Avant Mutual Group Limited
ABN 58 123 154 898

Registered office
Level 6, Darling Park 3
201 Sussex Street, Sydney NSW 2000

Postal address
PO Box 746 Queen Victoria Building
Sydney NSW 1230

DX 11583 Sydney Downtown

avant.org.au

Telephone 02 9260 9000 **Fax** 02 9261 2921
Freecall 1800 128 268 **Freefax** 1800 228 268

10 January 2022

Privacy Act Review
Attorney-General's Department
Robert Garran Offices
3-5 National Circuit
BARTON ACT 2600

By email PrivacyActReview@ag.gov.au

Privacy Act Review

Thank you for the opportunity to comment on the Privacy Act Review Discussion Paper.

Avant is the largest medical defence organisation in Australia. We provide professional indemnity insurance and legal advice and assistance to more than 78,000 medical practitioners and students around Australia.

Our submission is attached.

We have appreciated meeting directly with the Review team and we would welcome the opportunity to continue to engage with the Attorney-General's Department to elaborate on any of the issues raised as the Review progresses.

Yours sincerely

Georgie Haysom
General Manager, Advocacy Education and Research
Direct: 0466 779 105
Email: georgie.haysom@avant.org.au

Avant submission on the Privacy Act Review Discussion Paper

Avant is the largest mutual medical defence organisation in Australia. We provide professional indemnity insurance and legal advice, assistance and education to more than 78,000 medical practitioners and students around Australia.

We assist members in civil litigation, professional conduct matters, coronial matters and a range of other matters including employment disputes and privacy-related complaints. We have a medico-legal advisory service that provides support and advice to members and insured medical practices when they encounter medico-legal issues.

We also provide medico-legal education to our members with a view to improving patient care and reducing medico-legal risk. Privacy is a key area for medico-legal advice and education.

We have provided comments on several, but not all, of the proposals and questions outlined in the Discussion Paper. We have greyed out the proposals that we have not commented on. In some cases, we have referred to and rely upon the contents of our submission to the Issues Paper without repeating them.

As a preliminary comment, we note that the Discussion Paper does not review either the permitted general situations or permitted health situations at all. In our view, these generally work well but there are some nuances with the wording of some of the provisions that could be clarified to strengthen the protections under the Act. For example, provision of a patient's medical records to a complaints body may not squarely fit within the exemptions under the Act.

General comments

1. We agree that the requirement to balance the protection of privacy with the interests of business can be difficult in the context of businesses whose core activity is acquiring and dealing in personal information. Dealing with personal information is integral to the delivery of both healthcare and insurance. Privacy laws should not be an impediment to either.

2. Overall privacy law is complex and technical. Understanding the complexities and ensuring compliance can therefore be difficult.

3. We agree with risk-based, "right touch" regulation that adopts the compliance pyramid approach to regulation.

4. We generally do not favour legislative change that increases the availability of causes of action or increases the scope of liability of Avant and/or members. We believe that

current remedies are appropriate. If there is a legitimate interest to be protected, it is important to balance the protection of that interest against the additional burdens on and liability of businesses. The scope of liability should be limited to ensure this.

5. We favour national consistency – inconsistency between the legislative requirements in different states, and between state/territory legislation and Commonwealth legislation is confusing and can lead to compliance difficulties.

6. A harmonised privacy regime would go a long way to reducing administrative and compliance burden on businesses and would enhance privacy protection for consumers.

Complete list of proposals

Part 1: Scope and application of the Act

1. Objects of the Act

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*.

2. Definition of personal information

2.1 Change the word 'about' in the definition of personal information to 'relates to'.

2.2 Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information.

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.

We support this proposal. It is consistent with the advice we give to our members and our approach at Avant as to whether information is identifiable.

2.4 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

From the perspective of medical practitioners and practices, Avant does not support the inclusion of inferred information in the definition of collection.

As noted in our submission to the Issues Paper, healthcare providers routinely collect and infer personal and sensitive information from a patient's presentation, history, and results. Imposing additional protections for inferred information would be impractical and unworkable in the healthcare context.

If, however, inferred information were to be included, healthcare entities should be exempt.

2.5 Require personal information to be anonymous before it is no longer protected by the Act.

We do not support this proposal. Requiring anonymisation before information is no longer protected by the Act would be unworkable in the context of healthcare, and in our corporate context. Anonymisation would remove so much of the relevant information that anything that remains would be meaningless. It could be a significant barrier to learning, education and training both in the healthcare context, and for Avant in its role in providing education to members on quality, safety and professionalism in medical practice and reducing medico-legal risk, based on the membership's claims experience.

2.6 Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments.

Questions

- What would be the benefits and risks of amending the definition of sensitive information, or expanding it to include other types of personal information?
- What further information or guidance would assist APP entities when classifying biometric information, biometric templates or genetic information as 'sensitive information'?

Expanding the definition of sensitive information to include financial information may cause unintended consequences for APP entities. For example, APP entities may have to obtain specific consents from consumers with respect to all goods viewed online or purchased (should these entities wish to retain this information), which could cause further consent fatigue in consumers.

The Discussion Paper refers to the uncertainties noted in the Australian Department of Health's submission to the Issues Paper about how the definition of health information applies to genomic information. The definition of health information in section 6FA(d) of the Act specifically refers to genetic information and, in our view, other subsections in section 6FA could also encompass genetic information.

We also note that in the slides for the stakeholder meeting for medical and research stakeholders, there is reference to genetic information that is not health information. From a medical perspective, genetic or genomic information will generally always be health information about the person to whom it relates and potentially their genetic relatives.

Defining “reasonably identifiable” as proposed in 2.3 and changing “relates to” to “about” as proposed in 2.1 would help to clarify any uncertainty in this regard.

The distinction raised in the Discussion Paper seems to be between genetic information used for the purposes of healthcare and genetic information used for other purposes (such as ancestry), rather than a distinction in the nature of the information itself. Therefore, we are not sure what additional guidance would be helpful to APP entities in this regard.

In our submission to the Issues Paper we referred to a significant consequence of the more stringent requirements that apply to the collection, use and disclosure of sensitive information. This is the impact that these requirements have on the transfer of health records between practices when either a medical practice is being sold or an individual practitioner is moving to a new practice. We refer to the discussion on this issue in our submission to the Issues Paper and do not restate it here.

3. Flexibility of the APPs

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

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.

3.3 Amend Part VIA of the Act to allow Emergency Declarations to be more targeted by prescribing their application in relation to:

- entities, or classes of entity
- classes of personal information, and
- acts and practices, or types of acts and practices.

3.4 Amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force.

5. Employee records exemption

Questions

- To what extent are employers collecting personal information about employees beyond what is reasonably necessary for their functions or activities?
- Are employers using or disclosing personal information about employees in ways that meet community expectations?
- How might the employee records exemption be modified to address the impact of the Full Bench of the Fair Work Commission’s decision in *Lee*?

- How might the employee records exemption be modified to better protect those records while retaining the flexibility employers need to administer the employment relationship?
- To what extent would the fair and reasonable test for the collection, use and disclosure of personal information proposed in Chapter 10 be suitable for the employment context?
- To what extent would the current exceptions in APPs 12 and 13 address concerns about the need for employers to conduct investigations and manage employee performance if the exemption were modified?
- What would be the benefits and costs associated with requiring employers to take reasonable steps to prevent employees' personal information from misuse, interference or loss?
- What challenges or barriers would there be to requiring employers to comply with the NDB scheme in relation to eligible data breaches involving all employee records?
- What would be the benefits and limitations of providing enhanced protections for employees' privacy in workplace relations laws?

In our experience, most employers are not collecting information beyond what is reasonably necessary, and most employers are using and disclosing personal information in line with community expectations.

In the last two years, COVID-19 issues have become relevant, with employers collecting employees' health information such as information about temperature, vaccination status, rapid antigen test results, PCR test results, booster information etc. In most cases, it is reasonably necessary for employers to collect this information to comply with work health and safety obligations and public health directions. However, many employees would disagree and find this an invasion of their privacy. The current workplace law deals with this by considering whether the direction to provide information is a "reasonable and lawful direction".

In our experience, most employers are aware of the need to keep employee information, particularly health information, private and confidential, despite the fact that this is not required under the *Privacy Act*.

The rationale for excluding employee records from the *Privacy Act* when it was amended in 2000 (as noted in the second reading speech and explanatory memorandum) was that this would be better dealt with under workplace relations legislation. However, nothing has been done since that time to progress this. On balance, it may be better to have this dealt with in the Commonwealth *Privacy Act*. This would have the benefit of national consistency rather than having a state-based approach, and would be able to cover and therefore protect the privacy of individuals in all types of engagement arrangements with entities, not just those in an employer/employee relationship.

Part 2: Protections

8. Notice of collection of personal information

8.1 Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.

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.

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.

8.4 Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of 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*.

Questions

- Is Proposal 8.4 likely to result in any practical difference when compared with the current requirement on entities to take such steps (if any) as a reasonable in the circumstances to notify individuals?
- Is Proposal 8.4 sufficiently flexible to permit APP entities to provide no notice where it would be harmful or where an entity collects, uses or discloses personal information on behalf of another entity? If not, how might the requirement be framed so as to increase individuals' awareness of personal information handling while not subjecting individuals to notice fatigue?

We support this proposal.

Proposal 8.4 would provide reassurance to entities that they are not required to provide a collection notice in the circumstances listed. We agree with the comments in the Discussion Paper that some flexibility in the requirement to provide notice in these circumstances should be retained.

In response to the second question, we would suggest an additional exception be added to cover the situation where notice could harm the individual. Consistent with other sections in the Act and APPs, and (as noted in the Discussion Paper) the APP guidelines, this exception would apply where the entity reasonably believes that giving notice would pose a serious threat to the life, health or safety of any individual, or to public health or public safety.

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

9.1 Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

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.

Questions

- Are there additional circumstances where entities should be required to seek consent?
- Should entities 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?
- Does the proposed requirement for valid consent have any particular implications for different sectors, such as healthcare?

We agree that consent should be voluntary, current, specific and demonstrated through an unambiguous indication through clear action (ie, consent can be implied). While we agree with the notion of consent being informed, we have some concerns about the use of this terminology, as it could be confusing in the healthcare context.

In healthcare, "informed consent" is a well-established concept, and a term of art. While the High Court in *Rogers v Whitaker* (1992) 175 CLR 479 rejected the use of this term in the context of medical negligence law, it is a principle well known in healthcare. It encompasses the obligation on medical practitioners to inform patients of the benefits and material risks of a procedure or treatment, potential complications and outcomes, and alternatives, to allow the patient to make an informed decision about their healthcare. It is patient-centred, and the medical practitioner has an obligation to explore with the patient what is important and material to them and advise them accordingly.

While standardised consents could be helpful, as we say in our medico-legal education to doctors, consent is a process not a form. Informed consent is more than providing patients with written material and asking them to sign a form. Merely providing a standardised consent and asking the patient to accept it does not mean that consent is informed or that the patient has understood the information provided.

Healthcare providers are also familiar with the concept that consent should be renewed if circumstances change, but otherwise that consent is valid unless specifically withdrawn. It would be impractical to impose a standard time period for renewal of consent in a healthcare context, and would impose a significant administrative burden on healthcare practitioners and practices. These matters are likely appropriately addressed in the process of APP entities reviewing, and updating if necessary, their privacy policy.

10. Additional protections for collection, use and disclosure of personal information

10.1 A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

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
- 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.

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 procedures or seeking contractual warranties that the information was collected in accordance with APP 3.

Questions

- Does the proposed fair and reasonable test strike the right balance between the interests of individuals, APP entities and the public interest?
- Does the proposed formulation of the fair and reasonable test strike the right balance between flexibility and certainty?
- What impacts would the fair and reasonable test have on the business operations of entities?
- What factors would likely to be more challenging for entities to comply with?
- Should entities be required to satisfy each factor of the fair and reasonable test, or should the factors be interpretative considerations in determining whether something is, in its entirety, fair and reasonable?
- Should the fair and lawful collection requirement in APP 3.5 be subsumed by an overarching fair and reasonable requirement, or should a fair and reasonable requirement apply only to purposes for use and disclosure in APP 6?
- How should an overarching fair and reasonable test interact with the exceptions in APP 3.4, APP 6.2 (a) and 6.2(b)-(f)?

We support the proposal to include that collection, use and disclosure should be fair and reasonable. It would be preferable to have one test for collection, use and disclosure, rather than different tests for collection on the one hand and use and disclosure on the other.

The legislated factors would be helpful to guide entities about what this entails. However, we do not agree that entities should be required to meet all of the factors as this would be too prescriptive. Consistent with the principles-based approach under the *Privacy Act* generally, we believe that the factors be interpretative considerations in determining whether something is, in its entirety, fair and reasonable, rather than in the manner of a checklist.

We agree with the position taken in the Discussion Paper that the exceptions not be made subject to the fair and reasonable test. Many of the exceptions, including permitted general situations or where personal information handling is required or authorised by an Australian law or court order, are grounded in public interest considerations or are already qualified by 'reasonableness' requirements.

We are concerned about how proposal 10.3 would work in our corporate context. One of the main activities of Avant is to provide professional indemnity insurance to our medical practitioner members and their practices, to cover their liability to patients. Practitioners and practices are required under the *Insurance Contracts Act* to notify Avant of incidents that might give rise to a claim under the policy and, when a claim is made, to provide all relevant information in relation to the claim. This necessarily involves sensitive information about the patients involved, contained in hospital and medical records and reports. Often this information is collected from other healthcare providers as well as the patient and in some circumstances their family members or other individuals. It would be difficult for an organisation like Avant to satisfy itself that the information was originally collected from the individual.

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.

Question

- Would the proposed definition of a secondary purpose inadvertently restrict socially beneficial uses and disclosures of personal information, such as public interest research?

We are not certain how proposal 10.4 would work in practice. The Discussion Paper states that "the Act could be amended to provide additional legislative certainty as to what is a primary and secondary purpose, and encourage APP entities to classify a greater range of uses and disclosures as primary purposes." However 10.4 refers to "*the* primary purpose" (emphasis added) so it is not clear whether it is possible to have more than one primary purpose.

In relation the proposed definition of secondary purpose, we would be concerned if the consequences of this were to restrict socially beneficial uses and disclosures of personal information, and therefore we do not support the amendment on this ground.

11. Restricted and prohibited acts and practices

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
- 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.

Questions

- Would the introduction of specified restricted and prohibited practices be desirable?
- Should restricted practices trigger a requirement for APP entities to implement additional organisational accountability measures, or should individuals be provided with more opportunities to self-manage their privacy in relation to such practices?
- What acts and practices should be categorised as a restricted and prohibited practice, respectively?
- Should prohibited practices be legislated in the Act, or developed through Commissioner-issued guidelines interpreting what acts and practices do not satisfy the proposed fair and reasonable test, following appropriate public consultation?

It is difficult to comment on this proposal without detail about what would amount to "large scale".

In any event, we are concerned about the application of this proposal to the healthcare context, particularly the inclusion of "genetic data", and "any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual". The latter could arguably include all sorts of sensitive health information. The requirement to identify privacy risks and implement measures to mitigate those risks would be unworkable in the healthcare context that deals with information of this nature on a daily basis. It would not

be desirable to impose these requirements in this context, where many practices are small businesses, and would be an administrative and compliance burden.

If there are to be restricted and prohibited practices, these should not be legislated in the Act, but developed through Commissioner-issued guidelines interpreting what acts and practices do not satisfy the proposed fair and reasonable test, following appropriate public consultation. This would allow these practices to be considered on an industry-by-industry basis.

12. Pro-privacy default settings

12.1 Introduce pro-privacy defaults on a sectoral or other specified basis.

- **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.

13. Children and vulnerable individuals

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. The Review is also seeking feedback on the circumstances in which parent or guardian consent must be obtained:

- **Option 1** - Parent or guardian consent to be required before collecting, using or disclosing personal information of the child under the age of 16.
- **Option 2** - 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.

13.2 Require APP 5 notices to be clear, current and understandable, *in particular for any information addressed specifically to a child*.

Questions

- Are there other contexts aside from children's use of social media services that pose privacy risks to children, which would warrant similar privacy protections to those proposed by the OP code?
- Should consent of a parent or guardian be required for *all* collections of a child's personal information, or only for the existing situations where consent is required under the APPs?

- Should the proposed assumed age of capacity of 16 years in the OP Bill apply to all APP entities?
- Should APP entities also be permitted to assess capacity to consent on an individualised basis where appropriate, such as in the healthcare sector?
- Should the proposed assumed age of capacity determine when children should be able to exercise privacy requests independently of their parents, including access, correction, objection or erasure requests?

We strongly oppose the proposal to require consent to be provided by a parent or guardian where a child is under the age of 16. This would be unworkable in the healthcare context. This would be at odds with the well-established common law principle regarding capacity of children and young people to make healthcare decisions. Capacity is assessed on a case-by-case basis, based on the notion of *Gillick* competency and the "mature minor" principle.

The proposed reform could lead to the unworkable situation where a young person with capacity to make a healthcare decision could not give consent to the collection, use and disclosure of health information about that decision. That would diminish privacy protections for a young person rather than enhance them. An example is where a young person attends a consultation with a general practitioner for the contraceptive pill but does not wish to tell their parents. Requiring parental consent to collection of health information (which under the proposals needs to be specific and informed) could also have the unintended consequence of dissuading children and young persons from seeking care at all, reducing young persons' access to care.

We confirm the position in our submission to the Issues Paper that the current common law test should be adopted, certainly in the context of healthcare. APP entities in healthcare should be permitted to assess capacity to consent on an individualised basis, where appropriate, as they do currently in relation to healthcare decisions. This would apply to exercising other privacy requests including access, correction, objection or erasure.

In relation to vulnerable individuals, medical practitioners are accustomed to dealing with adults who lack decision-making capacity. In this context, we agree with the comment in the Discussion paper that on balance, where the Act does not currently prevent third parties acting with consent or with legal authority, no changes are required.

14. Right to object and portability

14.1 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 to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

We agree with the principle that an individual should be entitled to object or withdraw their consent to collection, use or disclosure of their personal information. However, we are concerned about the requirement that on receiving a notice an entity must take reasonable

steps to stop collecting, using and disclosing the individual's information. This would be onerous and unworkable in the healthcare context where practices collect patient information from third parties such as other healthcare providers, and often electronically. They may also be required to disclose information for the ongoing care of the patient.

Operationalising this would require healthcare providers to ask other healthcare providers not to send information to them and this would be administratively burdensome.

We note the Discussion Paper states that it would not prevent permissible secondary uses under the *Privacy Act*, specifically uses or disclosures that occur in response to a permitted general situation or a permitted health situation.

If this proposal were to be introduced, healthcare entities should be exempt.

15. Right to erasure of personal information

15.1 An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions:

- 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.

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.

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.

Questions

- In light of submitter feedback, should a 'right to erasure' be introduced into the Act?
- Should an erasure request be only available on a limited number of grounds, as is the case under Article 17 of the GDPR?
- What exceptions should apply to address the concerns raised in the government response to the ACCC's DPI report in relation to freedom of speech, challenges during law enforcement and national security investigations, and practical difficulties for industry?
- How would entities determine whether one of the exemptions applies in practice?
- Would the proposed public interest exception appropriately protect freedom of speech?

- Should a right to erasure apply to personal information available online, including search results?

We do not support introducing a right to erasure, for the reasons outlined in our submission to the Issues Paper. As all health information is deemed to be sensitive information the right to erasure would apply to all health information. It would be particularly problematic in the context of children as a child's health information may not become relevant to their healthcare until they are an adult and to erase it may have a significant impact on their future healthcare.

While we agree with the possible further exemptions outlined on page 122 of the Discussion Paper, we do not believe they go far enough in the healthcare context. Thus, if a right to erasure were to be introduced, healthcare entities should be exempt.

16. Direct marketing, targeted advertising and profiling

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.

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.

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.

16.4 Repeal APP 7 in light of existing protections in the Act and other proposals for reform.

We do not support this proposal. We are concerned that express consent for all forms of direct marketing will cause consent fatigue and unnecessary burden for entities. Direct

marketing could be differentiated from targeted advertising, with targeted advertising requiring express consent.

APP 7 achieves its purpose of regulating direct marketing and in our view is a sufficient check on entities' conduct. We therefore do not believe this privacy principle needs to be removed. APP 7's regulation of direct marketing is an important aspect of the privacy regime and having a separate privacy principle reflects this.

17. Automated decision-making

17.1 Require privacy policies to include information on whether personal information will be used in automated decision-making which has a legal, or similarly significant effect on people's rights.

18. Accessing and correcting personal information

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.

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.

We agree with the proposal to include an additional ground to refuse access where the information relates to external dispute resolution services and giving access would prejudice the dispute resolution process.

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.

We support this proposal. In the context of healthcare, this will allow a practitioner to provide a healthcare summary to a patient and is consistent with the position in NSW.

Question

- Is there evidence that individuals are being refused access to personal information that has been inferred about them? In particular, is the exception at APP 12.3(j) being relied on to refuse individuals' requests to access inferred personal information?

In our experience, patient requests for access to healthcare records (which often includes inferred information) is usually only refused on limited grounds, mostly on the grounds that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety (APP 12(a)) or giving access would have an unreasonable impact on the privacy of other individual (APP 12(b)).

19. Security and destruction of personal information

19.1 Amend APP 11.1 to state that 'reasonable steps' includes technical and organisational measures.

19.2 Include a list of factors that indicate what reasonable steps may be required.

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.

As noted in our submission to the Issues Paper, lack of clarity over what is appropriate in terms of security can operate as an impediment to the appropriate delivery of healthcare or access to information. It can also lead to lack of security. In our experience, there are varying levels of understanding and capability among medical practices (which are often small businesses) about best practice cyber security measures. It is telling that in the last reporting period, healthcare providers reported the most ransomware-related data breaches to the OAIC under the Notifiable Data Breaches scheme.

We would therefore support clearer security requirements, but agree that flexibility needs to be maintained.

The factors outlined in the current APP guidelines (referred to in the Discussion Paper) that influence what reasonable steps may be required are helpful, but we do not have a strong view about whether or not they should be included in the legislation.

In the healthcare context, anonymisation is impractical and unworkable, and destruction of information is subject to other legislation that requires it to be obtained for a specified period.

20. Organisational accountability

20.1 Introduce further organisational accountability requirements into the 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.

Questions

- Would the proposed additional accountability requirement in relation to restricted practices encourage APP entities to adopt a privacy by design approach?

- How might the requirement be framed to reduce the likelihood of APP entities adopting a compliance mentality to the requirement?
- What assistance could be provided to APP entities to support them in meeting these accountability requirements?

We agree with the comment in the Discussion Paper that:

> Organisational accountability measures must strike the right balance to ensure APP entities incorporate adequate measures in their organisational governance, systems and practices to ensure compliance with the Act without unduly burdening APP entities with overly prescriptive compliance requirements.

We are concerned that additional accountability requirements would be unduly onerous for medical practices, many of which are small businesses, without dedicated privacy officers, and which already have significant healthcare accreditation requirements for the operation of their practices. We believe that this proposal would not increase organisational accountability or lead to any improvement in privacy practices, but instead risks being regarded as a "tick-box" compliance activity.

22. Overseas data flows

22.1 Amend the Act to introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a).

22.2 Standard Contractual Clauses for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information.

22.3 Remove the informed consent exception in APP 8.2(b).

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.

22.5 Introduce a definition of 'disclosure' that is consistent with the current definition in the APP Guidelines.

22.6 Amend the Act to clarify what circumstances are relevant to determining what 'reasonable steps' are for the purpose of APP 8.1.

We strongly support this proposal, for the reasons outlined in our submission to the Issues Paper. We agree this would facilitate overseas disclosures of personal information in the absence of the informed consent exception.

23. Cross Border Privacy Rules and domestic certification

23.1 Continue to progress implementation of the CBPR system.

23.2 Introduce a voluntary domestic privacy certification scheme that is based on, and works alongside CBPR.

We can see many benefits to a voluntary domestic certification scheme, for companies wishing to demonstrate that they are privacy complaint and for individuals and businesses using products and services.

As noted in our submission to the Issues Paper, during the initial phase of the COVID pandemic and the move to telehealth, many medical practitioners were concerned to ensure that the videoconferencing product they wanted to use was compliant with Australian privacy laws. Similar issues arise in the context of apps and other systems used by practitioners for digital communication in the provision of healthcare. Certification for privacy compliant products would be useful in this regard, for all entities that hold personal information.

Such a certification scheme should be voluntary.

Part 3: Regulation and enforcement

24. Enforcement

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.

24.2 Clarify what is a 'serious' or 'repeated' interference with privacy.

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.

24.4 Amend the Act to provide the IC the power to undertake public inquiries and reviews into specified matters.

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 <u>identify, mitigate and</u> redress <u>any actual or reasonably foreseeable</u> loss or damage suffered by the complainant/those individuals.

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.

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.

24.8 Amend the annual reporting requirements in the AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground.

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.

We are concerned that the addition of civil penalties for interferences of privacy that are not serious or repeated will lead to increased litigation costs.

We agree with the proposal to clarify what is a serious or repeated interference with privacy. We agree with the comment in the Discussion Paper that the threshold could be more clearly expressed in terms of the number of individuals to which it applies. We agree that the legislation could more clearly capture breaches involving:

- highly sensitive information
- those adversely affecting large groups of individuals
- those impacting vulnerable individuals
- repeated or wilful misconduct,
- serious failures to take proper steps to protect personal data.

We agree with the comment in the Discussion Paper that this would increase clarity for the OAIC, entities and the Courts.

We oppose the industry funding proposal, particularly for the medical profession. This has the potential to impose a significant financial burden on medical practices, many of which are small businesses, funded either partly or entirely through Medicare payments, and which deal with sensitive healthcare information on a daily basis.

25. A direct right of action

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) 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.

We oppose this proposal on the grounds outlined in our submission to the Issues Paper, which we will not repeat here.

We note the proposal that a direct right of action be available to individuals and representative classes of individuals. Like other submitters to the Issues Paper (referred to in the Discussion Paper) we are concerned about the potential for class actions under this right. We are seeing increasing class actions in the medical liability space and we would be concerned if this were to follow in the privacy space as a consequence of these reforms.

If a direct right of action were introduced, we would strongly support gateway provisions including compulsory conciliation and leave of the court to proceed. Costs should follow the event as per the usual costs orders in the Federal Court.

26. A statutory tort of privacy

26.1 **Option 1**: Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.

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.

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.

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.

We oppose this proposal on the grounds outlined in our submission to the Issues Paper, which we will not repeat here.

In addition to the issues canvassed in this Discussion Paper, consideration should be given to how this tort might align with other legislative regimes, such as state-based civil liability and defamation legislation, particularly in terms of recovery of compensation and heads of damage.

27. Notifiable Data Breaches scheme

27.1 Amend subsections 26WK(3) and 26WR(4) to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates.

Questions

- In what specific ways could harmonisation with other domestic or international data scheme notifications be achieved?
- What aspects of other data breach notification schemes might be beneficial to incorporate into the NDB scheme?

We refer to our submission to the Issues Paper and confirm our position that:

- Notification requirements under the *Privacy Act* and the *My Health Records Act* should be aligned.
- An exemption from the obligation to notify individuals should be added where doing so would pose a serious threat to the life, health and safety of an individual.

28. Interactions with other schemes

28.1 The Attorney-General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.

28.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.

28.3 Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

Question

- What aspects of Commonwealth, state and territory privacy laws should be considered for harmonisation by this working group if it is established?

We agree with the proposal to establish a Commonwealth, state and territory working group to harmonise privacy laws. Aspects of privacy laws that should be considered for harmonisation are:

- Extension of privacy protections to deceased individuals.

  As noted in our submission to the Issues paper, legislation in NSW, Victoria, the ACT and NT applies to medical records of deceased patients, whereas the Commonwealth *Privacy Act* does not. We noted that we consider it would be beneficial to healthcare providers if there was a clear and consistent approach to the way in which the states, territories and the Commonwealth managed the storage and retention of, and access to deceased patients' medical records. This approach should cover access when it is required for compassionate and legal reasons. The issue of who is entitled to access records after death needs clarification, particularly where probate or letters of administration have not yet been granted.

- Privacy regimes for heath information

  We are of the strong view that there is a need for harmonisation of privacy protections for health information not only under Commonwealth laws, but also across jurisdictions and between public and private sectors.

  Victoria, NSW and the ACT have legislation specifically relating to health records and health information which must be complied with in those jurisdictions along with the Commonwealth privacy legislation. In our submission to the Issues Paper, we referred to some inconsistencies between states and federal privacy requirements in the context of health care. For example, in NSW, where there is request for access to health information it is mandatory to suggest that the patient nominate a medical intermediary. This is not the case under the Commonwealth *Privacy Act*.

Avant Mutual
10 January 2022