27 November 2020

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 Issues 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 would be welcome the opportunity to engage further with the Attorney-General's department to elaborate on any of the issues raised as the review progresses.

Yours sincerely

Georgie Haysom
Head of Research, Education and Advocacy
Direct: (02) 9260 9185
Email: georgie.haysom@avant.org.au

Avant submission on the Privacy Act Review Issues 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.

Over the last three financial years, Avant received 12,969 calls from members to our Medico-Legal Advisory Service relating to confidentiality or records, comprising 17% of all calls. Members called us about issues including access to and disclosure of clinical records, security of records and cyber issues, and notifiable data breach notification.

Avant and its subsidiaries hold a large amount of personal and health information about our members, insureds and customers, as well as information about patients and others who have made complaints or taken legal action against our members.

Privacy-related claims made by members on their insurance policies include claims where there are allegations of unauthorised access to records, failure or refusal to release information or to transfer records, release of information without consent and unauthorised disclosure.

We would welcome the opportunity engage further with the Attorney-General's department to elaborate on any of the issues raised as the review progresses.

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.

Questions for consideration

Objectives of the Privacy Act

1. Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?

We agree with the comment in the Issues paper that the requirement to balance the protection of privacy with the interests of businesses can be difficult where the core activity of the business is in acquiring and dealing in personal information. This balance is appropriately met with the current objectives.

In our view privacy law should not be used as the vehicle to fill gaps in the consumer protection regime. The interests of consumers are protected by key objects of the Act including to promote the protection of individuals, promote responsible handling of personal information and provide a means to complain about an alleged interference with privacy. We do not consider the current objectives need to be changed. It remains important to recognise the interests of entities in carrying out their functions or activities which includes sole medical practitioners without the benefit of compliance or privacy units.

An even greater emphasis on consumer protection may lead to increased regulatory and administrative burdens for medical practice. For insurers (like Avant) this may lead to more claims and complaints on insurance policies, adding to insurance costs. For healthcare practitioners this will increase compliance and administration costs.

Definition of personal information

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

We agree that the application of the definition of personal information is unclear in the context of technical data and online identifiers, and that this should be clarified. The

definition should ensure that it relates to information that is capable of being used to identify or re-identify an individual.

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

No. We do not support offering protection to inferred information as this would be unworkable in the health context (see further below in answer to questions 35 and 36).

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

Although this question asked about additional protections, we have some comments on the current system. APP 2 already provides individuals the option of requesting to be anonymous (APP 2). This is not practical for healthcare providers where the ability to bill Medicare depends on an identifier, and continuity of care depends on access to identifiable notes and results. In our view healthcare providers should be exempt from the requirements in APP2.

In relation to de-identified information, it would be helpful to have greater clarity in the legislation that APP entities can retain and use information that is not reasonably identifiable provided they manage the risk of identification or re-identification and comply with other applicable laws. This would give much more certainty around the use of, for example, de-identified clinical photographs that are an important education tool for healthcare providers. Similarly, it would alleviate the concerns of many GP providers about sharing de-identified data for health policy and quality improvement projects with primary health networks.

We do not consider that the legislation should prescribe standards or a specific methodology for de-identification as this would impose an unnecessary additional burden on small healthcare practices, but also because it is an area that is changing and could be quickly out of date. It would, however, be helpful for the OAIC to continue to provide updated guidance and practical recommendations on this issue in its information sheets.

We do not believe that there should be any additional protections are required. Requiring anonymisation in the healthcare context would be unworkable.

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

The Issues Paper notes at pages 20-21 that the protections under the Act only apply to personal information of living, natural persons. This is consistent with the GDPR and other privacy regimes, on the basis that only living people have "privacy rights".

However, as pointed out at page 21, some states have legislation that applies to the medical records of deceased patients (Victoria, NSW, ACT and NT). Similarly, the My Health Record regime covers deceased patient information.

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, retention and access of 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.

As to the definition of personal information generally, with the definition of personal information becoming increasingly complex with technological advances, another option for consideration is whether it would be useful to consider an exclusionary definition of personal information, ie what it is not.

Flexibility of the APPs in regulating and protecting privacy

6. Is the framework of the Act effective in providing flexibility to cater for a wide variety of entities, acts and practices, while ensuring sufficient clarity about protections and obligations?

It is stated at page 22 that a key objective of the APPs is to balance the protection of the privacy of individuals with the interests of public and private sector entities in carrying out their lawful and legitimate functions and activities. This is said to be achieved through the "scalability of the APPs" to a wide range of entities and practices and "legislative flexibility to adapt the APPs".

An issue our members have faced suggests there is a lack of flexibility and scalability in the APPs when applied in the healthcare context.

The issue involves the requirement to obtain consent to transfer medical records when either a medical practice is being sold or an individual specialist is moving to a new practice. This arises from the requirement that entities must obtain consent of the individual to collect their information.

This issue reveals a misalignment between notions of ownership and privacy rights. A practice or practitioner may own the medical records, and those assets will generally form part of the sale of business agreement (if a practice is being sold) or a practitioner will be entitled to take these assets with them when they move practices.

This requirement is a barrier to continuity of care and inhibits patient choice about their healthcare provider. A delay in providing information can have negative impacts on patient care.

It is useful to compare the position under the Victorian Health Records Act 2001 and the Commonwealth Privacy Act 1988.

In Victoria, where a medical practice is being sold, the statutory guidelines confirm that the HPPs do not apply. It is therefore not necessary for the "old" practice to seek consent from patients to transfer the medical records to the "new" owner, or for the "new" owner to seek consent to "collect" the information. This facilitates the smooth handover of medical records and facilitates continuity of care for patients; patients are still entitled to request a transfer of their records to another practice.

By contrast, the Commonwealth Act does not address this issue. The OAIC produced draft guidelines which indicated that under the APPs it is necessary for healthcare providers to obtain patient consent for the disclosure (APP6) and collection (APP3) of health information. Avant provided submissions at the time highlighting the practical difficulties this would have, particularly if a large number of records was involved.

We noted the additional potential risk of a data breach if letters were sent to patients at old addresses requesting consent to transfer their records to a new practice.

The OAIC attempted to resolve this issue in draft guidelines that acknowledged there may be an exception to the need to obtain a patient's consent where a specialist is leaving a practice, but effectively carrying on the same business at the new location, as in this case the reason the information is being "used" or "disclosed" (to facilitate the specialist's continued treatment of the patient) aligns with the primary purpose for which it was collected (treatment of the patient). However, these guidelines were removed from the OAIC website and the new guidelines published in 2019 do not address the issue.

In the absence of any further clarity from the OAIC, there has been confusion amongst medical practices. Consequently, specialists have been prevented from taking their own medical records from the shared database without express patient consent on the basis that such removal of the records is a "secondary purpose" and a potential data breach.

We strongly recommend that this issue is resolved by adopting the approach taken in Victoria, namely statutory guidelines that confirm APPs 3 and 6 do not apply to the sale of a medical practice or where a specialist is re-locating his or her practice to a new location, and requires the records of patients referred to and seen by them, to enable continuity of care. Alternatively, it may be appropriate to exempt healthcare providers from the requirement to obtain consent to transfer records to a new practice under the permitted health situations.

Exemptions

Small business exemption

7. Does the small business exemption in its current form strike the right balance between protecting the privacy rights of individuals and avoid imposing unnecessary compliance costs on small business?
8. Is the current threshold appropriately pitched or should the definition of small business be amended?
    a. If so, should it be amended by changing the annual turnover threshold from $3 million to another amount, replacing the threshold with another factor such as number of employees or value of assets or should the definition be amended in another way?
9. Are there businesses or acts and practices that should or should not be covered by the small business exemption?
10. Would it be appropriate for small businesses to be required to comply with some but not all of the APPs?
    a. If so, what obligations should be placed on small businesses?
    b. What would be the financial implications for small business?
11. Would there be benefits to small business if they were required to comply with some or all of the APPs?
12. Should small businesses that trade in personal information continue to be exempt from the Act if they have the consent of individuals to collect or disclose their personal information?

We accept that, given the sensitive nature of health information, it is reasonable to put in place measures to regulate access to and security of the information held by healthcare providers.

However, as the privacy protections apply to all healthcare providers regardless of turnover, it remains important to ensure that any changes to the protections do not create an unreasonable cost or administrative burden. The time and cost of compliance need to be factored into any changes.

For consistency we suggest that the definition of small business be consistent with the Fair Work Act which focusses on the number of employees (less than 15 employees) rather than turnover. This is a good measure of availability of staff and financial resources in a business for compliance activities.

Employee records exemption

13. Is the personal information of employees adequately protected by the current scope of the employee records exemption?
14. If enhanced protections are required, how should concerns about employees' ability to freely consent to employers' collection of their personal information be addressed?
15. Should some but not all of the APPs apply to employee records, or certain types of employee records?

There is much confusion around the need for a collection notice for employee records and the scope and application of the exemption: see the decision of the Fair Work Commission in Lee v Wood regarding biometric data collected after employment was already on foot. The Commission found that the Privacy Act did not apply once the information was collected. This raises the question as to whether employees' information is being adequately protected in light of this exemption.

Notice of Collection of Personal Information

Improving awareness of relevant matters

20. Does notice help people to understand and manage their personal information?
21. What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?
22. What sort of requirements should be put in place to ensure that notification is accessible; can be easily understood; and informs an individual of all relevant uses and disclosures?

The discussion at pages 38-40 of the Issues Paper only refer to the notification requirements at APP5. There is no reference to the concurrent requirement in APP1 for businesses to have a privacy policy. In our view there is a lot of crossover and /or duplication in medical practices between the privacy policies and the collection statement, and when considering what information is given to consumers or patients it is appropriate to consider the interaction between APPs 1 and 5.

When patients attend medical practices there is an understanding that doctors will collect information about them to facilitate ongoing healthcare.

We agree that the central concepts of "reasonableness" and "practicability" should be retained so there is sufficient flexibility for medical practices to adapt their collection notices to the nature of the practice and needs of the patient. We do not agree with the DPI report that the collection of personal information – whether directly or indirectly – needs to be accompanied by a collection notice; this would not always be practical in a healthcare setting where information is being collected from different sources (eg. hospital discharge summaries) and would add to compliance costs without any significant benefit where there is likely to be a "reasonable contemplation" that such information will be shared and collected.

Third party collections

23. Where an entity collects an individual's personal information and is unable to notify the individual of the collection, should additional requirements or limitations be placed on the use or disclosure of that information?

We note the ACCC's view that an individual should always be provided with notice when their personal information is collected regardless of whether the collection is direct or indirect.

Complexities arise in the context of indemnity insurance products Avant offers because personal information is collected about consumers/patients via our insureds/members.

The Issues paper notes that there is a question of how this could be implemented where the entity does not have the individual's contact information. We agree that this is an important question that needs consideration, as it is impractical and unworkable for an insurer to provide notice to a consumer that we might collect their information via our insureds.

In any event, there are existing exemptions that allow collection, use and disclosure where it is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim, but we believe this exemption could be strengthened/broadened to make it clear that information can be collected, used or disclosed for these purposes as well as to obtain advice about a complaint or adverse incident.

Limiting information burden

24. What measures could be used to ensure individuals receive adequate notice without being subject to information overload?
25. Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?

In our view it is unnecessary to have another notice for matters that are dealt with in an entity's Privacy Policy.

Consent to collection and use and disclosure of personal information

Consent to collection, use and disclosure of personal information

26. Is consent an effective way for people to manage their personal information?
27. What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?
28. Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?
29. Are the existing protections effective to stop the unnecessary collection of personal information?
    a. If an individual refuses to consent to their personal information being collected, used or disclosed for a purpose that is not necessary for providing the relevant product or service, should that be grounds to deny them access to that product or service?
30. What requirements should be considered to manage 'consent fatigue' of individuals?

Existing protections are effective.

We do not agree with the recommendations of the ACCC to strengthen consent requirements as outlined on page 42 of the Issues Paper, as these would be unworkable in the healthcare context.

The consent-based model for privacy can be problematic and adds to the administrative burden on entities particularly in the context of healthcare:

- As noted above in answer to question 6, the requirement that an individual must consent to the collection of their sensitive information does not work in the context of a practice that holds medical records being acquired by another practice.
- A requirement to obtain consent on each occasion a patient attends a practice for healthcare is unnecessary where there is an ongoing relationship between the patient and the practice.
- Requiring separate consents for each purpose can be difficult in the healthcare context and would be an administrative burden.
- Application of the provisions relating to unsolicited information (eg information provided to a healthcare provider by a family member which might be highly relevant to their ongoing care) int this context is confusing.

In our view, in the healthcare context, it is the way in which entities use and disclose information they collect that is the fundamental issue, rather than collection.

It could be useful to consider a standing consent model for collection of health information as per the model under the *My Health Records Act 2012 (Cth)*, with a list of legitimate purposes for which the information can be used and disclosed.

Exceptions to the requirement to obtain consent

31. Are the current general permitted situations and general health situations appropriate and fit-for-purpose? Should any additional situations be included?

We believe that the permitted health situations could be strengthened and expanded, to include an exemption for:

- Use and disclosure for the purposes of quality assurance, quality control, education and training.
- Use and disclosure for the purposes of obtaining legal advice or advice from a medical indemnity provider about a complaint or adverse incident, as well as for the establishment, exercise or defence of a legal or equitable claim.
- Transfer of records following the sale of a practice or where a practitioner moves practices (as outlined in answer to question 6 above).

The exceptions to giving access to medical records should cover the situation where information is provided to a medical practice “in confidence”, not to be disclosed to a patient.

The way in which the Privacy Act is drafted with the APPs in the schedule and the permitted general exceptions and permitted health exceptions in the body of the Act is confusing and makes the legislation difficult to navigate.

Obtaining consent from children

33. Should specific requirements be introduced in relation to how entities seek consent from children?

We recognise the concerns relating to children accessing digital platforms, and acknowledge that the recommendations in the DPI report are aimed at addressing these concerns. However, it is important to consider any unintended consequences that may arise when addressing the safety of children in one privacy related sphere. In our view if the requirements for obtaining consent from or on behalf of children are too prescriptive there is a risk some children may be dissuaded from seeking healthcare.

Lack of consistency causes confusion, and inconsistency in age settings leads to continuing misunderstandings about the age at which children have decision-making capacity generally.

It is widely assumed, incorrectly, that the age at which a child is legally considered to have medical decision-making capacity is set at 14. This is not correct as there is no specified age at which a child is considered to have capacity to consent; capacity in a child is based on an assessment that they have achieved "a sufficient understanding and intelligence to enable then to understand fully what is proposed" (in accordance with the common law test in *Gillick v West Norfolk AHA* , adopted in Australia in *Department of Health & Community Services v JWB & SMB* ("Marion's Case")).

A person is not presumed to have decision-making capacity until the age of 18 (16 in South Australia).

The current common law test, which requires clinicians to make a clinical assessment and to be satisfied a minor has sufficient maturity to understand fully the proposed treatment or medication, provides sufficient flexibility to account for the variations in the maturity of young people. The NSW *Health Records and Information Privacy Act 2002* includes a similar test for capacity in children for the purposes of the application of that legislation.

The role of consent for IoT devices and emerging technologies

34. How can the personal information of individuals be protected where IoT devices collect personal information from multiple individuals?

Collection of information and IoT devices is increasingly an issue that practices and health care providers face. It is necessary for health care providers to understand the need to have agreements in place with third party providers, and for patients to understand and accept –

personally - the terms and conditions of third party applications that may be used to help facilitate health care.

Many thirds party apps, data sharing tools and remote monitoring devices place the onus on practices and practitioner, through their standard form agreements, to obtain consent for collection, use and disclosure of information. This is an emerging area and we agree that the privacy implications need careful consideration.

Inferred sensitive information

35. Does the Act adequately protect sensitive information? If not, what safeguards should be put in place to protect against the misuse of sensitive information?
36. Does the definition of 'collection' need updating to reflect that an entity could infer sensitive information?

It is our view that the Act adequately protects sensitive information. In some instances, as outlined above, the protections contained in the Act go too far and present a barrier to the provision of healthcare.

The Issues Paper at page 19 states that inferred personal information is "information collated from a number of sources which reveals something new about an individual". We do not agree that the definition of personal information or the definition of collection should be changed or updated to include inferred personal or sensitive information.

Healthcare providers routinely collect and infer personal and sensitive information from the patient presentation, history, results etc which reveals something new about an individual.

Imposing additional protections for inferred information would be impractical in the healthcare context. This is likely to have unintended consequences for healthcare providers and could be a barrier to the provision of care to a patient.

We strongly disagree with extending the scope of the legislation to include inferred information, but if this is to occur, healthcare entities should be exempt.

Withdrawal of consent

38. Should entities be required to refresh an individual's consent on a regular basis? If so, how would this best be achieved?

As noted above in answer to question 30, requiring individuals to obtain consent on each occasion a patient attends a practice for healthcare is often unnecessary where there is an ongoing relationship between the patient and the practice.

Control and security of personal information

Security and retention

43. Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?

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. The use of email is a good example. Many healthcare providers and organisations are concerned that email may not be sufficiently secure to comply with privacy requirements, but using other means of communication perceived to be more secure (fax, mail or even in person delivery) can impact on the delivery of care.

44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?

The requirement to destroy or de-identify personal information must always be read subject to other laws concerning the retention of records.

In our view, there needs to be harmonisation of the laws in Australia so there is a clearer position on how long private medical records should be retained across the states and territories. This would be best achieved by aligning the Commonwealth with the existing requirements in NSW, Victoria and the ACT to retain adult records for 7 years from the date of the last consultation and until children are 25 years old.

As medical practices and doctors have an independent ethical and legal duty of confidentiality it is not necessary in our view for greater requirements to be imposed on destroying or de-identifying personal information. These issues should continue to be reinforced in guidance from the OAIC.

Right to erasure

46. Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?
47. What considerations are necessary to achieve greater consumer control through a 'right to erasure' without negatively impacting other public interests?

We do not agree that a right to erasure should be introduced, and if it is, healthcare entities should be exempt.

The Issues Paper acknowledges at page 51 that any "right to erasure" should not override existing obligations to retain personal information for legal reasons such as healthcare purposes and law enforcement requirements.

Many organisations are required to retain personal information in order to provide their services lawfully. In the context of healthcare, a right to erasure is inconsistent with

legislation noted above NSW, Victoria and the ACT, to retain adult records for 7 years from the date of the last consultation and until children are 25 years old. Destroying health records may have significant negative impacts on the provision of healthcare.

In addition, where there is a significant amount of information held "erasure" would be an extensive administrative burden.

Overseas data flows and third party certification

48. What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information?
    a. Are APP 8 and section 16C still appropriately framed?
49. Is the exception to extraterritorial application of the Act in relation to acts or practices required by an applicable foreign law still appropriate?
50. What (if any) are the challenges of implementing the CBPR system in Australia?
51. What would be the benefits of developing a domestic privacy certification scheme, in addition to implementing the CBPR system?
52. What would be the benefits or disadvantages of Australia seeking adequacy under the GDPR?

The discussion at pages 54 -57 of the Issues Paper highlights the complexity created by APP8 and section 16 for medical practices. For example, the distinction between "use" and "disclosure" of data that is stored in overseas servers is very nuanced and difficult for healthcare providers to consider when choosing a provider with servers based overseas (eg cloud server providers).

The difficulties were illustrated during the COVID pandemic and the use of videoconferencing for telehealth where the software providers were based overseas. Many practitioners were concerned to ensure that the videoconferencing product they wanted to use was compliant with Australian privacy laws. Certification for privacy compliant products would be useful in this regard, for all entities that hold personal information.

Similarly, healthcare providers are not familiar with the privacy regimes of overseas jurisdictions and many of them do not have the resources to research such issues. Greater clarity about the processes required to transfer information overseas would be useful.

A system that operates in a similar way to information exchange/double tax agreements would be helpful in dealing with privacy as relates to data held offshore, for example if covered by standards similar to Australia, satisfies Australia privacy requirements.

Enforcement powers under the Privacy Act and role of the OAIC

53. Is the current enforcement framework for interferences with privacy working effectively?
54. Does the current enforcement approach achieve the right balance between conciliating complaints, investigating systemic issues, and taking punitive action for serious non-compliance?
55. Are the remedies available to the Commissioner sufficient or do the enforcement mechanisms available to the Commissioner require expansion?

a. If so, what should these enforcement mechanisms look like?

We believe the current enforcement framework is working effectively.

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

Direct right of action

56. How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

We do not agree that a direct right of action is necessary. The OAIC's powers to investigate and make privacy determinations are sufficient to protect privacy.

Our concern is that allowing the option of direct action will increase costs to the system via increased legal costs and court costs. As with any direct right of action, there is a risk of unmeritorious claims and overinflated views of damages entitlements. We suggest that as part of this review analysis be conducted to determine the likely potential for increased legal and court costs if a direct right of action were to be introduced. The availability of insurance for this risk should also be considered.

If a direct right of action were to be introduced, it should be subject to a threshold, and only apply to serious breaches of privacy. There should be compulsory conciliation and other alternative dispute resolutions options and a cap on any compensation awarded, to ensure that court resources are appropriately directed.

Statutory tort

57. Is a statutory tort for invasion of privacy needed?
58. Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?
59. What types of invasions of privacy should be covered by a statutory tort?
60. Should a statutory tort of privacy apply only to intentional, reckless invasions of privacy or should it also apply to breaches of privacy as a result of negligence or gross negligence?
61. How should a statutory tort for serious invasions of privacy be balanced with competing public interests?
62. If a statutory tort for the invasion of privacy was not enacted, what other changes could be made to existing laws to provide redress for serious invasions of privacy?

As per our submissions about a direct right of action, we do not agree that a statutory tort of privacy is necessary.

Our concern is that legislating a statutory tort of privacy will increase costs to the system via increased legal costs and court costs. We suggest that as part of this review analysis be conducted to determine the likely potential for increased legal and court costs if a statutory

tort were to be introduced. The availability of insurance for this risk should also be considered.

If a statutory tort of privacy were to be introduced, it should only apply to intentional or reckless invasions of privacy, and should not extend to negligence or be based on strict liability. It should be clear what is to be covered under this tort, as compared with a direct right of action. There should be compulsory conciliation and other alternative dispute resolutions options and there should be a cap on any compensation awarded.

Notifiable Data Breaches scheme – impact and effectiveness

63. Have entities' practices, including data security practices, changed due to the commencement of the NDB Scheme?
64. Has the NDB Scheme raised awareness about the importance of effective data security?

The Issues paper notes on page 78 there is significantly more reporting of data breaches as a result of the NDB Scheme. In 2017 and 2019 we conducted surveys of our members about the scheme and a comparison of the results are reported in our article here. While there was an increase in awareness of the scheme by 2019, there were still misunderstandings about how the scheme operates.

There is more awareness of the scheme but whether this has changed entities' data security practices is unclear.

65. Have there been any challenges complying with the data breach notification requirements of other frameworks (including other domestic and international frameworks) in addition to the NDB Scheme?

Yes. There is a different regime for data breach notification requirements under the *My Health Records Act* (MHR Act) and data breach notifications under the *Privacy Act*. This causes confusion and is administratively burdensome. Practices need to have different processes and procedures depending on whether the notification is under the MHR Act or the *Privacy Act*.

Reporting obligations under the MHR Act are stricter than those under the *Privacy Act*. Under the *Privacy Act* a data breach is notifiable to affected individuals and OAIC if the breach is likely to result in serious harm to an individuals or individuals, and remedial action cannot be taken to prevent the likelihood of serious harm.

By contrast, all breaches or potential breaches are notifiable under the MHR Act. There is no need for serious harm, and even a breach that has been rectified or where remedial action has been taken must still be notified.

It would be preferable to align the notification requirements under the MHR scheme with those under the *Privacy Act*, to avoid confusion and to reduce the risk of non-compliance.

It would be useful to consider including further exceptions to notification requirements under the NDB scheme. Current exceptions are only available in extreme circumstances or on special application to the Information Commissioner.

We have assisted members in matters where the potential harm from notifying the person about the breach was worse than the potential harm from the breach itself. This is particularly the case where a patient may have mental health or other issues where there is a risk that their response to being notified of the breach will be out of proportion to the risk of serious harm from the data breach, leading to a risk of harm to themselves or others. We recommend that consideration should be given to having an exemption, similar to the exception that currently applies in respect of access under APP 12.3, where there is a serious threat to the life, health or safety of to an individual.

There may also be an overlap between the notifiable data breach scheme (which enlivens the jurisdiction of the OAIC) and state-based regulators, eg the Health Complaints Commission in Victoria, the Health Care Complaints Commission, and Privacy Commission in NSW, which may investigate complaints about the same incident if a complaint is made to those bodies by the affected individual. This can lead to the situation where there are concurrent investigations into the same issue.

Interaction between the Act and other regulatory schemes

66. Should there continue to be separate privacy protections to address specific privacy risks and concerns?
67. Is there a need for greater harmonisation of privacy protections under Commonwealth law?
    a. If so, is this need specific to certain types of personal information?
68. Are the compliance obligations in certain sectors proportionate and appropriate to public expectations?

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

There is inconsistency between state and federal legislative requirements. 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. As noted above in answer to question 5, legislation in NSW, Victoria, the ACT and NT applies to medical records of deceased patients, whereas the Commonwealth Privacy Act does not.

There is a significant compliance and administrative burden on businesses due to privacy and security requirements and this is amplified in those jurisdictions with their own privacy regimes. Slightly different requirements between Commonwealth and state/territory privacy laws leads to confusion and increased administrative costs, with limited benefit to patients.

The recently released OAIC draft guidance on the use of QR codes in COVID-safe plans for contact tracing is a good illustration. Each state and territory has its own rules around contact tracing including what information must be collected, how much and how long it must be stored for.

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

Avant Mutual Group
27 November 2020