behaviour or decisions' were clarified to narrowly target activities that adversely impact individual privacy or autonomy.

As noted in relation to proposal 16.2 above, we are also concerned that the phrase '*influencing an individual's behaviour or decisions'* may be unintentionally and unreasonably broad and could encompass a very wide range of activities carrying little privacy risk.

If this phrase is to be adopted, it will require further clarification within the Act and through guidance. Alternatively, it may be more appropriate to focus protections on specific activities aimed at influencing an individual's behaviour or decisions, such as profiling or algorithmic variation of content served to an individual (eg: via search, recommendations, or a news feed). These may be appropriate for inclusion in the Online Privacy Code.

Repealing APP 7

Proposal 16.4	*Repeal APP 7 in light of existing protections in the Act and other proposals for reform.*
elevenM position	We support proposal 16.4.

Not all forms of direct marketing present privacy risks. The privacy risks associated with mailing a catalogue or newsletter to an existing customer base for example, are minimal and do not warrant a dedicated privacy principle.

As we have noted in relation to proposal 16.1, the main privacy harms today (and community concerns) associated with direct marketing, flow from the tracking, profiling and discrimination that precede, support and follow the actual marketing communication.

We agree with the position taken in the Discussion Paper that the risks associated with direct marketing can be more appropriately managed through a combination of the ordinary application of APP 6 and the following proposals:

- Proposals 2.1 and 2.2 to expand the definition of personal information to include technical identifiers and other data used to explicitly target an unidentified individual's personal preferences.
- Proposal 2.4 to clarify that inferred information is 'collected'.
- Proposal 8.1, 8.2 and 8.3 to strengthen notice requirements.
- Proposal 9.1 to strengthen the standard required for consent.
- Proposal 10.1 and 10.2 to establish a general requirement that personal information handling be fair and reasonable.
- Proposal 11.1 to introduce obligations to assess and manage privacy risks in relation to certain acts and practices (including targeted advertising, behavioural modification and automated decision making).

17. Automated decision-making

Proposal 17.1	*Require privacy policies to include information on whether personal information will be used in ADM which has a legal, or similarly significant effect on people's rights.*
elevenM position	We do not support proposal 17.1 in its current form, but would support a stronger proposal requiring at minimum that notice of ADM include meaningful information about the decision-making logic involved, as well as the significance and the envisaged consequences of such

processing for the data subject (consistent with the equivalent GDPR obligation).

In addition to requiring notice and transparency with respect to ADM, we recommend the Review adopt similar measures to California and the EU to allow individuals to access further information, opt out, question results, request human review or contest an automated decision.

Automated decision-making (**ADM**) has significant potential benefits, but also presents serious new risks to human rights, individual welfare and social cohesion. These risks go beyond the lack of transparency noted in the Discussion Paper. In its 2021 report on Human rights and technology, the Australian Human Rights Commission (**AHRC)** concluded that in order to ensure that human rights are protected, in addition to being transparent, AI-informed decision making should be lawful, explainable, used responsibly, and subject to appropriate human oversight, review and intervention.[57]

We consider that ADM based on personal information is a proper subject for regulation through the Privacy Act, and has sufficiently significant potential impacts to warrant specific treatment within the Act, in line with other jurisdictions.

Coverage of ADM should not be limited to fully automated processes. We also support the AHRC's preference for the terminology 'AI informed decision-making'. There is increasing evidence that human oversight has only limited effectiveness in preventing or managing harms arising from ADM.[58] Even when deployed in meaningful ways, it can be difficult to meaningfully evaluate algorithmic advice, and human oversight can suffer from automation bias (the tendency to defer to or over-value conclusions made by automated systems).

Requiring a bare notice of the use of ADM within an organisation's privacy policy will do nothing to empower individuals, or to shift organisational behaviours towards responsible uses. Without also requiring some level of transparency as to the nature and function of the ADM system or how it is used, we submit that the proposal would achieve little. At a minimum, notice of ADM should also be required to include meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (consistent with the equivalent GDPR obligation).

Further, we submit that even full transparency with respect to ADM is of little value unless individuals have some recourse when they have concerns. In addition to requiring notice and transparency with respect to ADM, we recommend the Review adopt similar measures to

[57] Australian Human Rights Commission, *Human Rights and Technology Final Report* (2021) 12.

[58] See, eg, Ben Green and Amba Kak, 'The false comfort of human oversight as an antidote to AI harm' *Slate* (Web Page, 15 June 2021) <https://slate.com/technology/2021/06/human-oversight-artificial-intelligence-laws.html>.

California and the EU to allow individuals to access further information, opt out, question results, request human review or contest an automated decision.

Finally, as we have argued above in relation to proposal 10.1 and elsewhere, we are generally sceptical of controls that place primary responsibility for investigating, understanding and avoiding harms on the individual. While individual rights are important with respect to ADM, we believe that organisations, not individuals, should be primarily responsible for preventing privacy harms. We anticipate that proposals 10.1 ('fair and reasonable' requirement) and 11.1 (restricted and prohibited practices) would be effective in driving greater organisational accountability for ADM.

18 Accessing and correcting personal information

Identifying the source of personal information

Proposal 18.1	*An organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort.*
elevenM position	We strongly support proposal 18.1.

We strongly support proposal 18.1. Requiring an entity to identify the sources of personal information that it has not collected directly from the individual would be an important step toward enhancing transparency and enabling individuals to benefit from the various data subject rights (for example, the right to object or withdraw consent, and the right to erasure) proposed in the Discussion Paper.

Businesses are increasingly able to glean valuable insights about their customers through the acquisition of personal information, including inferences, from a range of third-party providers. As the commodification of personal information increases, largely unregulated, individuals often have no way of knowing who has acquired or holds information about them (particularly if they have no direct relationship with those businesses).

The former United Kingdom Information Commissioner, Ms Elizabeth Denham, commented in 2020 on the issues with the data broking industry:

> *The data broking sector is a complex ecosystem where information appears to be traded widely, without consideration for transparency, giving millions of adults in the UK little or no choice or control over their personal data. The lack of transparency and lack of lawful bases combined with the*

> *intrusive nature of the profiling has resulted in a serious breach of individuals' information rights."*[59]

There is a growing international trend toward enhancing transparency around the collection and sale of personal information. We note the California Consumer Privacy Act (**CCPA**), for example, requires data brokers (with annual revenue above USD25 million or that collect data on more than 50,000 people) to:

1. register annually with the Californian Attorney General, and
2. ensure a conspicuous 'do not sell my personal information' link is included on all web and mobile sites.

These requirements help consumers understand which organisations are in the business of collecting and selling personal information and give consumers an express ability to opt-out of the sale of their data by those businesses.

Proposal 18.1 would go some way toward enhancing individuals' understanding about which companies – including those they may have no direct relationship with – hold information about them. While it would not go as far as the CCPA, it would allow an individual to take steps to control the handling of their personal information, including via the proposed new right to object or right to erase, once they become aware (via an access request) of the businesses that might hold information about them for purely commercial purposes.

We suggest that any exceptions to this enhanced access right be very clearly constrained so as not to enable entities to rely on a 'disproportionate effort' exception to justify poor information management practices or a desire to not be transparent.

Other refinements to access rights

Proposal 18.2 *Introduce the following additional ground on which an APP organisation may refuse a request for access to personal information:*

- *the information requested relates to external dispute resolution services involving the individual, where giving access would prejudice the dispute resolution process.*

[59] Information Commissioner's Office, 'ICO takes enforcement action against Experian after data broking investigation' (Web Page, 27 October 2020) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation>.

Proposal 18.3	*Clarify the existing access request process in APP 12 to the effect that:* • *an APP entity may consult with the individual to provide access to the requested information in an alternative manner, such as a general summary or explanation of personal information held, particularly where an access request would require the provision of personal information that is highly technical or voluminous in nature, and* • *where personal information is not readily understandable to an ordinary reader, an APP entity must provide an explanation of the personal information by way of a general summary of the information on request by an individual.*
elevenM position	We support proposals 18.2 and 18.3.

We support proposals 18.2 and 18.3 and consider that to provide any meaningful benefit to individuals, information provided under an access right should be easily digestible by a lay consumer. We support measures to encourage an open dialogue between entities and individuals, and a requirement for entities to help customers understand the nature of the personal information the business holds about them.

19. Security and destruction of personal information

Clarifying 'reasonable steps for security

Proposal 19.1	*Amend APP 11.1 to state that 'reasonable steps' includes technical and organisational measures.*
Proposal 19.2	*Include a list of factors that indicate what reasonable steps may be required.*
elevenM position	We support proposal 19.1. We do not support proposal 19.2. We recommend instead that both the relevant factors for determining what reasonable steps may be required and the specific types of measures that may amount to

	reasonable steps be maintained in the APP Guidelines, where they are more easily kept current. In support of this approach, we repeat our recommendation from section 3, that APP entities be required to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

We support proposal 19.1 as it would remove any possible doubt that the current accepted interpretation of APP 11 as including both technical and organisational measures is correct.

We recommend that the review should avoid, wherever possible, enshrining too much detail about relevant factors and particular measures relating to security in the Act, particularly where such detail may constrain the flexible application of the reasonableness standard, or fall out of date over time.

In our view, the best approach to providing greater clarity about security requirements is through detailed guidance from the OAIC, or from other agencies or standards bodies, and adopted and incorporated into the APP Guidelines by the OAIC.A primary reason for this is to ensure the ability to keep this information up to date over time in a fast moving environment. The OAIC is well placed (provided it is adequately funded) to work between industry, security professionals, standards bodies, the Australian Signals Directorate and any other relevant stakeholders to provide guidance on baseline and best practice security measures in various contexts (from small business through to large enterprise). OAIC guidance already includes the range of factors relevant to determining what security controls are reasonable but could be expanded to provide more explicit guidance and expectations for organisations in varying contexts.

In support of this approach, we repeat our recommendation from section 3 that APP entities be required to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

Strengthening destruction requirements

Proposal 19.3	*Amend APP 11.2 to require APP entities to take all reasonable steps to destroy the information or ensure that the information is anonymised where the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs.*
elevenM position	We support proposal 19.3.

Deloitte's observation it its submission, that 'despite legislative requirements and recommended best practice to the contrary, many Australian organisations currently retain

personal information for longer than is reasonably necessary for a particular function or activity',[60] is consistent with our insights into various operating environments. Though some do perform well, many Australian organisations have poor retention and destruction standards.

We recognise that data minimisation through destruction or de-identification/anonymisation of personal information is an important control to mitigate security risks: the less data being held, the lower the impact of any potential breach. While we support the adoption of a higher standard for APP 11.2, we note that changing the standard alone is unlikely to have a significant impact on compliance or on the maturity of APP entities' retention and destruction standards. The issue of poor compliance with APP 11.2 will only be addressed by resourcing and empowering the OAIC to effectively police the requirement (see section 24 below).

20. Organisational accountability

Determining and recording secondary purposes in advance

Proposal 20.1	*Introduce further organisational accountability requirements into the Privacy Act, targeting measures to where there is the greatest privacy risk:* • *Amend APP 6 to expressly require APP entities to determine, at or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.*
elevenM position	We do not support proposal 20.1. Instead, the obligation to determine and record known primary and secondary purposes should apply at collection. Under this approach organisations would still have the flexibility to determine new purposes over time, which they could add to their record.

Proposal 20.1 aims to increase organisational accountability by introducing a record-keeping obligation analogous to (but weaker than) the GDPR obligation to maintain records of processing activities. We support this objective but consider that the time of the first secondary use is not the right trigger for this obligation to crystalise.

[60] Deloitte, Submission to the Attorney-General's Department, *Privacy Act Review – Issues Paper* (27 November 2020) 132.

Organisations are already required to consider the range of purposes for which personal information may be used or disclosed prior to collection in order to comply with APP 3 and as part of a privacy by design approach. It would be natural to require that purposes be determined and recorded at that point.

Additionally, many common secondary uses, such as audit, reporting or fraud prevention may be continuous or immediate upon the establishment of a new process for collection. As a result, we anticipate that in practice the proposed new APP 6 obligation would always have to be considered and would often be triggered upon the collection being established. Linking the obligation to APP 3 and applying it at the point of collection (or as soon as practicable afterwards) would be simpler, more intuitive, and better aligned with established privacy by design approaches.

Additional organisational accountability measures

elevenM position	We support the OAIC's recommendation for additional organisational accountability measures to be incorporated into APP 1 to expressly require APP entities to: • implement a risk-based privacy management program, • implement a 'privacy by design' approach, • appoint a privacy officer or privacy officers, and • provide the Commissioner, on request, with evidence of the steps taken to ensure compliance with the APPs and any registered APP code. In addition, we recommend that APP entities be required to maintain a record of their personal information holdings.

Several times throughout this submission we have put forward the argument that organisations, not individuals, should be primarily responsible for preventing privacy harms. In our view, one of the principal goals of this Review should be to drive a regulatory framework centred on organisational accountability and harm prevention, rather than on individual self-management. As we have argued above, this shift aligns with consumer expectations, and with the regulatory approach adopted in similar contexts — such as product safety, consumer protection, occupational health and safety, and the regulation of financial services — where it is recognised that 'buyer beware' is neither effective nor economically efficient.

The Discussion Paper lists several proposals that would support greater organisational accountability. We agree that proposal 11.1 (restricted practices) would contribute significantly towards this goal but would do so largely on a per-project basis.

Other proposals focused on increasing transparency (for example, with respect to overseas disclosure, use of third parties for online marketing and ADM) may require organisations to institute internal governance processes in order to comply but ultimately perpetuate the

privacy self-management model and do little to shift responsibility for preventing harm back onto the APP entity.

None of the proposals in the Discussion Paper appear directed towards requiring organisations to develop and maintain a wholistic, risk-based privacy management program.

To this end, we support the OAIC's submission that the Act should build on the existing APP 1.2 requirement that APP entities take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs, and include explicit requirements to:

- implement a risk-based privacy management program,
- implement a 'privacy by design' approach,
- appoint a privacy officer or privacy officers, and
- provide the Commissioner, on request, with evidence of the steps taken to ensure compliance with the APPs and any registered APP code.

In addition to this, we would further add a baseline requirement that APP entities maintain a record of their personal information holdings.

Adding these explicit requirements to the act would help clarify entities' obligations under APP 1.2 and set the expectation that APP entities of all sizes take proactive steps to manage privacy. The proposed additional requirements scale effectively with the size and complexity of an organisation and would require little more from a smaller APP entity than the appointment of a privacy officer and a means of assessing privacy risk in the business.

Additionally, these requirements are already mandated for agencies in the *Privacy (Australian Government Agencies – Governance) APP Code 2017*. Expanding these requirements to the public sector would set a consistent standard across all APP entities.

21. Controllers and processors of personal information

elevenM position	We recommend the Act be amended to introduce the concepts of data controllers and data processors.

As the Discussion Paper notes, the controller-processor distinction is common to many international jurisdictions and is also a feature of the Asia-Pacific Economic Cooperation (**APEC**) Cross-Border Privacy Rules (**CBPR**) system. This is for good reason. The distinction allows for a clearer and more accurate mapping of privacy obligations onto typical business relationships.

The controller-processor relationship is extremely common. Even small businesses commonly rely on multiple software-as-a-service or infrastructure-as-a-service providers to hold or process information, or to manage business processes. Larger APP entities typically maintain hundreds of controller-processor relationships.

The Act as currently drafted does not map neatly onto these relationships and relies heavily on interpretation and reasonableness standards to make privacy obligations fit. This adds complexity and makes compliance harder for non-experts.

A distinction between controllers and processors would help to clarify the application of the APPs by more clearly allocating responsibilities relating to notification, consent and security between contracting parties. It would also align the requirements of the Act with community expectations that the primary organisation they deal with retains ultimate accountability for their personal information, which it cannot pass off to a supplier/processor.

22. Overseas data flows

A mechanism to prescribe countries and certification schemes

Proposal 22.1	*Amend the Act to introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a).*
elevenM position	We strongly support proposal 22.1.

As well as providing companies with certainty about their obligations when disclosing personal information overseas, a central mechanism would be much more efficient and would reduce compliance costs by freeing APP entities from making the assessment themselves.

The OAIC would need to be adequately resourced to administer the mechanism, manage reciprocal arrangements with overseas regulators and assess and monitor safeguards in prescribed countries and schemes.

Introduce standard contractual clauses

Proposal 22.2	*SCCs for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information.*
elevenM position	We strongly support proposal 22.2.

Standard Contractual Clauses (**SCCs**) are a well-established, widely used and effective mechanism for aligning data protection standards across jurisdictions. Introducing SCCs

would significantly reduce the regulatory burden on APP entities (particularly small businesses) transferring data across borders.

Using and managing obligations under SCCs can require some sophistication, both as a sender and recipient of personal information. For organisations dealing with SCCs for the first time, some uplift around privacy management is often required. Becoming familiar with managing an Australian regime of SCCs would also better prepare Australian entities to implement SCCs when asked to as a supplier to entities in overseas jurisdictions which already have SCCs.

The OAIC would need to be adequately resourced to develop and keep up to date standard contractual clauses.

Remove the exception to accountability where consent is obtained

Proposal 22.3	*Remove the informed consent exception in APP 8.2(b).*
elevenM position	We support proposal 22.3.

As a general rule, it is not appropriate to permit organisations to rely on consent as a basis for avoiding obligations under the Act. As we have argued above, particularly in section 10, organisations are better placed to understand and manage potential harms than their customers.

Strengthen transparency requirements

Proposal 22.4	*Strengthen the transparency requirements in relation to potential overseas disclosures to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in entity's up-to-date APP privacy policy required to be kept under APP 1.3.*
elevenM position	We support proposal 22.4.

The current transparency requirements with respect to overseas disclosures provide little value to individuals. Privacy policies present a list of countries without any indication of the volume and type of personal information disclosed, or of any controls that may be in place to prevent its misuse. As such, it is impossible even for an expert reader to make a meaningful assessment of any risk that might be associated with the overseas disclosures.

Proposal 22.4 would provide more information by requiring a statement of the personal information that may be disclosed overseas. This would allow readers better understand how

their personal information is moving and better understand any risks. However, we recognise that this may

Introduce a definition of 'disclosure'

Proposal 22.5	*Introduce a definition of 'disclosure' that is consistent with the current definition in the APP Guidelines.*
elevenM position	We support proposal 22.5.

Defining the concepts of 'use' and 'disclosure' in line with the OAIC's definitions in the APP guidelines would provide clarity and stability in the interpretation for such important terms. This is important given the absence of judicial consideration of those terms within the context of the Privacy Act and reduce the risk that a determination by a court may alter the established operation of the Act.

Amend APP 8.1 to clarify the meaning of 'reasonable steps'

Proposal 22.6	*Amend the Act to clarify what circumstances are relevant to determining what are 'reasonable steps' for the purpose of APP 8.1.*
elevenM position	We do not support proposal 22.6. We recommend instead that detail clarifying what reasonable steps may be required and the specific types of measures that may amount to reasonable steps be maintained in the APP Guidelines, where they are more easily kept up to date. In support of this approach, we repeat our recommendation from section 3 that APP entities be required to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

As we have argued in relation to proposal 19.2 above, we recommend that the review should avoid, wherever possible, enshrining too much detail in the Act, particularly where such detail may constrain the flexible application of the reasonableness standard, or fall out of date over time.

In our view, the best approach to providing greater clarity on the interpretation of the reasonableness standard is through detailed guidance from the OAIC.

As the Discussion Paper notes, OAIC guidance already includes the range of factors relevant to determining what steps may be reasonable to ensure an overseas recipient does

not breach the APPs. In order to address concerns raised by submitters, OAIC guidance could be expanded to provide more explicit guidance and expectations for organisations in varying contexts.

In support of this approach, we repeat our recommendation from section 3, that APP entities be required to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

23. Cross-border privacy rules and domestic certification

General data protection regulation (GDPR)

elevenM position	We recommend pursuing GDPR adequacy.

Achieving GDPR adequacy would have significant benefits for Australian businesses in the form of reduced compliance costs associated with negotiating contractual provisions and streamlined interactions with businesses trading in the EU.

We agree with the observation made in the Discussion Paper that the key barriers to adequacy remain the small business and employee records exemptions. We have argued above for the removal of these exemptions on grounds other than achieving adequacy. With their removal, adequacy may be achieved without significant amendment to the Act.

The Cross-border privacy rules (CBPR) system

Proposal 23.1	*Continue to progress implementation of the CBPR system.*
elevenM position	We support proposal 23.1.

The CBPR system would present an alternative mechanism to facilitate cross-border data flows for Australian businesses. To the extent that the CBPR promises safer and more streamlined data sharing arrangements between participating economies and businesses, we are supportive of its implementation.

However, usability and workability of the system is as yet unproved in the Australian context, and the OAIC has limited resources and many competing priorities. So far as the OAIC is involved in progressing implementation of the CBPR system, it must be provided with additional funds to do so.

Domestic privacy certification

Proposal 23.2	*Introduce a voluntary domestic privacy certification scheme that is based on, and works alongside CBPR.*
elevenM position	We support proposal 23.2.

A domestic privacy certification scheme could help build digital trust by providing businesses with a means of demonstrating compliance with Australian privacy laws and providing individuals with an easy to consume indicator of the privacy posture of an APP entity.

It could also lower compliance costs for some businesses by providing a mechanism for assurance over the privacy practices of suppliers. If adopted, we see supplier assurance to be a key use case. Any scheme should be designed with this in mind, and to the extent possible, should be scalable and accessible to smaller businesses.

As the Discussion Paper notes, there is a range of international and domestic certification regimes currently in operation. We would support the introduction of a domestic privacy certification scheme that draws from best practice across other jurisdictions, as outlined in the Discussion Paper.

24. Enforcement

Civil penalty provisions

Proposal 24.1	*Create tiers of civil penalty provisions to give the OAIC more options so they can better target regulatory responses, including:* • *A new mid-tier civil penalty provision for any interference with privacy, with a lesser maximum penalty than for a serious and repeated interference with privacy.* • *A series of new low-level and clearly defined breaches of certain APPs with an attached infringement notice regime.*
elevenM position	We support proposal 24.1, noting that smaller fines are likely to be most effective when issued publicly.

The current civil penalty under section 13G for serious and repeated interferences with privacy does not sufficiently deter poor privacy practice as it is so rarely applied. We expect that infringement notices and mid-tier civil penalties that are more regularly applied may help to drive better corporate behaviours, particularly for small and medium enterprises.

However, there is a risk, particularly for larger organisations, that low value penalties, even if more regularly applied, will not be substantial enough to make it onto an organisation's risk matrix or may merely be considered a cost of doing business. To counter this, we suggest maintaining a discretion for the OAIC to publish the name of entities receiving these penalties, as reputational impact will drive compliant behaviours where infringements may not.

We recognise the work done by the Commissioner following the introduction of the Notifiable Data Breach scheme to encourage proactive notification of data breaches. Thought should be given to how proactive notifications can be quarantined to avoid unintentionally discouraging entities from notifying out of fear of penalty and/or publication.

The 'serious' or 'repeated' civil penalty

Proposal 24.2	*Clarify what is a 'serious' or 'repeated' interference with privacy.*
elevenM position	We support proposal 24.2.

Clarification of 'serious' or 'repeated' interferences with privacy would assist entities in identifying activities in their environments that may lead to serious or repeated interferences with privacy, and encourage additional resource allocation and focus to minimise such interferences. Additional clarification could also better inform consumers of the kinds of breaches the Commissioner considers 'serious'.

This proposal should seek to clarify whether an APP entity 'repeatedly does an act, or engages in a practice' when the same non-compliant process is applied multiple times or across a number of individuals. For example, if an organisation breaches APP 7 by failing to act on an opt-out request, does the interference with privacy become 'repeated' for the purposes of section 13G upon the second non-compliant message being sent to a given individual?

OAIC powers: assessments, investigation and inquiries

Proposal 24.3	*The powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 (Regulatory Powers Act) would apply to investigations of civil penalty provisions in addition to the IC's current investigation powers.*
Proposal 24.4	*Amend the Act to provide the IC the power to undertake public inquiries and reviews into specified matters*
elevenM position	We support proposals 24.3 and 24.4.

The powers proposed in 24.3 would assist the OAIC in accessing relevant information for an investigation when required, and result in more thorough and well-informed investigations.

Proposal 24.4 would support the OAIC in being a more proactive regulator, enabling public inquiries that can be used to better understand industry practices and educate the industry on whether particular acts or practices are consistent with the Act.

Investigations of this nature encourage entities to review their own processes and controls, and make proactive changes where required to improve organisational compliance. In our view, investigations of this nature could result in compliance uplift across the industry.

Determinations

Proposal 24.5	*Amend paragraph 52(1)(b)(ii) and 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined:* • *a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals.*
elevenM position	We support proposal 24.5.

Privacy harms commonly arise as small or potential impacts spread across groups of individuals. Understanding, quantifying and managing these harms is difficult, but it is clear that many harms do not materialise immediately. Lost or stolen personal information may remain available online or on the dark web indefinitely and may be aggregated with other data over time before it is exploited against the affected individual.

APP entities' obligations under APP 11.1 extend to taking steps to prevent and remediate foreseeable misuse of personal information. Similarly, when an organisation experiences a data breach, it is the clear community expectation that that organisation should bear the whole cost of that incident and protect those affected.

It is also an important policy objective to ensure that organisations internalise the full cost of data breaches and other privacy incidents, so that they are correctly incentivised to invest in preventing them.

For these reasons, it is important that the Commissioner be empowered to require APP entities to identify and mitigate reasonably foreseeable losses or damage.

Range of available Federal Court orders in a civil penalty proceeding

Proposal 24.6	*Give the Federal Court the power to make any order it sees fit after a section 13G civil penalty provision has been established.*
elevenM position	We support proposal 24.6.

Appropriate remedies following an interference with the privacy of an individual can vary significantly depending on the circumstances of the breach. Financial compensation is not always the best outcome for the complainant or the only necessary next step for the respondent. Allowing the Court to make orders it sees fit would recognise that the impact of a breach of privacy cannot always be resolved through financial means, and would provide the Court with flexibility to make appropriate orders to deal with all aspects of a matter, including to minimise further impacts to the complainant and/or other individuals, where compensation alone may not.

Fund the OAIC through an industry funding arrangement

Proposal 24.7	*Introduce an industry funding model similar to ASIC's incorporating two different levies:* • *A cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments, and* • *A statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment.*
elevenM position	We support proposal 24.7. Whatever funding model is adopted, adequate funding for the OAIC to perform its expanding functions and to exercise its full range of regulatory powers is critical to the success of the entire regulatory scheme.

As most submissions to the Review have observed, current funding for the OAIC is entirely inadequate. Though the OAIC has performed admirably with the limited resources available, budget limitations have meant limited support for business seeking to comply with their privacy obligations, poor experiences and long wait times for complainants, little deterrence for the few bad actors, and a lower general standard of compliance in the absence of meaningful enforcement.

Ultimately, a poorly funded regulator leads to a loss of trust and stagnation in the digital economy.

It seems to us that an industry funding model enshrined in legislation could contribute a more consistent and predictable annual funding source. However, we suggest that any industry funding be in addition to, rather than replace, any current or future Government funding. The OAIC is an important Australian Government agency that performs critical public service functions, and should be recognised as such through appropriate Budget allocation. This is particularly important noting the OAIC performs various functions, including enforcement and regulatory functions, which we do not consider industry should have to bear the full cost of.

An industry funding model, in addition to Government funding, could provide the Commissioner with a greater degree of independence and allow her to better plan and deliver a long-term regulatory strategy. We understand that models adopted by other regulators, including ASIC and the UK ICO have been successful, and we see no reason why an equivalent regime could not work for the OAIC.

Careful consideration will need to be given to the design of the levy. It will need to scale with the size of a business in order to ensure it does not disproportionately impact small businesses. A higher levy for organisations in certain high-risk industries, such as those who collect or trade in large amounts of personal data, may also be appropriate.

We warn against hypothecating levy revenue too specifically. The Commissioner should retain flexibility to spend her budget on those matters that she considers most pressing or of the greatest strategic importance. Inflexible requirements to spend a certain proportion of budget on specified activities is likely to lead to inefficiency and waste.

Annual reporting requirements

Proposal 24.8	*Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41.*
elevenM position	We support the OAIC publishing information about complaint handling to increase transparency.

We support the publication of complaint handling-related information such as the types of complaints, outcomes, which provisions complaints are being dismissed under etc. This information, like the OAIC Notifiable Data Breaches Reports, would provide both industry and individuals with greater information on trends and common outcomes, and be a tool for insights and guidance through examples.

While we support the inclusion of this information in the Commissioner's Annual Report, we consider these benefits could be realised without an amendment to the *Australian Information Commissioner Act 2010*. To enhance transparency, we suggest consideration be given to the development of a specific report, where these statistics are not hidden among other information. We consider a standalone report that is specific, consumer and industry-

focused, and similar in style and frequency to the Notifiable Data Breaches report, would provide greater value.

Regulatory model

Proposal 24.9	*Alternative regulatory models* • ***Option 1*** *- Encourage greater recognition and use of EDRs. APP entities that handle personal information could be required to participate in an EDR scheme. APP entities that are not part of a recognised EDR scheme could be required to pay a fee for service to the OAIC as the default complaint handling provider if a complaint is made against them.* • ***Option 2*** *- Create a Federal Privacy Ombudsman that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR schemes.* • ***Option 3*** *- Establish a Deputy Information Commissioner – Enforcement within the OAIC.*
elevenM position	We support the creation of a Federal Privacy Ombudsman, but have reservations about increased reliance on industry focused, non-privacy-specialist EDR schemes.

We support the creation of a Federal Privacy Ombudsman to focus on the efficient and effective conciliation of privacy complaints, allowing the OAIC to re-allocate resources to take a more strategic, proactive and enforcement-focused regulatory approach.

Option 2 couples the creation of a Federal Privacy Ombudsman with greater use of existing EDR schemes. We understand that EDR schemes can be particularly effective in high volume complaint areas such as telecommunications, energy and water. However, in our experience, it is not uncommon for high-volume, specialised, industry focused EDR schemes to fail to properly understand or give appropriate weight to privacy concerns that do not fall neatly within established case categories or resolution processes. Consistent management of privacy complaints is an important element in improving consumer understanding, maintaining consumer trust, and educating industry. Existing EDRs have deep subject matter knowledge on their relevant industry, and whilst industry-specific knowledge may support some privacy matters, a deep understanding of privacy is the core component of effective privacy complaint management. Even with targeted training, we have concerns about some EDRs managing complex privacy complaints consistently and with sufficient subject matter experience to provide the same outcome and experience as a Federal Privacy Ombudsman.

In line with our comments above about the significant funding issues the OAIC currently experiences, we stress that any new office or agency established to deal with privacy complaints must in no way detract from the very limited resources available to the OAIC.

Funding for any new agency should be considered separately, rather than as an offset of existing privacy budget allocations.

25. A direct right of action

Proposal 25.1	*Create a direct right of action with the following design elements:* • *The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.* • *The action would be heard by the Federal Court or the Federal Circuit Court.* • *The claimant would first need to make a complaint to the OAIC (or FPO)1 and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman.* • *The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application.* • *The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.*
elevenM position	We strongly support the creation of a direct right of action for individuals to litigate their privacy complaints. While we support elements of the proposed model, we are concerned that some aspects – including the proposed gatekeeper role for the OAIC and legal forum for complaints – may result in inefficiencies and access to justice issues for individual claimants.

Currently, individuals have limited legal recourse against entities that breach personal information protection obligations under the Privacy Act. Actions available to an affected individual are generally limited to:

1. making a complaint to the OAIC about an act or practice that may interfere with their privacy,
2. applying for enforcement of an OAIC determination, or
3. seeking a court injunction for conduct that breaches the Privacy Act.

We strongly support measures to enable Australians to litigate their data subject rights and to seek redress, via the legal system, for harms they suffer due to interferences with those rights. As the risks posed by the misuse or abuse of personal information continue to grow in the digital age, and the impacts of privacy breaches result in ever-increasing harms to

individuals, it is imperative that Australians be given recourse to effective remediation for the misuse or abuse of their personal information.

We agree that any model for a direct right of action should strive to balance claimants' interests, including in relation to accessibility and efficient resolution, with the need to manage court resources and protect businesses from involvement in frivolous or vexatious litigation. While there are elements of the proposed model we support, including the right extending to class actions, the ability to bypass an elective conciliation process, the role of OAIC as *amicus curiae* in proceedings, and broad court discretion in determining appropriate remedies, we consider some elements of the proposed model may limit access to a just and efficient resolution for many claimants.

Legal forum

Under the proposed model, the legal forum for pursuing a right of action would be the FCA or Federal Circuit Court (**FCC**). As the Discussion Paper outlines, the proposed model mirrors, to an extent, the current model for complaints under existing Federal anti-discrimination legislation. We note the various criticisms that have been made about that model over the years.[61] Primarily, stakeholders have expressed concerns that the time and costs of litigating claims in those forums; the formality of proceedings, including in relation to onerous evidentiary requirements; and the risks associated with adverse costs orders for unsuccessful claims, act as barriers to the pursuit of meritorious discrimination complaints.[62]

While we support the right of action extending to class actions, for which the FCA or FCC may be appropriate forums, joining a class action should not be a substitute for a claimant's ability to independently bring an action against an offending entity. For many individual complainants, FCA or FCC proceedings are not viable options. We note the Discussion Paper's statement that the intention is to create 'a greater body of jurisprudence to be developed by the court, which would assist the public and APP entities to better understand their rights and obligations',[63] however we consider that this aim is unlikely to be realised if claimants do not have practical access to resolution in those forums.

We note the Discussion Paper's suggestion that a 'small claims procedure' could be 'created for privacy matters in the FCC to reduce the burden on individuals seeking to exercise the

---

[61] Legal Aid NSW, Submission to the Senate Legal and Constitutional Affairs Committee Inquiry, *Draft Human Rights and Anti-Discrimination Bill 2012* (January 2013); Attorney-General's Department, *Consolidation of Commonwealth Anti-Discrimination Laws – Discussion Paper* (September 2011); Productivity Commission, *Review of the Disability Discrimination Act 1992* (Report no 30, 30 April 2004), vol 1.

[62] Legal Aid NSW, Submission to the Senate Legal and Constitutional Affairs Committee Inquiry, *Draft Human Rights and Anti-Discrimination Bill 2012* (January 2013).

[63] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) 187.

direct right of action – both in terms of costs, and the burden of complying with the procedural rules in the Federal Court'.[64] We would welcome further information about any such model, including in relation to filing fees, evidentiary requirements and jurisdictional limits. If such a procedure is not adopted, then we suggest serious consideration be given to imbuing lower level courts or tribunals with jurisdiction to hear privacy complaints.

Gatekeeper model

The proposed model would require a complainant to make a complaint to the OAIC, and to await the OAIC's assessment about conciliation before seeking leave from the relevant court to make an application. Following a decision from the OAIC, litigation could be pursued instead of conciliation, after conciliation has proven unsuccessful, where the OAIC has determined the matter not suitable for conciliation, or where the OAIC has terminated the matter.

No timeframe is stipulated for the making of the OAIC assessment. The Discussion Paper is also silent on whether the outcome of an OAIC assessment would have any bearing on a claimant's ability to pursue the matter (for example, it is unclear what the consequences for the claimant would be if the OAIC considers the claim to be vexatious or unmeritorious).

We query the necessity of this 'gatekeeper' role for the OAIC at all, particularly noting the proposed model would not require a claimant to pursue OAIC conciliation before commencing formal litigation (which we consider to be appropriate). As a claimant would be unable to pursue their right of action unless and until the OAIC makes a decision about conciliation, this step may result in unnecessary costs, delays and duplication of process.[65]

We consider that various other elements of the proposed model would already protect against some of the risks that are intended to be addressed through OAIC intervention in the process. We suggest that if the purpose of the gatekeeper role is to:

1. limit the risks of overburdening the legal system and ensuring that vexatious or frivolous claims do not proceed, then the requirement to seek leave to appear, in addition to the risks of costs orders for unsuccessful claims, would be sufficient to address such issues,
2. ensure the OAIC has oversight of complaints for tracking, monitoring or other purposes, then complainants could be required to notify the OAIC once leave is sought and / or an application has been made, or
3. encourage claimants to pursue less adversarial forms of dispute resolution, then we note that courts can, and as a matter of course do (where appropriate), refer proceedings to ADR.

---

[64] Attorney-General's Department, (n 12) 187.

[65] Australian Competition and Consumer Commission (n 65) 18.

We therefore suggest the requirement for a claimant to lodge a complaint with the OAIC in the first instance be removed. Removing this prerequisite would not preclude the OAIC from issuing guidance or encouraging claimants to lodge a complaint with it and attempt to conciliate via that channel.

If the gatekeeper model is retained, however, then at a minimum, we suggest a time limit be inserted for the making of the OAIC's assessment decision (for example, 30 days), with a failure to make a decision in the prescribed timeframe enlivening the right to commence formal proceedings.

Additional considerations

We suggest the following additional issues be considered in developing a model for a direct right of action:

1. **Limitation periods**: the Discussion Paper is silent on any limitation periods that may apply to the lodging of a claim in court. Currently, the Privacy Act requires a complainant to make a complaint to the OAIC within 12 months of becoming aware of the relevant act or practice. The nature of privacy breaches often means that a claimant might not be aware of a breach for months, if not years, after it occurs. The true consequences of such a breach, or the level of harm suffered, may take even longer to manifest or fully comprehend. We suggest that if any limitation periods are included, that they acknowledge the unique challenges posed by privacy breaches and adopt an appropriately inclusive formulation. Any limitation period should also be formulated so as not to penalise a claimant whose limitation period expires before lodging a claim in court but after making a complaint to the OAIC. We also recommend inclusion of a discretionary power for the court to extend any prescribed limitation period.
2. **Binding determinations powers for the OAIC**: to complement a direct right of action, we suggest consideration be given to empowering the OAIC to make binding determinations. We consider such a power would act as an incentive for claimants to pursue the OAIC conciliation process and provide greater confidence in appropriate resolution through that process. Removing the requirement for a claimant or the OAIC (as the case may be) to seek a court order for the enforcement of a determination could also serve to counterbalance any increase in litigation that may result from the creation of a direct right of action. We suggest such binding determinations be reviewable by whichever legal forum is ultimately imbued with jurisdiction to hear privacy complaints.

26. A statutory tort of privacy

Proposal 26.1	***Option 1:*** *Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report*
Proposal 26.2	***Option 2:*** *Introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts.*
Proposal 26.3	***Option 3:*** *Do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person.*
Proposal 26.4	***Option 4:*** *In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.*
elevenM position	We support the availability of a tort for serious invasions of privacy (and have therefore not commented on options 3 or 4). We support implementation of option 1. We do not support option 2.

We consider there is a need for a tort for serious invasions of privacy. For the reasons articulated in the Discussion Paper, we consider such a tort would be an appropriate addition to the suite of actions available (or that may become available) to individuals to enforce their privacy rights.

We agree with the position the ACCC articulated in the final report of its *Digital Platforms Inquiry*, that a privacy tort would complement a direct right of action and 'address existing gaps in the privacy framework and increase the deterrence effect of Australian privacy laws against harmful data practices that seriously invade Australians' privacy'.[66] Unlike a direct right of action, which would operate within the present constraints of the Privacy Act framework, applying only to breaches of personal information protections by regulated APP entities, a tort for serious invasions of privacy would recognise privacy as a standalone right and provide legal recourse for serious invasions of that right.

We agree with stakeholders that the formulation of any such tort will need to be carefully considered and appropriately formulated. We note, however, that the ALRC was referred the

[66] Ibid. 493.

task of designing such a tort under the Terms of Reference for its inquiry into *Serious Invasions of Privacy in the Digital Era.* Over the course of 12 months, the ALRC focused specifically on considering the implications of, and balancing the competing interests relevant to, enactment of a tort for serious invasions of privacy. For the better part of the last decade, government-commissioned reviews and inquiries, some of which have included their own stakeholder consultation processes, have recommended the adoption of the ALRC's model.

We support option 1 and suggest a tort for serious invasions of privacy be based on the ALRC's model, with any necessary modifications made (for example, we suggest it may be worth considering whether an additional fault element of negligence is appropriate). In our view, the ALRC's model, which would include a seriousness threshold, require consideration of countervailing interests and insert a broad range of defences, would appropriately balance individual privacy rights with other fundamental interests, including freedom of expression and freedom of the media to report on matters of public interest.

We do not support the introduction of a minimalist statutory tort as outlined in option 2. We consider the absence of specificity would likely result in years (if not decades) of uncertainty, as well as expensive legal action to determine the limits of such a tort. Relying on the ALRC's considered model would provide greater clarity and certainty.

Noting our support for the development of a tort for serious invasions of privacy, we have not commented on options 3 or 4.

Contributors

Jordan Wilson-Otto – Principal · LinkedIn: Jordan Wilson-Otto

Jordan is a privacy specialist with experience in regulatory investigations, policy development, information security and open data. Jordan has conducted high profile regulatory investigations for both the State and Federal privacy regulators. He was Assistant Commissioner for Operational Privacy and Assurance at the Office of the Victorian Information Commissioner, where he established and led the investigations and assurance function. Jordan has also held leadership roles at GovHack and the Victorian Society for Computers and the Law. He has completed a Master's thesis on how open data approaches could aid transparency and public trust in the justice system.

Melanie Marks – Principal · LinkedIn: Melanie Marks

Former President of IAPP ANZ, Melanie has also served on the advisory board of Information Governance ANZ and the Privacy Advisory Board of Hello Sunday Morning. She is an Expert Advisor to LexisNexis on privacy and data protection. Melanie has established and run privacy governance programs for CBA and the National eHealth Transition Authority. In her current capacity as privacy practice lead at elevenM, Melanie works with Australia's most prominent brands to manage privacy, data governance and other risks of the digital age. In this role, Melanie has worked extensively with listed companies, SMEs, Commonwealth and jurisdictional agencies and privacy regulators to solve privacy problems and drive change and innovation.

Adi Prigan – Senior Consultant

Adi is a privacy consultant at elevenM with a background in policy, legislation and law reform advocacy. Adi began her career in legal policy roles within the Commonwealth Government, where she delivered policy and legislative reform initiatives in the areas of criminal and discrimination law. Most recently, in her role as a policy lawyer with the Law Society of New South Wales, Adi managed the Privacy and Data Law Committee, where she engaged in law reform initiatives and advocacy on behalf of the NSW legal profession in the area of privacy and data law.

Emma Mackenzie — Senior Consultant · LinkedIn: Emma Mackenzie

Emma is a privacy professional with extensive experience supporting businesses in achieving data-driven goals whilst building consumer trust. Prior to joining elevenM, Emma led the privacy program at Australia Post, where she partnered with the business to provide pragmatic and actionable solutions and develop ethical data handling practices. Emma has hands on experience navigating the operational challenges facing privacy compliance in complex corporate environments. Emma holds a Bachelor of Laws and Bachelor of Commerce, is CIPM accredited by the International Association of Privacy Professionals (IAPP) and is the current chair of the IAPP Melbourne KnowledgeNet Chapter.