Australian Government

Attorney-General's Department

Privacy Act Review

Discussion Paper

October 2021

Terms of Reference

Objective

The review will consider whether the scope of the *Privacy Act 1988* and its enforcement mechanisms remain fit for purpose.

Context

In its response to the Australian Competition and Consumer Commission's (ACCC) *Digital Platforms Inquiry*, the Government committed to undertake a review of the Privacy Act and to consult on options for implementing a number of privacy-specific recommendations to better empower consumers, protect their data and best serve the Australian economy.

The digital economy has brought with it immense benefits including new, faster and better products and services. The ability of businesses to engage with consumers online is vital to economic growth and prosperity. As Australians spend more of their time online, and new technologies emerge, such as artificial intelligence, more personal information about individuals is being captured and processed raising questions as to whether Australian privacy law is fit for purpose.

At the same time, businesses that are trying to do the right thing are faced with an increasingly complex regulatory environment with respect to managing personal information. This is particularly true for businesses who work across international borders where complying with information protection standards can be a requirement for access to overseas markets.

Matters to be considered by the review

The review will examine and, if needed, consider options for reform on matters including:

- The scope and application of the Privacy Act including in relation to:
    - the definition of 'personal information'
    - current exemptions, and
    - general permitted situations for the collection, use and disclosure of personal information.
- Whether the Privacy Act effectively protects personal information and provides a practical and proportionate framework for promoting good privacy practices including in relation to:
    - notification requirements
    - consent requirements including default privacy settings
    - overseas data flows, and
    - erasure of personal information.
- Whether individuals should have direct rights of action to enforce privacy obligations under the Privacy Act.
- Whether a statutory tort for serious invasions of privacy should be introduced into Australian law.
- The impact of the notifiable data breach scheme and its effectiveness in meeting its objectives.
- The effectiveness of enforcement powers and mechanisms under the Privacy Act and the interaction with other Commonwealth regulatory frameworks.
- The desirability and feasibility of an independent certification scheme to monitor and demonstrate compliance with Australian privacy laws.

The review builds on reforms announced in March 2019 to increase the maximum civil penalties under the Privacy Act and develop a binding privacy code to apply to social media platforms and other online platforms that trade in personal information.

Matters that will not be considered

The review will not consider the following areas that have only recently been considered:

- Credit reporting under Part IIIA of the Privacy Act
- Operation of Part VIIIA of the Privacy Act relating to the COVIDSafe app

Conduct and outcomes of the review

Consultation and evidence

The review will draw on a range of sources. The review will:

- Invite submissions on matters for consideration in the review
- Meet with stakeholders on specific issues
- Consider research and reports which consider privacy issues, including the:
    - ACCC Digital Services Advertising Inquiry
    - ACCC Digital Platforms Inquiry Final Report, 2019
    - Data Availability and Use, Productivity Commission Inquiry Report, 2017
    - Serious Invasions of Privacy in the Digital Era, ALRC Final Report 123, 2014
    - For Your Information: Australian Privacy Law and Practice, ALRC Report 108, 2008

Reviewer

The review will be undertaken by the Australian Attorney-General's Department.

Timing and outcomes

The review will commence in October 2020. The report of the review will be made public after government consideration.

Table of Contents

Abbreviations

2020 ACAP survey	OAIC Australian Community Attitudes to Privacy Survey 2020
ACCC	Australian Competition & Consumer Commission
ACCI	Australian Chamber of Commerce and Industry
ACL	Australian Consumer Law
ACMA	Australian Communications and Media Authority
ACT	Australian Capital Territory
ADHA	Australian Digital Health Agency
ADM	Automated Decision-Making
Ad tech Inquiry interim report	ACCC Digital advertising services inquiry: Interim Report
AFCA	Australian Financial Complaints Authority
AFP	Australian Federal Police
AHRC	Australian Human Rights Commission
AHRC report	AHRC Human Rights & Technology: Final Report
AI	Artificial Intelligence
AIC Act	*Australian Information Commissioner Act 2010*
ALRC	Australian Law Reform Commission
ALRC Report 108	ALRC, *For your Information: Australian Privacy Law and Practice* (Report No 108, 12 August 2008)
APC	Australian Privacy Council
APEC	Asia-Pacific Economic Cooperation
APP Guidelines	Australian Privacy Principles Guidelines
APPs	Australian Privacy Principles
APRA	Australian Prudential Regulation Authority
APRA Prudential Standard CPS 234	Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 1 of 2018
Archives Act	*Archives Act 1983* (Cth)
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
Bill C-11	*Bill C-11 Consumer Privacy Protection act and the Personal Information and Data Protection Tribunal Act* (2020) (Canada)
CAIDE and MLS	Centre for AI and Digital Ethics and Melbourne Law School
CBPR	Cross-Border Privacy Rules
CCA	*Competition and Consumer Act 2010* (Cth)
CCPA	*California Consumer Privacy Act of 2018*
CCTV	Closed circuit television
CDPP	Commonwealth Director of Public Prosecutions
CDR	Consumer Data Right
CIIs	Commissioner Initiated Investigations
CPRA	*California Privacy Rights Act of 2020*
CRIS	Cost Recovery Implementation Statement
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DNCR Act	*Do Not Call Register Act 2006*
DP Act	*Data Protection Act 2018* (UK)
DPIA	Data protection impact assessments
DPI report	ACCC Digital Platforms Inquiry: Final Report
DPI response	Government Response and Implementation Roadmap for the Digital Platforms Inquiry
EDR	External Dispute Resolution

Enhancing Privacy Protection Bill	Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012
ePD	ePrivacy Directive
EU	European Union
EU Data Protection Directive	*Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* [1995] OJ L 281.31, 23.11.1995
FCC	Federal Circuit Court
FOI Act	*Freedom of Information Act 1982* (Cth)
FPO	Federal Privacy Ombudsman
GDPR	*General Data Protection Regulation* (European Union)
ICCPR	International Covenant on Civil and Political Rights
IGIS	Inspector-General of Intelligence and Security
IC	Information Commissioner
IoT	Internet of Things
IPP	Information Privacy Principles
IP address	Internet Protocol address
MAC address	Media Access Controller address
MHR Act	*My Health Records Act 2012* (Cth)
MIGA	Medical Insurance Group Australia
MoU	Memorandum of Understanding
NDB scheme	Notifiable Data Breaches Scheme
NPP	National Privacy Principles
NSWIPC	New South Wales Information and Privacy Commission
NZ	New Zealand
NZ Privacy Act	*Privacy Act 2020* (NZ)
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Co-operation and Development
ONDC	Office of the National Data Commissioner
Online Safety Act	*Online Safety Act 2021* (Cth)
OP Bill	Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021
OP code	Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 sch 1.
OPC (Canada)	Office of the Privacy Commissioner of Canada
PIA	Privacy Impact Assessment
PIPEDA	Personal Information Protection and Electronic Documents Act 2000 (Canada)
PJCCFS	Parliamentary Joint Committee on Corporations and Financial Services
Spam Act	*Spam Act 2003* (Cth)
the Act	*Privacy Act 1988* (Cth)
TIA Act	*Telecommunications (Interception and Access) Act 1979* (Cth)
UK ICO	Information Commissioner's Office (UK)

Executive Summary

In its response to the Australian Competition and Consumer Commission's (ACCC) *Digital Platforms Inquiry* report (DPI report), the government committed to undertake a review of the *Privacy Act 1988* (Cth) (the Act) and to consult on options for implementing a number of privacy-specific recommendations to better empower consumers, protect their data and support the digital economy. The Review commenced in October 2020 with the release of the Review's Terms of Reference and an Issues Paper. The Issues Paper outlined the current provisions of the Act and sought feedback on a number of areas for potential reform.

The Review received 200 submissions in response to the Issues Paper from a diverse range of stakeholders, including private sector organisations, academics and research centres, industry peak bodies, consumer and privacy advocates, Commonwealth and state and territory public sector agencies and individuals. The majority of these submissions have been published on the Attorney-General's Department website. The department has also been conducting targeted consultation with stakeholders including other Australian Government departments and agencies, state and territory government departments, private sector entities, stakeholder representative organisations and peak bodies and international governments and privacy regulators.

Key themes

Overall, submitters supported changes to clarify the scope and application of the Act and remove ambiguity from the current provisions. Submitters were supportive of transparency as a key component of privacy protection but were wary of overreliance on notice and consent mechanisms. Submissions were broadly supportive of compliance costs continuing to be commensurate to privacy risk posed, and favoured retaining the flexible, principles-based approach of the Act as a method of managing the compliance burden on entities. Submissions advocated for enhanced mechanisms to enforce compliance with the Australian Privacy Principles (APPs) as well as more guidance on how to comply with the Act and appropriate avenues for individuals to make complaints.

Scope and application of the Act

Submitters were largely in favour of expanding the scope and application of the Act, but did not support adopting an overly prescriptive approach. A number of submissions called for exemptions from the Act to be removed or narrowed, including the small business, employee records and political exemptions. The general view among these submissions was that all entities should be subject to the Act unless there is a strong justification for an exemption. Concerns about the burden of compliance were evident in submissions on the small business and employee records exemptions. Submissions advocated for broadening the Act by providing individuals with greater control over an expanded range of personal information, through additional mechanisms to withdraw consent, request the erasure of personal information and seek redress for interferences with privacy.

Notice and consent and additional protections

Submitters expressed a strong interest in how Australian privacy law should regulate the collection, use and disclosure of personal information. Submitters were of the view that future reforms should not place an overreliance on notice and consent, as this may place an unrealistic burden on individuals to understand the risks of complicated information handling practices. Submitters called for additional protections in relation to collection, use and disclosure so that individuals can be confident that when they engage with entities, the law will protect them from harm and their personal information from misuse. Submitters proposed that entities should be required to handle personal information in a fair and reasonable manner or in accordance with the 'legitimate interest' test, adopted from the General Data Protection Regulation (GDPR). It was also considered that certain practices should be subject to more stringent requirements, or prohibited entirely. Submissions also called for increased protection of children's privacy. A range of submissions

proposed greater organisational accountability through introducing express privacy by design requirements. Transparency and control were considered key to the effective regulation of direct marketing in light of privacy-intrusive forms of digital advertising.

The interoperability and consistency of the Act with privacy regimes overseas was a primary concern in a large number of submissions, with many submitters favouring adopting particular definitions and obligations in order to ensure international consistency. These submissions primarily raised the GDPR as a desirable international privacy standard, but also referred to approaches adopted in countries with GDPR adequacy such as Canada and New Zealand. Submissions justified the need for international consistency on the basis that data is inherently international and alignment with overseas regimes is needed to better facilitate the cross-border transfers of information required in the digital economy.

Regulation and enforcement

The need for effective mechanisms to encourage compliance with the Act and remedy non-compliance was a common theme throughout submissions. Submitters recognised the need for a well-resourced regulator and advocated for the creation of alternative enforcement mechanisms. Effective enforcement mechanisms were viewed as a method of increasing individual control over privacy and providing general deterrence. Submitters supported strengthening the powers of the Information Commissioner (IC) and expressed a desire for a more proactive approach to enforcement, greater procedural clarity and more efficient resolution of complaints. Overall, submitters considered education to be an important aspect of enforcement and encouraged the expansion of educational tools.

Consistency with domestic legislation was also an area of concern, particularly the lack of uniformity between state and with other Commonwealth legislation. This was raised in relation to the definition of 'personal information', regulation of direct marking provisions and the application of multiple frameworks to specific types of information such as health data and employee records. Concerns over the burden of compliance were raised in the context of the interaction between the Act with other domestic privacy schemes. Submitters supported retaining separate regimes where justified, but called for uniform definitions and the removal of duplicative obligations.

About the Discussion Paper

This is the second of two papers seeking public input. This paper outlines feedback received through submissions to the Issues Paper and puts forward possible proposals for reforms to address issues identified with the current operation of the Act. While a large number of submissions addressed the current exemptions to the Act, the paper does not put forward reform proposals in these Chapters as it is necessary to seek further feedback in light of the Proposals outlined in other Chapters of this paper – in particular, the potential regulatory impact of the Proposals outlined in Part 2 will need to be given careful consideration. The Discussion Paper is designed to elicit feedback on the merits of the ideas and proposals outlined in the paper, including their practical impact, how they may interact with each other and whether different or additional changes are needed.

Feedback received through submissions and further consultations to be conducted following the receipt of submissions to the Discussion Paper will inform the Review's Final Report to be considered by government.

The government will consider what, if any, reforms it wishes to make to the Act following consideration of the Final Report.

OP Bill

In parallel with the Review, the government is seeking feedback on the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (OP Bill). The OP Bill gives effect to the government's commitment to create a binding online privacy code (OP code) for organisations that provide social media services, data brokerage services and other large online platforms that collect Australians' personal information in the course of providing information, goods or services. The OP code will require organisations to take reasonable steps to stop using or disclosing an individual's personal information upon request, strengthen requirements for organisations to be transparent about data sharing, and require organisations to follow stricter rules about handling the personal information of children and other vulnerable groups, with specific rules for social media services. The OP Bill also increases penalties and enhances enforcement mechanisms. Further detail about the OP Bill can be found on the exposure draft page of the Attorney-General's Department website.[1]

The OP Bill and OP code are referred to throughout this Discussion Paper, as there are intersections. The OP Bill addresses the unique and pressing privacy challenges posed by social media and online platforms through the introduction of the OP code. The OP Bill also contains provisions that will affect all APP entities by increasing penalties and enhancing particular enforcement mechanisms. These provisions address the Office of the Australian Information Commissioner's (OAIC) immediate need to have an appropriate regulatory and enforcement toolkit to resolve matters more efficiently and effectively, ahead of any options that are implemented following the Review. The Review will build on the outcomes of consultations on the OP Bill exposure draft and feedback from the Review may also be considered during the development of the OP code.

Call for submissions

You are invited to make a submission in response to the proposals and questions in this Discussion Paper or any other matter relevant to the Review's Terms of Reference. We may publish your submission, unless you request for it to remain confidential, or if we consider (for any reason) that it should not be made public. We may also redact parts of published submissions as appropriate. Refer to our privacy policy to more information.

To assist us when publishing submissions, please clearly indicate when lodging your submission:

1. Do you consent to your submission being published on the Attorney-General's Department website?
2. If yes, do you require all personal information contained in your submission to be redacted prior to publication (for example, names, email addresses, phone numbers)?
    - If you require some but not all personal information contained in your submission to be redacted, please provide us with the relevant details to make those redactions.

Submissions should be returned by **10 January 2022** via the department's website or by email to PrivacyActReview@ag.gov.au. For further information about the consultation process for the Review, please visit Review of the Privacy Act.

[1] Exposure Draft, Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 ('OP Bill'); Explanatory Paper, Privacy Legislation Amendment (Enhancing Online Privacy and Enforcement) Bill 2021.

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.

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

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

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

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.

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*.

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.

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.

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.

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.

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*.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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 identify, mitigate and redress any actual or reasonably foreseeable 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.

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)[1] and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman.
- The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application.
- The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.

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.

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.

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.

Part 1: Scope and Application of the Privacy Act

1. Objects of the Act

The Issues Paper asked if any changes should be made to the objects in section 2A of the Act, including whether it remains appropriate to balance the protection of privacy with the interests of entities, in line with the recommendation in the DPI report.[2]

Submissions from individuals, civil society, not-for-profits, some businesses, academics and the OAIC considered that the objects should do more to value the protection of privacy.[3] A few of these submissions said the objects reflect a broader conceptual deficiency in the Act, including the lack of a definition of 'privacy'.[4] This view was related to the concern that, to avoid confusion, the object at subsection 2A(a) should clarify that the Act's protection applies only to personal information and not to privacy more broadly.[5]

Some submissions in favour of change said it was not enough to 'promote' or 'respect' privacy, but rather privacy should be unequivocally protected or 'ensured'.[6] Many also said the objects should expressly refer to privacy as a fundamental human right and treat the 'right to privacy' as the 'paramount' object of the Act.[7]

Submissions said the power of certain commercial entities, including digital platforms is such that the balance is now always weighed against individuals.[8] Some said the object at subsection 2A(b) should instead, at most, 'have regard to', 'consider', or 'take into account' the interests of entities, placing more emphasis on protecting privacy.[9] Some also said the objects should refer to specific

[2] *Privacy Act 1988* (Cth) ('*Privacy Act*'); Australian Competition and Consumer Commission ('ACCC'), *Digital Platforms Inquiry* (Final Report, June 2019) 439, 477 ('DPI report').

[3] Submissions to the Issues Paper: Dr Kate Mathews Hunt, 3; The New York Times, 1; Electronic Frontiers Australia, 1; Association for Data-driven Marketing and Advertising, 8; Calabash Solutions, 3; Australian Council on Children and the Media, 3; Australian Information Security Association, 5; Uniting Church of Australia, 2; Consumer Policy Research Centre, 2; SuperChoice, 2; Blancco, 15–16; Dr Caitlin Curtis, Prof Nicole Gillespie and Dr Steve Lockey (University of Queensland), 3; Queensland University of Technology Faculty of Law, 6; Salinger Privacy, 18, 27; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 2; Royal Australian College of General Practitioners, 2; Guardian Australia, 2; Office of the Australian Information Commissioner, 21 ('OAIC'); Law Council of Australia, 8; Australian Communications Consumer Action Network, 6; Data Synergies, 15; Prof Kimberlee Weatherall, 3; Shaun Chung and Rohan Shukla, 2; Australian Privacy Foundation, 9; Centre for Media Transition, University of Technology Sydney, 5; Obesity Policy Coalition, 3; Centre for Cyber Security Research and Innovation, 2; NSW Council for Civil Liberties, 3.

[4] Submissions to the Issues Paper: Data Synergies, 15; Minderoo Tech and Policy Lab, University of Western Australia Law School, 2, 19; Queensland University of Technology Faculty of Law, 6–7.

[5] Submissions to the Issues Paper: Association for data-driven marketing and advertising, 8; Prof Kimberlee Weatherall, 3.

[6] Submissions to the Issues Paper: ID Exchange, 6; Australian Banking Association, 3; Shaun Chung and Rohan Shukla, 2; Australian Privacy Foundation, 9.

[7] Submissions to the Issues Paper: Centre for Media Transition, University of Technology Sydney, 5; Centre for Cyber Security Research and Innovation, 2; Public Interest Advocacy Centre, 5; Castan Centre for Human Rights Law – Monash University, 11; Shaun Chung and Rohan Shukla, 2–3; HIV/AIDS Legal Centre, 1; Australian Privacy Foundation, 9; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 6; Australian Information Security Association, 5; Australian Council on Children and the Media, 3; Privacy108, 2; Consumer Policy Research Centre, 3. See also Submissions to the Issues Paper: Digital Rights Watch, Access Now, Centre for Responsible Technology Australia, Electronic Frontiers Australia, Fastmail and Reset Australia (joint submission), 1–2; Rights in Records by Design (Monash University), 1; Benevolent Society, 4.

[8] Submissions to the Issues Paper: Consumer Policy Research Centre, 3; Obesity Policy Coalition, 3–4; Australian Communications Consumer Action Network, 6.

[9] Submissions to the Issues Paper: Shaun Chung and Rohan Shukla, 3; Prof Kimberlee Weatherall, 3; Castan Centre for Human Rights Law – Monash University, 13.

high-risk actions, including automated decision-making, Artificial Intelligence (AI) and data analytics,[10] or more generally to the current era of mass data collection.[11]

However, several submitters, including digital platforms, industry groups and research bodies supported the balancing exercise as necessary to ensure entities can operate effectively and efficiently.[12] Many were concerned that individuals would lose benefits gained from innovation if subsection 2A(b) no longer acknowledged the interests of entities in carrying out their functions or activities, particularly from developments in data analytics.[13]

Overall, submitters across the spectrum said the balancing exercise should be guided by proportionality, reasonableness and actions that serve legitimate, public interests.[14]

Proposal

In recognition that the objects should make it clear that the Act is concerned with informational privacy and that the protection of privacy is properly balanced against the protection of other public interests, subsections 2A(a) and (b) could be amended respectively.

Subsection 2A(a) could be amended to make clear that the Act is about protecting the personal information of individuals, and not more general notions of privacy.

Subsection 2A(b) could be amended to make it clearer that the subjective interests of entities are not relevant if their functions and activities are not in the public interest. This would recognise that not all interests should be reconciled with the protection of privacy. This would also be consistent with the Act's recognition of public interests other than privacy, including public health and safety,[15] research,[16] national security, freedom of expression,[17] law enforcement and, regarding commercial entities, the economic wellbeing of the country.

This proposal would ensure that the objects continue to acknowledge the many, varied interests that compete and coexist with the protection of privacy. The Act reconciles these interests by

---

[10] Submissions to the Issues Paper: Electronic Frontiers Australia, 1; Centre for Media Transition, University of Technology Sydney, 6; Legal Aid Queensland, 2; Humanising Machine Intelligence Project, Australian National University, 4; Dr Caitlin Curtis, Prof Nicole Gillespie and Dr Steve Lockey (University of Queensland), 3–5. See also Submission to the Issues Paper: Centre for AI and Digital Ethics and Melbourne Law School, University of Melbourne, 2, 5 ('CAIDE and MLS').

[11] Submissions to the Issues Paper: Minderoo Tech and Policy Lab, University of Western Australia Law School, 19; Australian Information Security Association, 5. See also Submissions to the Issues Paper: Digital Rights Watch, Access Now, Centre for Responsible Technology Australia, Electronic Frontiers Australia, Fastmail and Reset Australia (joint submission), 1; Reset Australia, 2; IDCARE, 2; Guardian Australia, 2–4.

[12] Submissions to the Issues Paper: Australian Financial Markets Association, 3; Fundraising Institute Australia, 3; Ramsay Australia, 3; Ai Group, 4; Avant Mutual, 3; Arts Law Centre of Australia, 3; Communications Alliance, 3; Australian Medical Association, 1; Optus, 3; IGEA, 7; KPMG, 4; DIGI, 5; Cyber Security Cooperative Research Centre, 5; CSIRO, 3; Clubs Australia, 2; Insurance Council of Australia, 3; SBS, 3; MIGA, 5; Australian Retail Credit Association, 7; Assured Support, 2; Database Consultants Australia, 8. See also Submission to the Issues Paper: Australian Banking Association, 3.

[13] Submissions to the Issues Paper: Telstra, 14; Google, 3; SBS, 3–4; Federal Chamber of Automotive Industries, 7; Optus, 3; BSA | The Software Alliance, 2; Facebook, 23. See also Submissions to the Issues Paper: Information Technology Industry Council, 1; ANZ, 3; Australian Finance Industry Association, 2; Oracle, 3.

[14] Submissions to the Issues Paper: Google, 3; Data Synergies, 16; Guardian Australia, 2; Law Council of Australia, 8; Salinger Privacy, 18, 27; Minderoo Tech and Policy Lab, University of Western Australia Law School, 19; Castan Centre for Human Rights Law – Monash University, 13; Association for data-driven marketing and advertising, 8–9; Prof Kimberlee Weatherall, 3; Facebook, 23; IGEA, 7; DIGI, 5; Communications Alliance, 3; Centre for Media Transition, University of Technology Sydney, 6; Shaun Chung and Rohan Shukla, 3–4; Griffith University, 4; Queensland University of Technology Faculty of Law, 6; ID Exchange, 7; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 6–7; Public Interest Advocacy Centre, 5; Australian Information Security Association, 5; Uniting Church in Australia, 1–2; Privacy108, 2; Arts Law Centre of Australia, 3. See also Submissions to the Issues Paper: Australian Association of National Advertisers, 3; Queensland Law Society, 1; Experian, 4.

[15] Submissions to the Issues Paper: Ramsay Australia, 2; Australian Medical Association, 1; Avant Mutual, 3; MIGA, 5; Department of Health of Western Australia, 1.

[16] Submissions to the Issues Paper: Griffith University, 4; Murdoch Children's Research Institute, 2; Australian Society of Archivists, 3; Rights in Records by Design (Monash University), 2.

[17] Submission to the Issues Paper: Arts Law Centre of Australia, 3.

balancing them, to determine which interferences with privacy are arbitrary, per International Covenant on Civil and Political Rights (ICCPR) Art 17. It is not appropriate for the objects to refer to a 'right to privacy' because, despite common parlance, Art 17 does not confer such a right, nor does it amount to absolute protection.

This proposal also complements the proposed fair and reasonable test (Proposal 10.1), which would require an APP entity to consider if its collection, use or disclosure of an individual's personal information would attract societal harms, in recognition of privacy as a collective concern.

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. Personal information, de-identification and sensitive information

The definitions of 'personal information' and 'de-identified' determine the scope of the Act. Information that falls within the definition of 'personal information' must be handled in accordance with the Act. Once information is 'de-identified', the Act no longer applies. Within the definition of personal information, the definition of 'sensitive information' specifies types of personal information that are subject to additional protections.

The Issues Paper sought feedback on the ACCC's DPI recommendation that the definition of personal information in the Act be updated to clarify that it captures technical information, such as IP addresses and other online identifiers that may be used to identify an individual. This has been supported by the government in principle.[18] The Issues Paper also sought feedback on whether inferred personal information should be expressly included in the definition of 'personal information' and whether additional protections are required for de-identified, anonymised or pseudonymised information as recommended in the DPI report.[19]

The Issues Paper also sought feedback on whether the Act adequately protects sensitive information and highlighted that the current definition of personal information does not cover information about deceased individuals.

Personal information – technical and inferred information

Does personal information include technical information?

The definition of personal information was always intended to be expansive,[20] but it is somewhat unclear in its application to technical information. It may be possible for technical information to fall outside the definition of personal information on the basis that it does not meet the threshold of being 'about an individual', even if an individual is 'reasonably identifiable' from that information. Whether an individual is 'reasonably identifiable' will depend on an assessment of that information by APP entities in the context in which it is held or released.[21]

As outlined in the Issues Paper, the Act's application to technical information became uncertain following the decision in *Privacy Commissioner v Telstra Corporation Ltd* 2017 FCAFC 4 (Grubb). There it was held that an individual must be the subject matter of the information for it to be 'about an individual' and within the scope of the Act. This was found to involve an evaluative conclusion depending on the facts of the case, to be assessed alone or in conjunction with other available information.[22] This approach raises difficulties for APP entities that may not feel confident in assessing if information is 'about an individual'. Without greater legal clarity as to the meaning of the phrase, APP entities may contend that technical information is not 'about an individual', rather than 'err[ing] on the side of caution' as per the OAIC Guidelines.[23]

The DPI recommendation about coverage of technical information reflects concerns about the coverage of the Act in light of how data is collected across the digital economy. The recommendation supported clarifying that technical information could be covered by the Act because it would align with consumer expectations and provide privacy protection in relation to common data practices of particular concern.[24] These practices include collection of location data,

---

[18] Department of the Treasury, *Regulating in the digital age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Government Response, December 2019) ('Treasury, DPI response') 17.
[19] ACCC, DPI Report (n 2) 476.
[20] Explanatory Memorandum, Privacy Bill 1988 (Cth) 11.
[21] OAIC, Australian Privacy Principles Guidelines (July 2019) [B.91]–[B.94] ('APP Guidelines').
[22] *Privacy Commissioner v Telstra Corporation Ltd* 2017 FCAFC 4 [63]. Note the court was not required to determine if the information was 'personal information' or not, as this was not a ground of appeal.
[23] OAIC, APP Guidelines (n 21) [B.94].
[24] ACCC, DPI Report (n 2) 459–60.

online tracking for targeted advertising purposes, and online platforms sharing data with third parties.[25]

Overseas data protection frameworks more clearly apply to technical information that can be linked to an individual. For example, the GDPR's definition of 'personal data' explicitly includes location data and online identifiers.[26] The California Consumer Privacy Act (CCPA) defines 'personal information' to include online identifiers, IP addresses, account names and similar identifiers.[27] In Canada, the courts have ruled that a broad range of technical information can be 'personal information', including IP addresses, RFID tags, fingerprints, voiceprints and video surveillance.[28] However, New Zealand (NZ) takes a similar approach to Australia and relies on guidance to support compliance with the Act.[29]

Should the definition of personal information be amended to better cover technical information?

Submissions largely supported amending the definition of personal information to more explicitly capture technical information. These submissions spanned sectors, including fintech, academia, IT companies, peak bodies, community legal centres, private citizens and government bodies.[30] This support was based on concerns about identity theft and other harms related to increased proliferation of data.

IDCARE, a not-for-profit that supports victims of identity theft, addressed the issue of personal information and related technical information being sold on the 'dark web'. They specifically mentioned 'digital fingerprints', which are made up of aggregated technical information associated with a website user, such as IP addresses, device identifiers and location data. These fingerprints can uniquely identify website users, although each piece of information alone may not amount to 'personal information'. IDCARE supported broadening the definition of personal information to capture information such as digital fingerprints and to address the cybersecurity risk associated with their misuse.[31]

This issue reflects just part of the identity crime problem in Australia. The Australian Institute of Criminology estimated the direct and indirect cost of identity crime in Australia for 2018-2019 to be $3.1 billion. Out of this broader figure, the estimated direct cost to individuals was $500.5 million, with over 20 per cent of respondents reporting misuse of their personal information at some time during their lives.[32]

Submissions also raised concerns that the current definition of personal information is outdated because data is being handled in new ways and changing notions of 'identity'.[33] Dr Katharine Kemp

---

[25] Ibid 393.

[26] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection)* [2016] OJ L 119/1, art 4(1) ('GDPR').

[27] *California Consumer Privacy Act of 2018*, 1.81.5 Cal Civil Code §§ 1798.140(o)(1) (2020) ('CCPA').

[28] In reference to the definition of personal information in Canada's private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 2 ('*PIPEDA*'). See Office of the Privacy Commissioner of Canada, *Interpretation Bulletin: Personal Information* (Web Page, 2013).

[29] The *Privacy Act 2020* (NZ) s 7 defines personal information as 'information about an identifiable individual,' without any listed types of information captured.

[30] See, eg, Submissions to the Issues Paper: Anonymous 1; Atlassian; AusPayNet; Australian Association of National Advertisers; Australian Society of Archivists; CAIDE and MLS; Financial Services Council; Minderoo Tech and Policy Lab – University of Western Australia; HIV/AIDS Legal Centre; Karen Meohas; Office of the Information Commissioner Queensland; Reset Australia.

[31] Submission to the Issues Paper: IDCARE, 9.

[32] Australian Institute of Criminology, *Statistical Report 29 – National Identity and Security Strategy, 'Identity crime and misuse in Australia 2019* (Report, 2020) vii-ix.

[33] Submissions to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 19; Dr Chris Culnane and Associate Professor Ben Rubinstein, 4; Dr Katharine Kemp, 10; Salinger Privacy, 5.

outlined that the concept of identification should not be limited to data which is labelled with a person's legal name or contact details, but 'should extend to data which can be used to single out one consumer as distinct from other consumers'. Dr Kemp stated that 'the use of strategies which single out unique individuals and create a detailed picture of 'the consumer behind the device' exposes consumers to growing risks of re-identification, manipulation, exclusion and discrimination'.[34]

Salinger Privacy similarly suggested that the Act should cover 'individuation', which they defined as the ability to 'single out a person in the crowd, such that they can be tracked, profiled, targeted, contacted or subject to a decision or action which impacts them, even if that individual's 'identity' is not known'.[35]

The CSIRO elaborated on the scale with which technical data is collected, and how this may pose a privacy risk:

> *Technical datasets are produced when an individual interacts with software, hardware, or services relying on them, either in an online or offline setting. The manner to which an individual interacts with such systems may often be unique to that individual. This issue is compounded by the capability of collecting and retaining data over time, creating a unique pattern for an individual.*[36]

Guidance from the UK's privacy regulator, the Information Commissioner's Office (UK ICO), outlines how the GDPR more clearly captures this technical information and how regulated entities should determine whether information can indirectly identify someone in combination with other available data.[37] For example:

> *An individual's social media 'handle' or username, which may seem anonymous or nonsensical, is still sufficient to identify them as it uniquely identifies that individual. The username is personal data if it distinguishes one individual from another regardless of whether it is possible to link the 'online' identity with a 'real world' named individual*.[38]

Submissions that supported a broadened definition also highlighted the need for APP entities to have greater legal clarity following the Grubb case, and advocated for greater interoperability with foreign privacy laws such as the EU's GDPR. For example, Western Union noted that they work within the boundaries of 135 privacy laws, so a consistent definition would ease the burden of compliance.[39] The Financial Services Council expressed that a more internationally-aligned definition would support consumer protection and business efficacy.[40]

Other submissions did not support covering a greater range of technical information as personal information. These submitters largely considered that technical information which poses a privacy risk is already covered by the definition of 'personal information'. Submitters were also concerned about placing restrictions on the data economy and emerging technology, and the difficulty of defining the broad term 'technical information' in legislation. Telstra was one such submitter who supported maintaining the current definition and expressed that any uncertainty is best dealt with in

[34] Submission to the Issues Paper: Dr Katharine Kemp, 11.
[35] Submission to the Issues Paper: Salinger Privacy, 5. See also Submission to the Issues Paper: Fastmail, 2.
[36] Submission to the Issues Paper: CSIRO, 3.
[37] UK ICO, *Can we identify an individual indirectly from the information we have (together with other available information)?* (Web Page, 2021); with reference to the *Data Protection Act 2018* (UK).
[38] UK ICO, *What are identifiers and related factors?* (Web Page, 2021).
[39] Submission to the Issues Paper: Western Union, 1.
[40] Submission to the Issues Paper: Financial Services Council, 7.

OAIC guidance, 'which can be updated as technology evolves to cover new types of technical information'.[41]

Roche also considered the current definition to be sufficient and well understood, stating that, 'the basic requirement that information be 'about' an individual is a sensible prerequisite to enliven privacy protection for information'.[42] Data Synergies cautioned against including particular 'technical information' in the definition on the basis that 'any inclusion of particular technical information is likely to be unstable and potentially confusing as to coverage, either by inclusion or non-inclusion'.[43]

Others raised concerns about the possible effects of change on business interests and the broader data economy. For example, KPMG stated that 'including metadata or 'data about data' [in the definition of personal information] may blur the line between where an individual's information ends, and an APP entity's proprietary information starts'.[44]

The Federal Chamber of Automotive Industries expressed the need for any amendments to strike the right balance between personal information protection and innovation, citing examples around vehicle-generated data. Noting that the ACCC's concerns about the definition of personal information were based in the practices of digital platforms, they urged 'extreme caution' regarding any change to the definition that would apply across all sectors covered by the Act.[45]

Does personal information include information that has been inferred?

Inferred personal information is information collated from a number of sources which reveals something new about an individual.[46] Personal information can be inferred from other personal information, and/or from information that does not meet the definition of personal information.

Inferred information will meet the definition of 'personal information' if it is 'about an identified individual, or an individual who is reasonably identifiable'. The definition of personal information already contemplates inferences by seeking to cover 'opinions', 'whether true or not' about an individual. However, APP entities may find it difficult to practically determine the point at which the opinions or inferences they generate become personal information.

Requirements under the APPs are enlivened once an APP entity collects personal information for inclusion in a record or generally available publication.[47] The Act does not specify how information can be collected but the OAIC recommends that 'collection' is interpreted broadly to include 'gathering, acquiring or obtaining personal information from any source and by any means'.[48] This would include inferred information. However, this may be unclear to APP entities without clarification in the Act itself.

Should the definition of personal information be amended to better cover inferred personal information?

The DPI recommendation about coverage of inferred information was targeted at addressing consumers' concerns about the use of data analytics, especially where sensitive information is inferred.[49] At the time, ACCC consumer survey results indicated that roughly half of digital platform users considered inferred tastes and preferences to be their personal information.[50] More recently,

---

[41] Submission to the Issues Paper: Telstra Corporation Ltd and Telstra Health Pty Ltd, 6.
[42] Submission to the Issues Paper: Roche, 4.
[43] Submission to the Issues Paper: Data Synergies, 16.
[44] Submission to the Issues Paper: KPMG, 12.
[45] Submission to the Issues Paper: Federal Chamber of Automotive Industries, 9.
[46] See, ACCC, DPI Report (n 2) 460; OAIC, *Guide to data analytics and the APPs* (Web Page, 2018).
[47] *Privacy Act* (n 2) sub-s 6(1) 'collects'. See, eg, *Privacy Act* (n 1) sch 1, APP 3.
[48] OAIC, APP Guidelines (n 21) [B.27].
[49] ACCC, DPI Report (n 2) 36, 479.
[50] Ibid 479.

the 2020 Australian Community Attitudes to Privacy Survey (2020 ACAP Survey) found that 79 per cent of respondents thought that inferring personal information based on their online activity should be considered misuse.[51]

More than half of submitters who addressed the issue of inferred personal information supported amending the definition of personal information to explicitly cover it.[52] In 2008, the Australian Law Reform Commission (ALRC) considered changes in technology when recommending the current definition of personal information,[53] but ultimately concluded that the Act should not provide an unqualified 'right to be let alone'.[54] Several submitters to the Review highlighted that the definition no longer meets public expectations due to advances in technology, particularly in relation to data analytics. For example, Oracle's submission noted that that 'DoubleClick cookies are associated with 1.6 million websites and 75% of the top 100,000 websites on the internet use Google Analytics'.[55] These practices mean that a greater range of information can now result in an individual being targeted or subject to intervention.[56]

Submissions noted that a range of harms can result from inferring personal information.[57] At one end of the scale, inferring personal information can allow companies to personalise advertisements or implement dynamic pricing. At the other end, inferring personal information can facilitate unethical or unlawful practices. For example, a bank could use demographic data to infer a client's ability to repay a loan and offer them a different interest rate based on this information, potentially facilitating discrimination and entrenching historical biases.[58]

A range of submitters echoed these concerns about discrimination and manipulation, including the HIV/AIDS Legal Centre, which highlighted that HIV status can be inferred from data such as an individual's medication purchases, or geolocation of the health services they access.[59]

Submissions that opposed changes in relation to inferred information did so on similar grounds to those that opposed changes to the coverage of technical information. For example, some stated that the current definition is adequate to address privacy harms, especially with further guidance.[60]

Submissions from the technology sector generally opposed greater coverage of inferred information on the basis that it could discourage the use of data analytics or emerging technologies. [61] For example, Microsoft Australia submitted that broadening coverage could result in significant implementation challenges when inferences or predictions are drawn through artificial intelligence or machine learning.[62]

Facebook questioned whether the Act should cover inferred personal information which is not generated by or on behalf of an individual, noting that such insights are only made possible through the company's proprietary data analysis tools.[63] DIGI echoed these views and noted that it is difficult

---

[51] OAIC, *Australian Community Attitudes to Privacy Survey 2020* (Report, September 2020) 36 (*'2020 ACAP Survey'*).
[52] See, eg, Submissions to the Issues Paper: Blancco, 22; New South Wales Council for Civil Liberties, 4.
[53] See, eg, ALRC, *For Your Information: Australian Privacy Law and Practice* (Report No 108, 12 August 2008) [6.28]–[6.35], [6.61] (*'ALRC Report 108'*); ALRC, *For Your Information: Australian Privacy Law and Practice* (Discussion Paper No 72, 12 September 2007) Part B.
[54] ALRC Report 108 (n 53) [6.23], [6.61].
[55] Submission to the Issues Paper: Oracle, 51–2.
[56] Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 8–9; Salinger Privacy, 5, 20.
[57] See, eg, Submission to the Issues Paper: Shaun Chung and Rohan Shukla, 6–8.
[58] Submission to the Issues Paper: Shaun Chung and Rohan Shukla, 7.
[59] Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 9; HIV/AIDS Legal Centre, 2.
[60] See, eg, Submission to the Issues Paper: Telstra Corporation Ltd and Telstra Health Pty Ltd, 7.
[61] See, eg, Submissions to the Issues Paper: Data Republic, 3; United States Chamber of Commerce, 2.
[62] Submission to the Issues Paper: Microsoft Australia, 3.
[63] Submission to the Issues Paper: Facebook, 25.

to determine the point at which point inferences are drawn, and therefore when notice and consent requirements are triggered.[64]

Proposals

Broaden the definition of personal information

In light of the uncertainty about how the definition of 'personal information' applies to technical and inferred information, there is a need for reform. It is important that the definition of personal information is clear enough to provide APP entities with confidence about their obligations under the Act.

The proposed changes reflect aspects of the GDPR's definition of 'personal data'. This is in recognition of the high level of support across sectors for the GDPR definition or otherwise harmonising the Australian definition with GDPR.[65]

2.1-2.3 Overview of the proposed definition of personal information
Amend the definition of personal information to make clear that it includes technical and inferred personal information:

> *Personal information means information or an opinion that relates to an identified individual, or an individual who is reasonably identifiable:*
> *a) whether the information or opinion is true or not; and*
> *b) whether the information or opinion is recorded in a material form or not.*
> *An individual is 'reasonably identifiable' if they are capable of being identified, directly or indirectly.*

This definition would be supported by the following amendments to the Act:

- a non-exhaustive list of the types of information capable of falling within the new definition of personal information
- a list of objective factors to assist APP entities to determine when an individual is reasonably identifiable, and
- a definition of 'collection' that expressly covers inferred information.

Replace 'about' with 'relates to'

This proposed change would:

- capture a greater range of information from which an individual could be identified, particularly technical information
- remove uncertainty associated with the word 'about' following the Grubb case, and
- bring the Act into line with international examples, such as the GDPR.[66]

This proposed change would ensure that information 'related to' an individual would be captured by the definition where there is a risk of identification, even if the information is primarily about something else – such as the individual's telecommunications use. This change would capture a broader range of technical information without fundamentally changing the structure of the definition.

This change would also bring the Privacy Act's definition of personal information into line with other Commonwealth legislation that uses 'relating to' when seeking to regulate information on privacy

[64] Submission to the Issues Paper: DIGI, 6.
[65] Submissions to the Issues Paper: Australian Communications Consumer Action Network, 8; Atlassian, 3; Blancco, 23; Minderoo Tech & Policy Lab – University of Western Australia Law School, 6; New South Wales Information and Privacy Commission, 2.
[66] GDPR (n 26) art 4. Note that although this would diverge from Canada and NZ, their courts have adopted more expansive interpretations of 'about'. See, eg, Submission to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 14.

grounds. For example, the phrase 'relating to' is used in the definition of 'COVID app data' in Part VIIIA of the Act (regarding public health contact information) to capture a broad range of information with respect to the operation of the COVIDSafe contact tracing application. The phrase 'relates to' is also used to define key terms in the Consumer Data Right (CDR) legislation, and the *Telecommunications (Interception and Access) Act 1979* (TIA Act).[67]

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

Include a non-exhaustive list of technical information that is personal information within the Act

The Act could list examples of technical information that could be capable of falling within the definition of ***personal information***. These could include:

- an identifier such as a name
- an identification number
- location data
- an online identifier, or
- one or more factors specific to the physical, physiological, genetic, mental, behavioural (including predictions of behaviours or preferences), economic, cultural or social identity or characteristics of that person.[68]

The definition would cover circumstances in which an individual is distinguished from others or has a profile associated with a pseudonym or identifier, despite not being named.

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

Clarify the circumstances in which an individual is 'reasonably identifiable'

An additional definition could be added to the Act outlining that an individual will be 'reasonably identifiable' if an APP entity or a third party could directly or indirectly identify anyone from that information.

Including the phrase 'directly or indirectly' would make it clearer to APP entities that they should consider other information available when assessing whether information is personal information,[69] including publicly available information where there is a risk that the information could be made public.

This definition could be supported by guidance that draws upon international case law and guidance. For example, in the UK, information is considered 'identifiable' if a motivated intruder could identify someone from it, including by linking it with other information.[70] In Canada, it has been held that information is 'identifiable' if there is a *serious possibility* of someone being identified from it.[71]

The new definition could be supported by providing a list of objective factors to help APP entities assess whether an individual is 'reasonably identifiable'.[72] These factors could include the context in which the information is to be held or released, the costs and amount of time required for

---

[67] *Competition and Consumer Act 2010* (Cth) s 56AI ('*CCA*'); Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, 1.106; *Telecommunications (Interception and Access) Act 1979* (Cth) s 187LA *('TIA Act')*.

[68] This aspect of the definition draws from examples in the GDPR (n 26) art 4(1), rec 30.

[69] Submission to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 18; UK ICO, *Can we identify an individual indirectly from the information we have (together with other available information)?* (n 37).

[70] UK ICO, Anonymisation: managing data protection risk code of practice, (Web Page, 2021), 22. Note this Code is still used as a guide to interpret the GDPR, despite being made under the *Data Protection Act 1998* (UK) and *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* [1995] OJ L 281.31, 23.11.1995.

[71] See, eg, *Gordon v Canada (Health)* 2008 FC 258, [34]; See also for the EU approach, *Patrick Breyer v Bundesrepublik Deutschland* (European Court of Justice, C-582/14, 19 October 2016), ECLI:EU:C:2016:77.

[72] See, eg, Submission to the Issues Paper: Karen Meohas, 8.

identification, and available technology.[73] The definition would not capture information where there is only an extremely remote or hypothetical risk of identification.[74]

As the term 'reasonably identifiable' is also used when assessing whether information is 'de-identified' under the Act, this change would also affect how APP entities assess whether information is de-identified or anonymised. Information would need to *no longer be related to an identified or reasonably identifiable individual*, considering the above definition, for the Act to no longer apply.[75]

This proposal responds to concerns of APP entities who wanted a clearer definition and greater coverage of online identifiers, while avoiding an overly broad definition that fails to consider context.[76] The definition would reflect how 'identifiable' has been interpreted in other jurisdictions and support interoperability.[77]

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.

Define 'collection' to clearly cover inferred information

The definition of *collection* could be amended to mean *'*gathering, acquiring, inferring or obtaining personal information from any source and by any means.'

This will cover circumstances where an APP entity infers, derives, generates or otherwise creates personal information, whether or not this is done by or on behalf of an individual, and assist APP entities to more clearly understand and comply with their obligations. This approach was recommended by the OAIC and reflects current OAIC guidelines.[78]

The Australian Information Security Association suggested a different approach, recommending replacing the concepts of 'collection,' 'use' and 'disclosure' with a broader concept of 'data processing' to remedy issues around notice and consent requirements for inferred personal information.[79] This proposal would require a broad re-conceptualisation of the Australian privacy framework so has not been adopted in these proposals. However, the potential to introduce a 'controller/processor distinction' within the Australian framework is discussed later in Chapter 21.

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

Questions

- In practice, what types of information would the proposed definition of personal information capture which are not presently covered?
- What do APP entities estimate are the costs and benefits of amending the definition of personal information in the manner suggested?
- Would the proposed definition of personal information pose any unintended consequences for APP entities? How could these be mitigated?

[73] See GDPR (n 26) art 4, rec 26.
[74] See UK ICO, *Can we identify an individual indirectly from the information we have (together with other available information)?* (n 37).
[75] See *Privacy Act* (n 2) sub-s 6(1).
[76] See, eg, Submissions to the Issues Paper: Australian Department of Health, 3; Australian Institute of Health and Welfare, 2-3; Communications Alliance, 5; Department of Veterans' Affairs, 8; MyCRA Lawyers, 1; Queensland Law Society, 2; Roche, 5.
[77] See, eg, *Gordon v Canada (Health)* (n 71) [34]; UK ICO, *What are identifiers and related factors?* (n 38), cited in Submission to the Issues Paper: Dr Katharine Kemp, 10.
[78] Submissions to the Issues Paper: OAIC, 12; OAIC, APP Guidelines (n 21) B.27. See also Submissions to the Issues Paper: Australian Privacy Foundation, 11; Salinger Privacy, 5.
[79] Submission to the Issues Paper: Australian Information Security Association, 8, 19.

- Would the proposed definition of collection have any unintended consequences for APP entities? How could these be mitigated?

De-identified, anonymised and pseudonymised information

When is personal information de-identified?

Personal information is 'de-identified' if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.[80] Once information is de-identified, it is no longer personal information, so the Act no longer applies.

Under APP 11.2, APP entities must take reasonable steps to destroy or to ensure that personal information is de-identified once they no longer need it for any purpose. Under APP 2, APP entities generally must also give individuals the option to not identify themselves or to use a pseudonym.

To support robust de-identification practices and the management of re-identification risks, the OAIC and CSIRO's Data61 released a non-binding De-identification Decision-Making Framework in 2017.[81]

Figure 2.1: Diagram summarising the 10 components of the De-Identification Decision-Making Framework

Image reproduced from OAIC/Data 61, the De-Identification Decision-Making Framework (n 81), xi.

The framework is a standalone guide to de-identification that can help APP entities to evaluate their data situation, and put in place controls to manage identification risks.

The framework covers both technical and situational ways to manage identification risks and emphasises that after de-identification, the risk of identification generally cannot be reduced to zero.

The OAIC's guidelines on de-identification also encourage APP entities to consider the APPs which relate to use and disclosure, overseas transfers, and information security to mitigate any remaining privacy risks when handling de-identified information (APPs 6, 8 and 11).[82]

The ACCC's DPI report recommended that the government examine how the Act deals with de-identified information, and to consider 'whether there should be protections or standards for de-identification, anonymisation and pseudonymisation of personal information to address the growing risks of re-identification as data sets are combined and data analytics technologies become more advanced'.[83]

Are additional protections required for this type of information?

Submitters were split on whether they supported additional protections, and what form these should take. Those who supported some form of additional protections came from government,

[80] *Privacy Act* (n 2) sub-s 6(1).
[81] CM O'Keefe, S Otorepec, M Elliot, E Mackey, and K O'Hara, *The De-identification Decision-Making Framework* (CSIRO Reports EP173122 and EP175702, 18 September 2017).
[82] OAIC, *De-identification and the Privacy Act* (Web Page, 28 March 2018).
[83] ACCC, DPI Report (n 2) 36, 476.

academia, consumer groups, the technology sector and other large businesses.[84] These submissions generally reinforced the ACCC's observations about the increased risk of re-identification due to the amount of data in circulation, facilitated by advances in technology.[85]

One of the most common methods suggested to increase the level of protection was to require information to be anonymised instead of de-identified before the Act no longer applies.[86] Anonymisation is the process of irreversibly treating data so that no individual can be identified, *including by the holders of the data*.[87] Submissions also highlighted some confusion about whether the definition of 'de-identified' covers information that is pseudonymised but able to be re-identified by certain people. [88]

Other submitters were concerned that replacing de-identification with anonymisation or regulating de-identified information would put in place an unworkably high standard,[89] encourage APP entities to instead hold information in an identified form,[90] or have unforeseen consequences on research and medical use of data.[91]

Submitters were generally supportive of the De-Identification Decision-Making Framework, with a few submitters proposing they be mandatory for all APP entities, or at least for high-risk APP entities.[92] Others requested further guidance on de-identification requirements.[93]

Submissions that did not support any changes to the standard of 'de-identification' considered that the current standard strikes the right balance between managing privacy risk, and the use of de-identified information for purposes that benefit the community.[94] Some stated that current market forces are sufficient to encourage best practice de-identification techniques.[95]

Proposals

Require information to be anonymous before the Act no longer applies

The Act could be amended to require information to be 'anonymous' rather than 'de-identified' for the Act to no longer apply.

Under this proposal, the definition of 'de-identification' would be removed and a definition of 'anonymous information' inserted. This reflects the proposed changes to definition of personal information in Proposals 2.1-2.3. If the definition of personal information is expanded then understandably more will need to be done to 'de-identify' that information so it falls outside that definition. The word 'anonymous' could more clearly signal to APP entities that they are required to meet the higher, irreversible standard reflected by this term.

---

[84] See, eg, Submissions to the Issues Paper: Australian Communications Consumer Action Network; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law; AusPayNet; Blancco; Deloitte; Department of Veterans' Affairs; OAIC (Recommendations 8–12); Optus.
[85] See, eg, Submission to the Issues Paper: Dr Katharine Kemp, 9.
[86] See, eg, Submissions to the Issues Paper: IDCARE, 8; Australian Privacy Foundation, 11–12; Australian Information Security Association, 8; Legal Aid Queensland, 3; Data Synergies, 18–21; Dr James Scheibner and Dianne Nicol, 5; Consumer Policy Research Centre, 5. See also Submission to the Issues Paper: Blancco, 22–3.
[87] European Commission, *What is personal data* (Web Page, 2020); GDPR (n 26) rec 26.
[88] Submission to the Issues Paper: OAIC, 33. See also Submission to the Issues Paper: Optus.
[89] Submissions to the Issues Paper: ANZ, 11; Australian Banking Association, 3–4; WA Department of Health, 2.
[90] Submissions to the Issues Paper: US Chamber of Commerce, 2; Palo Alto Networks, 2–3; Information Technology Industry Council, 2.
[91] Submissions to the Issues Paper: Telstra Corporation Ltd and Telstra Health Pty Ltd, 7; Australian Institute of Health and Welfare, 3.
[92] Submission to the Issues Paper: SuperChoice, 2.
[93] Submissions to the Issues Paper: SBS, 5; Data Republic, 4.
[94] Submission to the Issues Paper: Federal Chamber of Automotive Industries, 9.
[95] Submission to the Issues Paper: CrowdStrike, 2.

Information would be considered 'anonymous' if it were no longer possible to identify someone from the information, considering the definition of 'reasonably identifiable' and the factors outlined in Proposal 2.3. This reform would not impose an absolute or unworkably high standard on APP entities that use data for research or service delivery. Information could be considered anonymous provided that the risk of re-identification was extremely remote or hypothetical.

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

Introduce penalties for malicious re-identification of information

In 2016, the Privacy Amendment (Re-identification Offence) Bill was introduced to Parliament. The purpose of the Bill was to deter the re-identification of publicly-released data sets and support the government's Public Data Policy Statement, which recommended that non-sensitive government data be made 'open by default'.[96]

The Bill proposed to introduce criminal and civil penalties into the Act for re-identification of de-identified information released by Commonwealth agencies. The general re-identification offence was supported by other provisions. For example, the Bill sought to prohibit the onwards disclosure of re-identified information, and included requirements to notify the responsible agency of re-identification and to comply with directions of that agency.[97] The Bill also contained exemptions to ensure APP entities would not be criminally accountable for re-identification in certain circumstances.[98]

In February 2017, the Senate Standing Committee on Legal and Constitutional Affairs released its report on the 2016 version of the Re-identification Offence Bill.[99] The Committee report recommended that the Bill be passed, stating that it provided a necessary and proportionate response to gaps in privacy coverage, and balanced this with the need to promote open data.[100] The dissenting report of the Australian Labor Party and Australian Greens recommended that the Bill not be passed on the basis it did not provide a proportionate, holistic response to de-identification issues.[101] The Bill lapsed in 2019.[102] Since the introduction of the Bill, a re-identification offence has been introduced in the United Kingdom. To date there have been no prosecutions.[103]

Re-introducing this Bill, with appropriate amendments to support the Review's reforms and address concerns raised by the Senate Committee, could be a useful tool to support the broader change to anonymisation. While anonymisation would mitigate privacy risk before information is publicly released, this offence could address concerns about malicious re-identification of information that has already been publicly released.

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

---

[96] Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Privacy (Re-Identification) Offence Bill 2016* (Report, February 2017) 1.3 ('*Re-identification Offence Bill Report*'); Department of the Prime Minister and Cabinet, *Australian Government Public Data Policy Statement* (Web Page, 7 December 2015).
[97] Privacy Amendment (Re-Identification Offence) Bill 2016 (Cth) cls 16E–16F.
[98] Ibid cls 16D(2) –(5).
[99] Re-identification Offence Bill Report (n 96).
[100] Ibid 2.48, 2.51.
[101] Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Privacy (Re-Identification) Offence Bill 2016* (Dissenting Report of the Australian Labor Party and the Australian Greens, February 2017) [1.1]–[1.2].
[102] Parliament of Australia, *Bills and Legislation: Privacy Amendment (Re-identification Offence) Bill 2016* (Web Page, 2016).
[103] See *Data Protection Act 2018* (UK) (n 37) s 171.

Information about deceased individuals

The Act only applies to information about living, natural persons.[104] Exceptions apply where the same information is also about a living person (for example, where information indicates the presence of an inherited disease in relatives). This approach is consistent with the international instruments upon which the Act is based.[105] Some Australian states and territories regulate information about deceased individuals.[106] In 2008, the ALRC recommended the Act be extended to cover information about the deceased.[107]

Should the Act cover information related to deceased individuals?

This issue was addressed by a small number of submissions, which were roughly split on whether the Act should be extended. These submissions primarily came from government, health and insurance bodies.[108]

Submissions in favour of extending the Act to the deceased cited the need for a respectful and appropriate framework to deal with information after death, given the impact that inappropriate disclosure can have on families and associates of the deceased. This was identified as particularly significant for certain cultural groups, including Aboriginal and Torres Strait Islander people.[109] The OAIC supported extending the Act to the deceased, stating that a recent New South Wales Law Reform Commission report on access to digital records upon death or incapacity should '…inform the development of a framework for asserting the privacy of deceased individuals under the Privacy Act'.[110]

Submitters against extending the Act to the deceased cited more diverse concerns, including the potential to hamper the ability of credit reporting bodies to prevent fraud, to negatively affect freedom of expression or to impede medico-legal processes such as coronial inquests.[111]

Both submissions for and against coverage emphasised the need for a less complex and nationally consistent approach, particularly in the healthcare context.[112]

Submissions also emphasised the need to consider broader legal frameworks. For example, the Department of Veterans' Affairs welcomed further discussion on whether the Act should apply to the deceased, but noted that 'consideration of this issue would also require a discussion about legal duties of confidence that arise in equity, contract or at common law, specifically around the applicability of material obtained or given in confidence'.[113]

Given the interaction of this issue with state and territory legislation, wills and probate law, trusts law, criminal offences, contract law and duties of confidence, any consideration of extending privacy protections to those of deceased individuals should not be looked at in isolation.

---

[104] *Privacy Act* (n 2) sub-s 6(1); *Acts Interpretation Act 1901* (Cth) s 2B.
[105] See, eg, Organisation for Economic Co-operation and Development, *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, 2013 [6]; International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.
[106] See, eg, *Privacy and Personal Information Protection Act 1998* (NSW) sub-s 4(3)(a); *Information Act 2002* (NT) s 4.
[107] ALRC Report 108 (n 53) 377.
[108] See, eg, Submissions to the Issues Paper: Australian Department of Health; Department of Veterans' Affairs; Avant Mutual; Records and Information Management Professionals Australasia; RACGP; Ramsay Health Care.
[109] Submission to the Issues Paper: Records and Information Management Professionals Australasia, 4.
[110] Submission to the Issues Paper: OAIC, 36, discussing New South Wales Law Reform Commission, *Access to digital records upon death or incapacity* (Report No 147, December 2019) 74; See also AGD, Council of Attorneys-General Communiqué (Web Page, 27 July 2020).
[111] Submissions to the Issues Paper: Australian Retail Credit Association, 8; Nine, 9; MIGA, 5; Department of Health of Western Australia, 2.
[112] Submissions to the Issues Paper: Australian Medical Association, 3–4; Avant Mutual, 5; RACGP, 2.
[113] Submission to the Issues Paper: Department of Veterans' Affairs, 18–19.

Definition of sensitive information

Categories of sensitive information are contained in subsection 6(1) of the Act and were derived from the special categories outlined by the GDPR's predecessor, the EU Data Protection Directive.[114] The categories have since been expanded to include genetic information, biometric information and biometric templates in response to recommendations in two ALRC reports.[115]

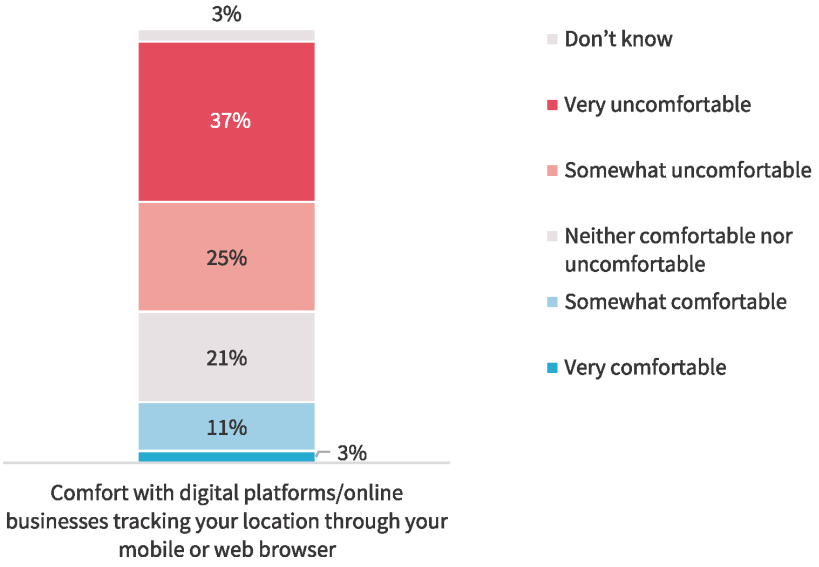
Sensitive information is subject to a number of additional protections in the Act. In particular, sensitive information may only be collected with consent unless an exception applies, and more stringent requirements apply to its use or disclosure.

Does 'sensitive information' require updating?

A small number of submissions addressed whether the categories of sensitive information require updating. While the majority sought to retain the categories of sensitive information or to alter them slightly to maximise interoperability with international frameworks,[116] there may be areas that warrant further consideration or guidance. These areas include location, financial, health, genomic and biometric information.

Although it did not recommend changing the categories of sensitive information, the OAIC pointed out the intrusive nature of location information, noting that it can reveal other sensitive attributes such as information about health or religious beliefs.[117] Oracle's submission examined how businesses currently use location information, noting that Google's default settings on Android's Google Location Services are set to 'high accuracy' – increasing the potentially intrusive nature of this information.[118] The 2020 ACAP Survey indicated that 62 per cent of respondents felt uncomfortable about digital platforms and other online businesses tracking their location.[119]

Figure 2.2: Graph from the 2020 ACAP Survey – 'Australians' comfort with businesses tracking location'



A16. How comfortable are you with each of the following data practices? Base: Australians 18+ (n=1510)

Image reproduced from OAIC, 2020 ACAP Survey (n 51), 79 (Figure 57).

[114] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 49.
[115] *Privacy Legislation Amendment Act 2006* (Cth) s 3; *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) s 41; ALRC, *Essentially Yours: The Protection of Human Genetic Information in Australia* (Report No 96, May 2003); ALRC Report 108 (n 53).
[116] Submission to the Issues Paper: Australian Information Security Association, 19.
[117] Submission to the Issues Paper: OAIC, 42.
[118] Submission to the Issues Paper: Oracle, 42–3.
[119] OAIC, 2020 ACAP Survey (n 51).

Internationally, privacy legislation is beginning to recognise how intrusive location information can be. Consumers' precise geolocation has recently been designated as sensitive information by the California Privacy Rights Act (CPRA), which will come into effect in 2023.[120]

Financial information, particularly transactional data were also highlighted as sensitive throughout submissions. This is because, like location, sensitive information is easily inferred from financial data. For example, a transaction history featuring clothes shopping or other purchases may strongly indicate gender, and subscriptions to union or political organisations could indicate political opinions.[121] As with location information, financial account information and access credentials will be explicitly covered as sensitive information by the CPRA.[122]

Currently, the Act does not address how personal information like location and transactional data can be used as a proxy for sensitive information. However, OAIC guidelines state that personal information may be sensitive if it clearly implies a category of sensitive information.[123] The Castan Centre for Human Rights Law suggested that the definition of sensitive information should be explicitly amended to include information that acts as proxies for sensitive information, because such proxies may be used as a basis for discrimination.[124]

Some submissions called for greater clarity about how biometric information and biometric templates are treated under the Act, particularly with reference to video surveillance and use of facial recognition in public where individuals may not be 'reasonably identifiable'.[125] Submissions also expressed confusion about how the term 'biometric information' may apply to recent technological changes such as gait recognition, and mouse use or typing recognition.[126]

Biometric information is also coming under increased scrutiny worldwide, as high-profile examples come to light. For example, the OAIC and the UK ICO recently launched a joint investigation into Clearview AI's facial recognition app, which allowed users to upload a photo of an individual and match it to a database that reportedly contains over 3 billion images collected or 'scraped' from the internet.[127] The Australian Human Rights Commission's (AHRC) recent Human Rights and Technology project examined the human rights implications of biometric technologies, especially facial recognition.[128] Specific biometric privacy laws are also emerging in a number of US states, including New York, Illinois and Washington.[129]

The Australian Department of Health noted uncertainties about how the definition of health information (and therefore sensitive information) applies to genomic information.[130] While these concerns are likely to be addressed by Proposals 2.1-2.3, they also identified a further issue where genetic information is collected for purposes other than healthcare, providing an example about commercial genetic tests that are offered to people researching their family histories:

---

[120] *California Privacy Rights Act of 2020* § 14, inserting a new § 1798.140 (ae) into 1.81.5 Cal Civil Code, (*'CPRA'*). This amendment will rename and amend aspects of the CCPA, commencing 2023. See also IAPP, *The California Privacy Rights Act of 2020* (Web Page, 2020).
[121] Submission to the Issues Paper: AusPayNet, 4.
[122] *CPRA* (n 120) § 1798.140 (ae).
[123] OAIC, APP Guidelines (n 21) [B.139].
[124] Submission to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 19.
[125] Submissions to the Issues Paper: KPMG, 12; Royal Australian College of General Practitioners, 2; Shopping Centre Council of Australia, 1.
[126] Submission to the Issues Paper: ANZ, 9.
[127] OAIC, *OAIC and UK's ICO open joint investigation into Clearview AI Inc* (Web Page, 9 July 2020).
[128] See AHRC, *Human Rights and Technology Final Report* (Report, 2021) 111 (*'AHRC report'*); Parliament of Australia – Parliamentary Joint Committee on Intelligence and Security, Advisory report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019 (Report, October 2019).
[129] *SHIELD Act*, N.Y. Gen Bus. Law § 899-bb (2020); New York Assembly Bill A27; Biometric Information Privacy Act 2008 (BIPA) 740 ILCS 14/15; Biometric Information Privacy Act, Rev Code WA §§ 19.975.010–19.375.900.
[130] Submission to the Issues Paper: Australian Department of Health, 3 (Attachment 1).

> *Potentially, unregulated provision of direct to consumer genetic testing services could …lead to the inappropriate disclosure of personal genomic information to third parties… Those direct to consumer genetic testing companies offering health and wellness related services could argue that they do not provide a 'health service' under s 6FA(a)(iii) of the Act*.[131]

Finally, a small number of submissions suggested removing the distinction between sensitive information and personal information entirely, and that the standard of protection afforded to sensitive information should be extended to all personal information.[132] Although the *Privacy Act 2020* (NZ) takes a similar approach, this was not a widely-supported view.[133]

In light of the preceding discussion, the Review is seeking further feedback about whether reform proposals are needed to update 'sensitive information' in the Act.

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'?

[131] Submission to the Issues Paper: Australian Department of Health, 3 (Attachment 1).
[132] Submission to the Issues Paper: Digital Rights Watch, 3.
[133] *Privacy Act 2020* (NZ) (n 29) s 7.

3. Flexibility of the APPs

The Issues Paper sought feedback on whether the framework of the Act is effective in providing flexibility to cater for a wide variety of entities, acts and practices with sufficient clarity about protections and obligations. There was a high level of stakeholder engagement with these issues, with submissions from private sector entities, consumer advocates, academics and public sector agencies. Submitters generally expressed support for the existing principles-based framework.[134]

Scalability of the APPs

The APPs enable personal information to be collected, used and disclosed where it is 'reasonably necessary' for (or for agencies, directly related to) one or more of the entity's functions or activities. This is an objective test, and it is the responsibility of an APP entity to justify that a particular collection, use or disclosure is reasonably necessary. A large number of submitters expressed support for this approach and noted that the current framework allows the APPs to be scalable to entities of various sizes and capabilities and to be adapted to different acts and practices of those entities.[135]

Submissions also acknowledged that the current framework provides limited opportunities for the APPs to prescribe specific requirements or treatments in relation to certain classes of entities, personal information, or acts and practices. A number of submissions considered that the protections and obligations under the Act should be clarified through greater prescription and referred to the GDPR as a possible model.[136] However, the general view among submitters was that flexibility is a key benefit of the APPs and that a more prescriptive approach would increase the regulatory burden for businesses and limit the effectiveness of the Act in protecting the privacy of individuals. Submitters were particularly supportive of the APPs remaining industry and technology neutral and suggested that where needed, greater prescription was better placed in a code or other guidance.[137] A number of submissions expressed support for the APP Guidelines providing greater clarity on how entities should interpret and apply the APPs.

Proposal – Improve the OAIC's ability to make codes

Submissions supported the use of codes to prescribe how the APPs should apply to specific industries, and to provide greater certainty to entities about how to comply with their obligations in specific circumstances.[138] The IC can develop an APP code if the IC considers that it is in the public interest to do so. However, the IC must first request an industry code developer to develop an APP

---

[134] Submissions to the Issues Paper: Crowdstrike, 3; Cyber Security Cooperative Research Centre, 6; Office of the Victorian Information Commissioner, 1; Ai Group, 8; Telstra, 2; Experian, 6; Google, 4; AusPayNet, 5; Ground Up, 5; Optus, 4; Law Council of Australia, 12; Royal Australian College of General Practitioners, 2; Australian Medical Association, 4; Federal Chamber of Automotive Industries, 8; Facebook, 27; Insurance Council of Australia, 3; Interactive Games and Entertainment Association, 9; ID Exchange, 9; Australian Banking Association, 4; Australian Department of Health, 4; Free TV Australia, 5; OAIC, 37.

[135] Submissions to the Issues Paper: Crowdstrike, 3; Cyber Security Cooperative Research Centre, 6; Office of the Victorian Information Commissioner, 1; Ai Group, 8; Telstra, 2; Experian, 6; Google, 4; AusPayNet, 5; Ground Up, 5; Optus, 4; Law Council of Australia, 12; Royal Australian College of General Practitioners, 2; Australian Medical Association, 4; Facebook, 27; Insurance Council of Australia, 3; Interactive Games and Entertainment Association, 9; ID Exchange, 9; Australian Banking Association, 4; Australian Department of Health, 4; Free TV Australia, 5; OAIC, 37.

[136] Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre, Financial Counselling Australia (joint submission), 11; Data Republic, 4; Legal Aid Queensland, 3; Griffith University, 6; Centre for Cyber Security Research and Innovation, 6; Australian Information Security Association, 9; Dr Kate Mathews Hunt, 5.

[137] Submissions to the Issues Paper: Google, 4; Law Council of Australia, 12; Interactive Games and Entertainment Association, 9; Australian Banking Association, 4; Free TV Australia, 5; OAIC, 37.

[138] Submissions to the Issues Paper: Records and Information Management Professionals Australasia, 4; AusPayNet, 5; Law Council of Australia, 12; Facebook, 27; Interactive Games and Entertainment Association, 9.

code and only if the request is not complied with, or the IC decides not to register the APP code that has been developed, may the IC develop and register an APP code.[139]

The factors that are to be taken into account by the IC in identifying an appropriate code developer include whether an entity, group of entities, or association or body has the capacity to develop a code, including whether they have the resources and expertise and whether the entity is generally representative of the entities in the sector or industry to which the code will apply.[140] The OAIC's submission notes that in certain circumstances, it is challenging to identify an appropriate entity or group of entities that meet these criteria.[141] For example, it may be necessary to develop a code to cover a particular activity that is being engaged in across a broad sector of the economy. In these circumstances it may be difficult to identify a code developer that is generally representative of the entities to be covered by the code. It may also be challenging to identify a developer with adequate resources and expertise to develop a code.[142]

Allowing the IC to make APP codes on the direction or approval of the Attorney-General would allow codes to be made more quickly and efficiently in some circumstances. Relevant industries and entities affected by an APP code to be made by the IC would be provided with sufficient opportunity to provide input into the code. Enhancing the ability for the IC to make codes would also provide individuals and entities greater clarity about the application and interpretation of the APPs for specific issues and industries.

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.

The OAIC's submission also expressed concern about the application of the existing APP code provisions in situations where an APP code needs to be developed as a matter of urgency.[143] The OAIC considered that, in urgent circumstances, it would be beneficial if the IC had the ability to expeditiously issue a temporary APP code where there was a clear public interest in doing so.[144] Allowing the IC to implement temporary codes would be consistent with the recent amendments to the NZ Privacy Act, which enable the NZ Privacy Commissioner to temporarily issue, amend or revoke a privacy code of practice in urgent circumstances where it is impracticable to follow the regular code-making procedures.[145]

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.

Emergency Declarations

Part VIA of the Act makes special provision for the collection, use and disclosure of personal information in emergencies and disasters.[146] While the Act contains other provisions which afford APP entities some flexibility in an emergency or disaster situation,[147] Part VIA was introduced in recognition of the practical difficulty in applying those provisions with confidence in crises involving

[139] Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012, 4.
[140] OAIC, *Guidelines for developing codes* (Web Page, September 2013).
[141] Submission to the Issues Paper: OAIC, 39.
[142] Ibid.
[143] Ibid.
[144] Ibid, 40.
[145] *Privacy Act 2020* (NZ) (n 29) s 34.
[146] *Privacy Act* (n 2) s 80F.
[147] See ibid s 16A.

mass casualties and missing persons, due to uncertainty as to the extent of their application.[148] Emergency Declarations under the Act have been made three times – in response to the Victorian bushfires in 2009, the floods in New South Wales and Queensland in 2011 and the bushfires across Australia in 2019/2020.[149]

The Attorney-General or Prime Minister can make an Emergency Declaration (ED) if they are satisfied that an emergency or disaster has occurred, it is of national significance and it has affected one or more Australian citizens.[150] An ED may also be made in relation to events outside Australia if additional conditions are met.[151] Once an ED is made, an entity may collect, use or disclose personal information relating to an individual if the entity believes the individual may be involved in the disaster, the handling of the personal information is for a permitted purpose in relation to the disaster and the disclosure is to an entity of a relevant class.[152] It is an offence to subsequently disclose personal information received as a result of a disclosure under an ED unless the entity complies with the APPs or the ED provisions.[153]

Proposals

Amend the Act to allow for more targeted EDs

Once an ED is made, it applies to all organisations and agencies covered by the Act, and allows for wide sharing of personal information so long as it relates to the declared emergency or disaster. When deciding whether or not to make an ED, a relevant consideration is whether the need to effectively respond to the emergency outweighs the need for the privacy protections that would ordinarily apply. The Australian Department of Health noted that greater flexibility in the application of the authorisations to share personal information, as determined by the Attorney-General or Prime Minister, would improve the balance between the need to protect the privacy of individuals and the need to share personal information to efficiently and effectively respond to emergencies and disasters.[154] The ED provisions could be amended so that an ED can be more specific and targeted about how information can be collected, used and disclosed when responding to an emergency. This could improve the use of the provisions.

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.

Allow organisations to disclose personal information to state and territory authorities

While Commonwealth agencies are authorised to disclose personal information to state and territory agencies, organisations cannot rely on the provisions of an ED to make disclosures to state and territory agencies. A number of submissions considered that it would be beneficial if private sector organisations could share personal information to states and territories in a similar way.[155]

---

[148] Explanatory Memorandum, Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006.
[149] *Emergency (Victorian bushfires) Declaration 2009 (No. 1); Emergency (Queensland and New South Wales floods) Declaration 2011 (No. 1); Privacy (Australian Bushfires Disaster) Emergency Declaration (No. 1) 2020*.
[150] *Privacy Act* (n 2) s 80J. An ED may also be made by the Prime Minister or Minister if a 'national emergency declaration' is in force and the Prime Minister or Minister is satisfied that the emergency is of a kind that is appropriate for an ED to apply – s 80J(2) Privacy Act, as inserted by the *National Emergency Declaration (Consequential Amendments) Act 2020*.
[151] Ibid s 80K.
[152] Relevant classes of entities are listed in section 80P. Permissible classes differ for agencies and organisations.
[153] *Privacy Act* (n 2) s 80Q – there are limited other exceptions that authorise disclosure.
[154] Submission to the Issues Paper: Australian Department of Health, 9.
[155] Submissions to the Issues Paper: Australian Department of Health, 9; Ramsay Australia, 7; Department of Health Western Australia, 8; ANZ, 13.

However, while the OAIC would be able to oversee the acts and practices of an organisation under an ED, they would not have the ability to oversee the activities of the states and territories who receive and use the information. Accordingly, it may be necessary to implement additional safeguards that could apply to the handling of personal information disclosed to states and territories under an ED alongside changes to allow organisations to make such disclosures.

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

Question

- What additional safeguards should be put in place to allow organisations to disclose personal information to states and territories under an Emergency Declaration?

4. Small business exemption

Subject to a number of exceptions, the Act does not apply to businesses with an annual turnover of less than $3 million. The Issues Paper sought feedback on whether the current scope of the Act strikes the right balance between protecting the privacy rights of individuals and imposing unnecessary regulation on small businesses.

There was a high level of interest in the issue, with the Review receiving submissions from a diverse range of stakeholders including government agencies, academics, research centres, private sector organisations and consumer advocates. Submissions noted that advances in technology have shifted the way small businesses operate and increased the privacy risk they pose.[156]

While a number of submitters supported the rationale for the exemption in seeking to reduce compliance costs for small businesses, they highlighted the privacy risks and other costs resulting from the limited scope of the Act.[157] Small business representatives acknowledged the importance of small businesses protecting individuals' privacy but were opposed to the exemption being removed.[158] One submission proposed increasing the turnover threshold to $7.5 million.[159]
A number of small business representatives supported increasing the threshold to $10 million[160] consistent with the small business threshold used by the Australian Taxation Office.[161]

The Issues Paper also sought feedback on the appropriateness of the consent provisions contained in section 6D, which allow small businesses that trade in personal information to be exempt from the Act if they gain the consent of individuals to collect or disclose their personal information. The submissions that addressed this issue considered that the consent provisions should be removed.[162]

The changing nature of business

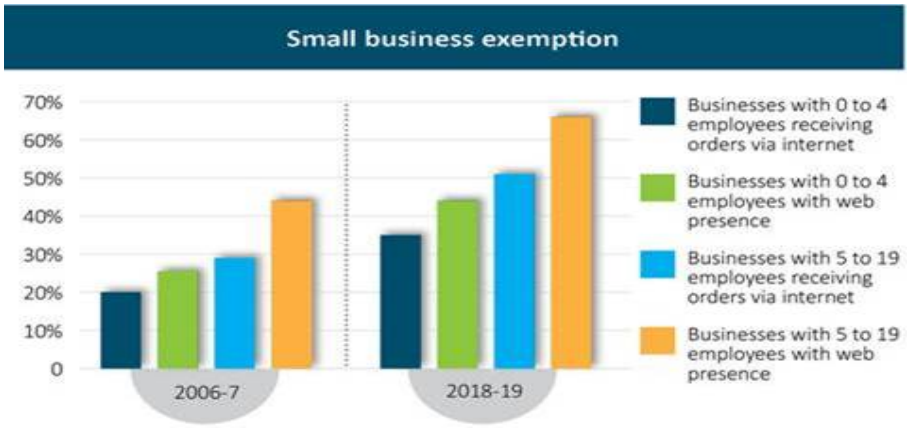
As at 30 June 2019, less than 5 per cent of the 2,375,753 businesses actively trading in the Australian economy had an annual turnover of more than $3 million.[163] Submissions that supported the Act applying to small business considered that the protection of an individual's privacy should not depend on the size of the entity they are dealing with,[164] and that annual turnover is not an accurate

[156] Submissions to the Issues Paper: New South Wales Information and Privacy Commission, 2; Salinger Privacy, 10; elevenM, 2; Calabash Solutions, 5; Centre for Media Transition, University of Technology Sydney, 10; Consumer Policy Research Centre, 4; Australian Communications Consumer Action Network, 9; Institute for Cyber Investigations and Forensics, University of the Sunshine Coast, 2; Office of the Victorian Information Commissioner, 4; Minderoo Tech and Policy Lab, University of Western Australia Law School, 29; Association for Data-driven Marketing and Advertising, 13; Superchoice, 2; Queensland Law Society, 2; OAIC, 59; Gadens, 1; Australian Privacy Foundation, 14; Australian Information Security Association, 10; CrowdStrike, 3; Data Republic, 5; Privacy108, 4; Queensland Council for Civil Liberties,4; Shogun Cybersecurity, 2.
[157] Submissions to the Issues Paper: Centre for Media Transition, University of Technology Sydney, 10; Salinger Privacy, 10; Association for Data-driven Marketing and Advertising, 13; Reset Australia, 4; ID Exchange, 9.
[158] Australian Chamber of Commerce and Industry, *Attorney-General's Department small business representatives consultation meeting* (30 March 2021) ('Meeting of small business representatives').
[159] Submission to the Issues Paper: Clubs Australia, 3.
[160] Meeting of small business representatives (n 158).
[161] Australian Taxation Office, *Small business entity concessions eligibility* (Web Page, accessed 23 May 2021).
[162] Submissions to the Issues Paper: Consumer Policy Research Centre, 4; Electronic Frontiers Australia, 4; Dr Kate Mathews Hunt, 6; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 14; Australian Privacy Foundation, 15; Legal Aid Queensland, 6; Department of Health Western Australia, 3.
[163] ABS estimate prepared for OAIC, see OAIC, 60. 95.2% of the 2,375,753 businesses actively trading in the Australian economy were small businesses with an annual turnover of $3 million or less. Note that this figure does not take into account entities that are treated as 'organisations' under sections 6D(4)-(9) or small businesses that have opted into the Act under s 6EA.
[164] Submissions to the Issues Paper: Calabash Solutions, 5; Institute for Cyber Investigations and Forensics, University of the Sunshine Coast, 2; Electronic Frontiers Australia, 4; Dr Kate Mathews Hunt, 6; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 12; Dr Chris Culnane and Associate Professor Ben Rubinstein, 19; Google, 4; Centre for Cyber Security Research and Innovation, 11; New South Wales Council for Civil Liberties, 5.

proxy for potential impact on privacy.[165] Submitters also noted that the exemption does not reflect consumer expectations or the seriousness of a potential breach.[166] An organisation that holds information as basic as name and address could potentially use or disclosure it in circumstances which could cause harm to an individual.[167]

As noted in the Issues Paper, in the 20 years since the small business exemption was introduced, technology has changed the way that small businesses operate. Minderoo Tech and Policy Lab's submission noted that even the simplest website could collect information including IP Address, timestamps of visits and which web browser and operating system a visitor used.[168] Businesses actively engaged in online sales are likely to collect far more information.[169] Small businesses also have access to tools such as 'Facebook pixel' which allow businesses to track customers across devices and show targeted advertising to people who have already visited the business' website, or to people who are similar to those already interacting with the website.[170]

Figure 4.1 Percentage of small businesses receiving orders via internet/with web presence, 2006-7-2018-19.



The latest Australian Bureau of Statistics (ABS) data shows that from 2006-07 to 2018-19,[171] the proportion of businesses with a web presence rose by 20 percentage points (to 44 per cent) for businesses employing 0-4 persons and 22 percentage points (to 66 per cent) for businesses employing 5-19 persons.[172] Over the same period, the proportion of businesses that received orders via the internet rose 15 percentage points (to 35 per cent) for businesses employing 0-4 persons and 22 percentage points (to 51 per cent) for businesses employing 5-19 persons.[173] A more recent estimate, based on surveys of small businesses conducted in 2020 found that 84 per cent of Australian small businesses had adopted online services.[174]

---

[165] Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 12; Centre for Cyber Security Research and Innovation, 11; Department of Health Western Australia, 3; Australian Information Security Association, 10; CrowdStrike, 3; CSIRO, 5; Data Republic, 5; Shaun Chung and Rohan Shukla, 12.

[166] Submissions to the Issues Paper: Office of the Victorian Information Commissioner, 4; Gadens, 1; Dr Kate Mathews Hunt, 6; New South Wales Council for Civil Liberties, 5; Financial Planning Association of Australia, 2; Professor Kimberlee Weatherill, 4; CAIDE and MLS, 4; Queensland Council for Civil Liberties,4; Financial Services Council, 10.

[167] Submission to the Issues Paper: Queensland Council for Civil Liberties,4;

[168] Submission to the Issues Paper: Minderoo Tech and Policy Lab, University of Western Australia Law School, 29.

[169] Ibid.

[170] Ibid.

[171] Earliest and latest data available.

[172] Note the ABS defines a small business as one that employs 19 workers or fewer. ABS *Characteristics of Australian Businesses, various years.* Business use of information technology; ABS, *Summary of IT Use and Innovation in Australian Businesses 2006*, Data cube 1.

[173] Ibid. Note that this data was collected prior to the onset of the COVID-19 pandemic. The shift to online trade in the wake of COVID-19 is expected to increase business web presence and orders received via the internet.

[174] Cynch Security, Deakin University, RMIT, AustCyber Projects Fund, *Big cyber security questions for small business* (January 2021) 18.

A number of submissions raised concerns about the potential risks associated with small businesses that were not covered by the Act that were required by public heath orders to record patrons names and phone numbers for COVID contact tracing purposes.[175] A number of media reports at the time suggested that patrons were not providing accurate information due to concerns about their personal details being visible to other patrons and some businesses subsequently using the information for personal or business marketing purposes.[176]

Cyber security

A common theme among submissions was the view that small businesses pose a significant cyber security risk. A number of submissions stated that small businesses are often the 'weakest link' in supply chains.[177] Some submitters were of the view that requiring small businesses to comply with the Act (in particular the APP 11 security requirements and the Notifiable Data Breaches Scheme) could be a mechanism to mitigate this risk. Submissions noted that data breaches pose a risk not only to individuals, but also to the business that experiences the breach and the broader economy.[178] The impact to an individual can be long lasting or permanent and a single data breach can have a 'devastating' impact on a small business.[179]

There is evidence that the cyber security threat to small businesses is continuing to increase. In Australia, NortonLifeLock found that 1 in 4 small businesses were subject to cybercrime in 2017 – an increase from 1 in 5 in 2016.[180] Of particular concern to submitters was the application of the Notifiable Data Breaches Scheme (NDB scheme). IDCARE, a not-for-profit national identity and cyber support service, submitted that the number of small businesses experiencing breaches that would otherwise be notifiable under the NDB scheme is increasing.[181]

IDCARE considered that the government needed to provide appropriate support for businesses to meet cyber security standards and noted that efforts to encourage small businesses to enhance their cyber security posture have had mixed results.[182] A cyber security white paper released earlier this year and authored by Cynch Security, Deakin University and RMIT University found that two out of five small businesses had direct experience with a cyber incident worthy of reporting at some level, and that Australians report cyber security incidents to cyber.gov.au every 10 minutes.[183]

Small business representatives explained that small businesses put a lot of trust in the operating systems they use to protect information entered into these systems. For example, a lot of small businesses use point-of-sale and customer relationship management systems provided by larger entities such as banks, with an expectation of information security. Representatives noted that it was important for small businesses to be able to trust that these systems provide an appropriate

---

[175] Submissions to the Issues Paper: New South Wales Information and Privacy Commission, 2; Office of the Victorian Information Commissioner, 4; Association for Data-driven Marketing and Advertising, 13; New South Wales Council for Civil Liberties, 5; CAIDE and MLS, 5; Shogun Cybersecurity, 2.

[176] Dan Jervis-Bardy, 'Contact tracing threatened by use of fake names: ACT police chief', *The Canberra Times* (online, 6 August 2020); Josh Taylor, 'Privacy concerns over Australian businesses collecting data for COVID contact tracing', *The Guardian* (11 August 2020); Donia Waseem and Joseph Chen, 'Pubs are reopening but research shows contact tracing still isn't working – here's how to fix it', *The Conversation* (9 April 2021); Finbar O'Mallon, 'Check-in websites a privacy ticking time bomb', *The Australian Financial Review* (25 August 2020); Ellen Coulter, 'Businesses' collection of information for coronavirus contact tracing raises privacy concerns for customers', *ABC News* (28 October 2020).

[177] Submissions to the Issues Paper: Office of the Information Commissioner Queensland, 2; Gadens, 3; Australian Information Security Association, 10; CrowdStrike, 3; Shogun Cybersecurity, 2; Palo Alto Networks, 3.

[178] Submissions to the Issues Paper: Dr Kate Mathews Hunt, 6; IDCARE, 3.

[179] Submission to the Issues Paper: CrowdStrike, 3.

[180] Submission to the Issues Paper: Gadens, 3; NortonLifeLock, *Norton SMB Cyber Security Survey* (2017) 3.

[181] Submission to the Issues Paper: IDCARE, 3.

[182] Ibid, 6.

[183] Cynch Security, Deakin University, RMIT, AustCyber Projects Fund *Big cyber security questions for small business* (n 174) 4.

level of security and should not be subject to adverse actions where they have relied upon such systems and those systems have failed.[184]

Impact on business competitiveness

APP entities that engage small businesses must take steps to ensure that any personal information which the small business handles as part of the transaction is adequately protected. This was cited in submissions as potentially resulting in APP entities being less willing to engage a small business to undertake activities involving processing of personal information.[185] For this reason, a number of submissions contended that applying the Act more broadly to small businesses could result in small businesses being more competitive within the market.[186] Other submissions noted that requiring small businesses to comply with the Act could lead to enhanced consumer trust in small businesses and a reduced likelihood of consumer complaints about small businesses, placing them on the same playing field as bigger businesses.[187]

However, small business representatives raised concerns about the impact of removing the exemption on the competitiveness of small business relative to larger business due to the disproportionate burden of new compliance costs on small businesses.[188] Overseas evidence suggests that it is harder for small and medium businesses to comply with prescriptive privacy protection requirements and are thus at a competitive disadvantage.[189] Larger firms experience economies of scale with regard to compliance because costs are spread over much larger data sets.[190]

International comparisons

No comparable jurisdiction exempts small businesses from the general privacy law.[191] The GDPR provides a limited exemption from the requirement to maintain records of processing activities for organisations with less than 250 employees.[192] However, the exemption does not apply if the processing is likely to result in a risk to the rights and freedoms of data subjects or if the processing is 'not occasional'.[193] The exemption also does not apply to the processing of sensitive information or information relating to criminal convictions and offences.[194]

A number of submitters expressed concern that Australia's approach is an international anomaly and could be a barrier to international trade.[195] In particular, some submitters expressed concern that

---

[184] Xero, Australian Chamber of Commerce and Industry, Australian Small Business and Family Enterprise Ombudsman, Meeting of small business representatives (n 158).
[185] Submissions to the Issues Paper: AGL Energy Limited, 2; Financial Services Council, 9.
[186] Submissions to the Issues Paper: Western Union, 2; AGL Energy Limited, 2; Financial Services Council, 9.
[187] Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 13; OAIC, 59.
[188] Council of Small Business Organisations Australia, Meeting of small business representatives (n 158).
[189] Soumava Bandyopadhyay and Kakoli Bandyopadhyay, 'The European General Data Protection Regulation and Competitiveness of Firms' (2018) 16(1) *Competition Forum* 50, 53.
[190] Michal S Gal and Oshrit Aviv, 'The Competitive Effects of the GDPR' (2020) 16(3) *Journal of Competition Law and Economics* 349, 370, 373.
[191] UK, New Zealand, Canada, EU. The Review also considered approaches adopted in Japan and Singapore.
[192] GDPR (n 26) art 30(5).
Note the record keeping requirements contained in Article 30 of the GDPR require controllers to record the contact details of the controller and data protection officer, the purposes of the processing, a description of the categories of data subjects and of the categories of personal data, the categories of recipients to whom the personal data will be disclosed, details of international transfers including documentation of appropriate safeguards, time limits for erasure of different categories of data and a general description of the technical and organisational security measure.
[193] Ibid.
[194] Ibid.
[195] Submissions to the Issues Paper: Salinger Privacy, 11; New South Wales Information and Privacy Commission, 2; Calabash Solutions, 5; Centre for Media Transition, University of Technology Sydney, 10; OAIC, 60; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 12; Professor Kimberlee Weatherill, 4; Palo Alto Networks, 3; The Guardian Australia, 5.

the exemption is a barrier to GDPR adequacy and failure to remove the exemption could lead to loss of trade and collaboration with the EU market.[196] Submissions noted that a number of businesses are already required to comply with the GDPR or other overseas privacy regimes such as the NZ Privacy Act.[197] Removal of the exemption would align Australia with international standards for small business.[198] Submitters suggested that removal of the exemption could help Australia to achieve GDPR adequacy and the OAIC's submission noted the decision of the Court of Justice of the European Union in 'Schrems II' had highlighted the importance of EU adequacy decisions as a means of enabling transfers of data from the EU to overseas jurisdictions.[199]

Possible approaches to increasing privacy protections

There are a range of possible alternative options that could be considered to address the issues that were raised in submissions, each with their own benefits and limitations. The below sets out what these are. The Review is interested in your views on which of these options might be appropriate in the Australian context.

Remove the small business exemption

Removing the exemption would require all Australian businesses to comply with the Act. Submissions generally acknowledged that removing the exemption would result in a cost to small business. A small number of submissions suggested small businesses could comply with the Act with minimal financial impact and that the cost of compliance has gradually decreased since the introduction of the private sector provisions of the Act.[200] Some submitters were of the view that compliance with the Act is a reasonable cost of doing business in the digital age,[201] with others suggesting compliance with the Act could lead to commercial benefits for small businesses.[202] One submission asserted that the compliance burden for small businesses has not proven too onerous overseas.[203] Another view among submitters was that the flexibility of the APPs allow businesses to take a risk-based approach to compliance, based on their particular circumstances, including size, resources and business model.[204] As a result, these submitters reasoned, small businesses would have compliance costs commensurate with their risk profile and a small business that poses a low privacy risk would have low compliance costs.

However, even if the costs for small business to comply with the Act could be perceived to be low or proportionate and could improve business competitiveness, the challenges small business would face should not be ignored. Small business representatives acknowledged that small businesses should adhere to best practice when handling personal information, but expressed concern about requiring businesses to learn a new set of principles and set up procedures to give individuals access to their personal information. Small business representatives noted that this could be particularly

[196] Submissions to the Issues Paper: Office of the Victorian Information Commissioner, 4; Association for Data-driven Marketing and Advertising, 13; OAIC, 60; Gadens, 4; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 12; Australian Privacy Foundation, 15; CAIDE and MLS, 4; Reset Australia, 4; The Allens Hub for Technology, Law and Innovation, 5; Interactive Games and Entertainment Association, 10.
[197] Submissions to the Issues Paper: Salinger Privacy, 11; Association for Data-driven Marketing and Advertising, 13; Privacy108, 5.
[198] Submissions to the Issues Paper: Office of the Victorian Information Commissioner, 4; Reset Australia, 4; KPMG, 5.
[199] Submissions to the Issues Paper: OAIC, 60; Office of the Victorian Information Commissioner, 4; Gadens, 4; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 12; Australian Privacy Foundation, 15; CAIDE and MLS, 4; Western Union, 2; KPMG, 6; The Allens Hub for Technology, Law and Innovation, 5; Interactive Games and Entertainment Association, 10.
[200] Submissions to the Issues Paper: Shaun Chung and Rohan Shukla, 12; Data Synergies, 28; Law Council of Australia, 13.
[201] Submissions to the Issues Paper: Consumer Policy Research Centre, 4; Data Synergies, 28; Law Council of Australia, 13.
[202] Submissions to the Issues Paper: Salinger Privacy, 11; Calabash Solutions, 5; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 13; ID Exchange, 9.
[203] Submission to the Issues Paper: Salinger Privacy, 11.
[204] Submissions to the Issues Paper: Institute for Cyber Investigations and Forensics, University of the Sunshine Coast, 2; OAIC, 61; Privacy108, 5; AGL Energy Limited, 2; Financial Services Council, 10.

challenging for micro businesses.[205] A number of submissions suggested the compliance burden associated with removing the exemption could be minimised through the provision of tailored support and recommended that small businesses be provided with additional support and free tools to assist them in complying with the Act.[206] This could include template privacy policies, a dedicated small business hotline, tax offsets commensurate to the costs of compliance or government grants, could be provided. As an example, the UK ICO provides a live chat service, helpline, webinars, step by step guides and interactive tools to support compliance.[207]

The OAIC's submission stated that the office would be well placed to support small businesses to meet their compliance obligations.[208] The role of the OAIC in supporting small businesses could be further established by amending the *Australian Information Commissioner Act* (AIC Act) to prescribe the provision of support to small businesses as one of the IC's functions. Some submissions also suggested that if the exemption were to be removed, the IC should be authorised to prescribe exemptions from the requirements of the Act if, in practice, compliance with specific obligations proves unduly burdensome for certain small businesses as a class.[209]

A small number of submissions expressed concern about the impact of pecuniary penalties on small businesses and recommended amending the Act to clarify the IC must give consideration to the size and resources of an entity when determining a penalty.[210] The OAIC's Privacy Regulatory Action Policy lists factors to be taken into account in deciding when the take privacy regulatory action – this includes a requirement to consider whether the burden on the entity that would result from regulatory action is justified by the risk posed to the protection of personal information.[211]

However, while some small business representatives expressed strong support for providing small businesses with educational resources and support, they were also concerned about the substantial impact COVID-19 has had on small businesses. Small business representatives suggested it would be very challenging for small businesses to bear any additional cost of implementing privacy law changes at this time. Small business representatives were of the view that if the exemption was removed, there would be an unjustified regulatory burden placed on small businesses that do not pose a significant privacy risk.

Reduce the annual turnover threshold

Reducing the annual turnover threshold would bring more businesses within the scope of the Act. However, the threshold would need to be reduced significantly to have a meaningful impact on the number of businesses brought within the scope of the Act. The latest ABS data shows approximately 60 per cent of Australian businesses have an annual turnover of less than $500,000.[212] A reduced annual turnover threshold would also not address the privacy concerns outlined above. This option was not put forward as a preferred option in any submissions.

---

[205] Australian Small Business and Family Enterprise Ombudsman, Council of Small Business Organisations Australia, Australian Chamber of Commerce and Industry, Meeting of small business representatives (n 158).

[206] Submissions to Issues Paper: Salinger Privacy, 11; Centre for Media Transition, University of Technology Sydney, 10; Office of the Victorian Information Commissioner, 4; Association for Data-driven Marketing and Advertising, 14; Queensland Law Society, 3; Gadens, 3; Dr Kate Mathews Hunt, 6; Australian Privacy Foundation, 15; Financial Services Council, 11; The Guardian Australia, 5; Reset Australia, 4; Law Council of Australia, 13; ID Exchange, 9; Queensland University of Technology Faculty of Law, 16.

[207] UK Information Commissioner's Office, *SME web hub – advice for all small organisations* (Web Page, accessed 24 May 2021)

[208] Submission to the Issues Paper: OAIC, 61.

[209] Submissions to the Issues Paper: Queensland Council for Civil Liberties,4; Data Synergies, 28; Law Council of Australia, 14.

[210] Submissions to the Issues Paper: Gadens, 3; The Guardian Australia, 5.

[211] OAIC, *Privacy regulatory action policy* (May 2018) 9.

[212] Australian Bureau of Statistics, *Counts of Australian Businesses, including Entries and Exits* (February 2021).

An employee number threshold

Avant Mutual recommended the threshold be amended to 15 employees (consistent with the *Fair Work Act 2009* (Cth) (Fair Work Act) definition of a small business) and suggested this was a good measure of availability of staff and financial resources in a business for compliance activities.[213] However, other submitters were of the view that using number of employees to determine whether a business was a small business was problematic in the privacy law context and should be avoided.[214] Businesses would be more likely to fall in and out of scope of the Act which would add to the complexity of the OAIC's investigations and enforcement activities. It is also possible that introducing an employee number threshold would exempt high-risk businesses that are currently outside the scope of the exemption.

Require small businesses to comply with some but not all of the APPs

Requiring small businesses to comply with some but not all of the APPs could address some of the privacy risks posed by small businesses while not imposing the regulatory cost of complying with the Act as a whole. This option was put forward by a small number of submissions, but there was no consensus as to which APPs should apply.[215] APPs 1, 3, 4, 5, 6, 7, 8, 10, 11, 12 and 13 were all suggested as APPs small businesses should comply with. This approach would exempt small businesses from the requirements of APPs 2 and 9 which would be unlikely to result in significant reduction in compliance costs for small business. A submission by Associate Professor Mark Burdon and Tegan Cohen noted that the APPs are interlinked and do not operate on a standalone basis and did not support the APPs being 'cherry-picked' for application to small business.[216] Requiring businesses to comply with some but not all of the APPs would likely increase the complexity of the Act as selected APPs would need to be modified for small business so they could be understood outside the context of the other APPs.

Simplified rules for small business

A small number of submissions put forward options that would require small businesses to comply with simplified rules.[217] However, the flexible, risk-based framework provided by the APPs would already achieve this by requiring compliance commensurate to a small business' particular circumstances, including size, resources and business model.

Prescribe further acts or practices

When the Act was extended to the private sector, it was considered that there were some small businesses, or acts and practices of small businesses that posed a higher risk to privacy and should be covered by the obligations set out in the Act, irrespective of the business's annual turnover.[218] The Issues Paper set out the acts and practices prescribed by the Act which bring small businesses that would otherwise be exempt within the scope of the Act.[219]

---

[213] Submission to the Issues Paper: Avant Mutual, 7.

[214] Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 13; Australian Financial Markets Association, 5.

[215] Submissions to the Issues Paper: Legal Aid Queensland, 6; Financial Services Council, 10; FinTech Australia, 9.

[216] Submission to the Issues Paper: Queensland University of Technology Faculty of Law, 16.

[217] Submissions to the Issues Paper: Association for Data-driven Marketing and Advertising, 13; FinTech Australia, 8;Law Institute of Victoria, 6.

[218] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 36.

[219] The small business exemption does not apply to health service providers, businesses that trade in personal information (subject to the consent exception), businesses that provide services under a Commonwealth contract, credit reporting bodies, businesses that operate residential tenancy databases, reporting entities for the purposes of the AMLCTFA, employee associations registered or recognised under the *Fair Work (Registered Organisations) Act 2009*, businesses that conduct protection action ballots, businesses accredited under the CDR system and businesses related to APP entities. See Attorney General's Department, *Privacy Act Review Issues paper* (October 2020) 26. See also *Privacy Act* (n 2) ss 6D(4)(b)-(f); 6E(1A)-(1D), 6D(9); *Privacy Regulation 2013* (Cth) s 7.

Further consideration could be given to whether these acts and practices are up to date and reflect all current high privacy risk acts and practices. The Australian Small Business and Family Enterprise Ombudsman submitted that if there was evidence of a problem with the exemption, the best practice approach would be to address the problem directly, rather than removing the exemption completely.[220] Prescribing further high risk acts and practices, while retaining the small business exemption, would preserve the Act's historical approach of balancing privacy risks against compliance costs on small businesses.

Potential further high-risk acts and practices

Submissions identified a number of high risk businesses, acts and practices, including collecting, using or disclosing the personal information of children under 15[221] or supplying products or services to children under 15[222], handling financial or sensitive information[223], buy now, pay later businesses,[224] offering products and services that use the Internet of Things (IoT), AI and data analytics[225] and IT businesses which provide services to healthcare providers.[226]

The UK ICO publishes a list of data processing operations 'likely to result in high risk' and for which businesses are required to complete a Data Protection Impact Assessment.[227] The list is based on guidelines adopted by the European Data Protection Board[228] and includes acts and practices similar to those identified by submitters, including the use of AI, machine learning and deep learning, IoT applications and smart technologies and targeting of children or other vulnerable individuals for marketing. It also lists further activities, including:

- intelligent transport systems and connected and autonomous vehicles
- market research involving neuro-measurement (i.e. emotional response analysis and brain activity)
- hardware and software offering fitness or lifestyle monitoring
- social media networks
- facial recognition and identity verification systems
- medical research
- data matching and aggregation
- direct marketing and online advertising
- web and cross-device tracking
- re-use of publicly available data
- loyalty schemes, and
- DNA testing.

Challenges of prescribing additional acts and practices

The current prescribed exceptions to the small business exemption capture acts and practices that are clearly understood by both businesses and the community. It would be important to ensure that any new exceptions were clearly defined and not too broad. Examples of high risk activities that could be covered by the Act provided by submitters included businesses that are 'digitally enabled' or technology-based businesses.[229] However prescribing businesses that are 'digitally enabled' could potentially capture any business with a website or social media presence. The OAIC's submission

[220] Submission to the Issues Paper: Australian Small Business and Family Enterprise Ombudsman, 1.
[221] Submission to the Issues Paper: Australian Council on Children and the Media, 3.
[222] Submission to the Issues Paper: Australian Council on Children and the Media, 3.
[223] Submissions to the Issues Paper: Law Institute of Victoria, 6; Anonymous 2, 3.
[224] Submission to the Issues Paper: Legal Aid Queensland, 6.
[225] Submission to the Issues Paper: Financial Services Council, 10.
[226] Submission to the Issues Paper: Australian Medical Association, 4.
[227] UK ICO, *Examples of processing 'likely to result in high risk'* (Web Page, accessed 24 May 2021).
[228] Ibid.
[229] Submission to the Issues Paper: FinTech Australia, 9.

warned that 'privacy risks are constantly emerging and evolving' and, as a result, prescriptions could quickly become out of date.[230]

It may also be difficult for the OAIC to identify businesses that engage in 'high risk' activities if these activities are not a core component of their business. This could lead to regulatory uncertainty for businesses as to whether they are required to comply with the Act. It would also be difficult for individuals to ascertain which businesses are covered by the prescriptions, particularly since the small business exemption is not well understood by consumers.[231]

Provide small businesses with additional support

Instead of subjecting small businesses to stricter regulation, small businesses could be provided with additional, targeted resources to educate and support them to adopt better privacy practices. There are a number of current government initiatives aimed at supporting small businesses in the digital economy. For example, the Australian Small Business Advisory Services Program provides low-cost, independent advice to small businesses on issues such as how going digital can help small business, websites and selling online, social media and digital marketing, small business software and online security.[232] The Australian Cyber Security Centre also provides guidance and advice to help small businesses protect themselves from cyber security incidents.[233]

In addition, the recently announced National AI Centre aims to assist small businesses with medium-high digital capability to adopt AI by providing them with access to cutting edge technology, experts and advice.[234] Encouraging small businesses to adopt digital solutions and innovative technologies could be supplemented by clear advice about the privacy risks posed by these technologies and how businesses can appropriately respond to these risks. These initiatives could be supported by tailored OAIC guidance and support for small businesses. More education and training could encourage more small businesses to opt in to the requirements of the Act under section 6EA.[235] Small businesses that opt-in to the Act could also benefit from participating in the domestic privacy certification scheme discussed further in Chapter 23.

Consent provisions

The consent provisions of the small business exemption provide that a small business that trades in personal information may still be exempt from the Act if it has the consent of individuals to collect or disclose their personal information.[236] Trading in personal information generally means buying or selling personal information. For example, buying a mailing list, or disclosing customer details for a commercial gain.[237] A business will trade in personal information if it collects or discloses an individual's personal information to someone else for a benefit, service or advantage including a financial payment, concession, subsidy or other advantage or service.[238] Submissions that addressed this issue did not consider it appropriate for businesses to rely on consent as a basis for being exempt from the Act. These submissions considered that the consent exception should be removed, given the significant privacy risk posed by trading in personal information.

---

[230] Submission to the Issues Paper: OAIC, 61.
[231] Submission to the Issues Paper: OAIC, 60.
[232] Australian Government, *Digital Solutions – Australian Small Business Advisory Services* (Web Page, May 2021).
[233] Australian Cyber Security Centre, *Small Business Cyber Security Guide* (Web Page, February 2021).
[234] Department of the Prime Minister and Cabinet, *Artificial Intelligence* (Web Page, May 2021)
[235] The OAIC maintains a register of small business operators that have opted-in to the Privacy Act. As at 20 September 2021, the register contained the names of 697 businesses.
[236] *Privacy Act* (n 2) sub-ss 6D(7)-(8).
[237] OAIC, *Trading in personal information* (Web Page, accessed 24 May 2021).
[238] Ibid.

Questions

- Are there further high privacy risk acts and practices that should be prescribed as exceptions to the small business exemption?
- What regulatory impact would this have on small businesses who engage in these acts and practices?
- What support for small business would assist with adopting the privacy standards in the Act and realising the benefits of improved privacy practices?
- How can small businesses be encouraged to adopt best practice information collection and handling?
- To what extent do small businesses that trade in personal information currently rely on the consent provisions?
- Would Proposal 9.1 to require consent to be voluntary, informed, current, specific and unambiguous address concerns about the privacy risks associated with the consent provisions of the small business exemption?
- Would Proposal 23.2 to introduce a voluntary domestic privacy certification scheme be useful to small businesses that wish to differentiate themselves based on their privacy practices?

5. Employee records exemption

An organisation that is or was an employer is exempt from the operation of the Act for an act or practice directly related to its employment relationship with an individual, and an employee record it holds relating to the individual. An employee record is a record of personal information relating to the employment of the employee. The Issues Paper sought feedback on whether the employee records exemption adequately protects the personal information of employees. It also asked whether some but not all of the APPs should apply to the personal information of employees and whether consent is an appropriate mechanism for authorising employers' handling of such information.

Protection of employees' privacy

A number of submitters, including the OAIC, expressed concern that the current scope of the employee records exemption fails to adequately protect the personal information of private sector employees. These submissions favoured either removing the exemption entirely,[239] or modifying it to apply specific APPs to employee records.[240] Other submitters considered that employees' privacy is adequately protected by the record-keeping requirements in workplace relations legislation.[241] These submitters favoured retaining the exemption.

Keeping employees' personal information secure

Some submissions considered that the protections that individuals generally enjoy under the Act should apply to their workplaces.[242] Of particular concern was the security of employees' personal information.[243] An employer is not required to comply with APP 11.1 in relation to the personal information contained in an employee record, and so is not required to take such steps that are reasonable in the circumstances to protect that information:

- from misuse, interference and loss, and
- from unauthorised access, modification and disclosure.

These submissions considered that individuals are at a greater risk of harm from the mishandling of their personal information in the employment context because the employment relationship inherently involves the significant collection of personal information, which is often sensitive in nature.[244] Submissions cited examples of the variety of information routinely collected by

---

[239] Submissions to the Issues Paper: OAIC, 62; Salinger Privacy, 11; Office of the Victorian Information Commissioner, 5; HIV/AIDS Legal Centre, 3; Law Institute of Victoria, 8; Centre for Cyber Security Research and Innovation, 7; Australian Information Security Association, 12; elevenM, 2; Centre for Media Transition, University of Technology Sydney, 10; CAIDE and MLS, 4; Google, 4; New South Wales Council for Civil Liberties, 5; Karen Meohas, 9; Digital Rights Watch, 5; Reset Australia, 5; Professor Kimberlee Weatherall, 4; Minderoo Tech and Policy Lab, University of Western Australia Law School, 29; Privacy108, 5; Financial Services Council, 13; ID Exchange, 10; Queensland Law Society, 3; Queensland University of Technology Faculty of Law, 17; The Allens Hub for Technology, Law and Innovation and Australian Society for Computers and Law, 5; Royal Australian College of General Practitioners, 2; Law Council of Australia, 16; Australian Communications Consumer Action Network, 10; Queensland Council for Civil Liberties, 4; Australian Privacy Foundation, 16.

[240] Submissions to the Issues Paper: Gadens, 5; Dr Kate Mathews Hunt, 7; Deloitte, 8; Castan Centre for Human Rights Law – Monash University, 20; Data Synergies, 29; Maurice Blackburn, 4. See also Submissions to the Issues Paper: Data Republic 6; SuperChoice, 3.

[241] Submissions to the Issues Paper: Australian Chamber of Commerce and Industry, 2, 4–5; Ai Group, 11; AGL Energy Limited, 3; Nine, 9; Optus, 5.

[242] Submissions to the Issues Paper: Law Council of Australia, 16; OAIC, 62; Centre for Cyber Security Research and Innovation, 7.

[243] Submissions to the Issues Paper: OAIC, 62-63; Salinger Privacy, 11; Office of the Victorian Information Commissioner, 5; Financial Services Council, 12; Australian Communications Consumer Action Network, 10; Castan Centre for Human Rights Law – Monash University, 20. See also Submission to the Issues Paper: Data Republic, 6.

[244] Submissions to the Issues Paper: Law Council of Australia, 14; OAIC, 62; Law Institute of Victoria, 7; Office of the Information Commissioner Queensland, 2; Humanising Machine Intelligence Project, Australian National University, 4; Australian Privacy Foundation, 15; Australian Information Security Association, 12; Australian Communications Consumer Action Network, 9; Centre for Cyber Security Research and Innovation, 7; Castan Centre for Human Rights Law – Monash University, 20.

employers, such as contact details, health and genetic information, including personality and aptitude testing, as well as results of bankruptcy, identity, credit and criminal history checks.[245]

The Financial Services Council said that although some employers may already have systems and procedures in place to keep employees' personal information secure, this did not negate the need for a legislative standard. It said the widespread adoption of security practices, such as the partitioning of HR and payroll functions as well as the use of physical and electronic access controls for employee records supported the removal of the exemption because it would be unlikely to cause a significant compliance burden on employers.[246]

In addition to general security concerns, a small number of submissions also considered whether the NDB scheme should apply to employee records. Currently, private sector employers that are subject to APP 11.1 for acts or practices outside of the employee records exemption will already have measures in place to assess and report eligible data breaches for personal information they hold about individuals other than employees (e.g. customers). There are also already some circumstances in which they are required to notify employees of data breaches, such as for eligible breaches involving tax file number information.[247] Salinger Privacy said there was no valid reason to offer less protection to the remainder of employee records.[248]

Employers' changed information-handling practices

Some submissions said the risks to privacy have increased as a result of the blurring of boundaries between employees' personal and professional lives since the exemption was introduced in 2001.[249] These submissions considered that the increase in work-from-home arrangements in recent years (and due to the COVID-19 pandemic) has extended workplace surveillance into employees' personal lives, making it harder to clearly discern whether their personal information is protected or exempted under the Act.[250] The Queensland Law Society said the requirement to separate non-work related personal information captured on work-assigned mobile phones, for example, is unnecessary and confusing for employers.[251]

Submissions also considered that employees are uniquely vulnerable to excessive or unreasonable collection of their personal information because the workplace is often where individuals may be exposed to advances in information-gathering technologies, including artificial intelligence, closed-circuit television (CCTV) and data analytics.[252]

These submissions considered that employers should be required to demonstrate their uses of these technologies are reasonable and necessary.[253] Maurice Blackburn said there was a need for clearer articulation of when an employer has 'gone too far' in their collection or use of employee

---

[245] Submissions to the Issues Paper: Office of the Victorian Information Commissioner, 5; HIV/AIDS Legal Centre, 3; Law Institute of Victoria, 7; New South Wales Council for Civil Liberties, 5; Reset Australia, 5.
[246] Submission to the Issues Paper: Financial Services Council, 13. See also Submission to the Issues Paper: Deloitte, 9.
[247] *Privacy Act* (n 2) sub-s 26WE(1)(d).
[248] Submission to the Issues Paper: Salinger Privacy, 11. See also Submissions to the Issues Paper: Australian Privacy Foundation, 15; Office of the Victorian Information Commissioner, 5.
[249] Submissions to the Issues Paper: Maurice Blackburn, 4; Office of the Victorian Information Commissioner, 5; Queensland University of Technology Faculty of Law, 17; Reset Australia, 5; Queensland Law Society, 3; Financial Services Council, 12; Australian Privacy Foundation, 16.
[250] Submissions to the Issues Paper: Professor Kimberlee Weatherall, 4; Financial Services Council, 12; Queensland University of Technology Faculty of Law, 17.
[251] Submission to the Issues Paper: Queensland Law Society, 3–4. See also Submission to the Issues Paper: OAIC, 63.
[252] Submissions to the Issues Paper: Law Council of Australia, 14; New South Wales Council for Civil Liberties, 5; Reset Australia, 5; Professor Kimberlee Weatherall, 4; Minderoo Tech and Policy Lab, University of Western Australia Law School, 28; Privacy108, 6; Dr Kate Mathews Hunt, 7; Castan Centre for Human Rights Law – Monash University, 20; Humanising Machine Intelligence Project, Australian National University, 4.
[253] Submissions to the Issues Paper: Dr Kate Mathews Hunt, 7; Data Synergies, 29; Privacy108, 6. See also Submission to the Issues Paper: New South Wales Council for Civil Liberties, 5.

information.[254] Minderoo Tech and Policy Lab expressed a particular concern about the collection of sensitive information being exempted from the Act merely on account of being 'directly related' to the employment relationship.[255] The submission said it had observed a trend of certain employers, in logistics, sport, mining and healthcare collecting a substantial amount of health information to assess employees' 'conduct or performance' using GPS trackers, video and biosensors, as well as results of fitness, stress, blood and urine tests and body scanning and imaging – even where the connection between the data and performance might be tenuous.[256]

This view was shared by submissions that considered there was a need to apply the Act's distinction between personal and sensitive information to employee records.[257] However, these submissions did not always agree on where the line should be drawn. For example, Gadens considered that employees' health and genetic information should be covered by the Act, but also said that employees might now reasonably expect the use of facial and fingerprint recognition and other biometric technologies in their workplaces (as in their personal lives).[258]

Protection of employee privacy under workplace relations laws

Submissions in favour of retaining the exemption considered it unnecessary for the Act to apply in the employment context because current workplace relations legislation, including the Fair Work Act and model Work Health and Safety laws, effectively protect employee records.[259] ACCI and Ai Group were of the view that employees enjoy stronger privacy protections under the Fair Work Act, given the onus on employers to demonstrate compliance with record-keeping requirements and increased fines for non-compliance.[260]

Both also emphasised that employee privacy continues to be better addressed by workplace relations legislation, in line with the exemption's policy rationale, given the uniqueness of personal information collection and use in the employment context.[261] ACCI cautioned against altering the exemption on the basis of survey data alone, stating that, unlike privacy law, employment law is made through tripartite consultations between government, employers and unions.[262]

Submissions that supported narrowing the exemption did not consider that current workplace relations legislation adequately protects employees' privacy.[263] Legal Aid Queensland noted that the current provisions in the Fair Work Act only outline the requirement for national system employers to keep records and the procedural aspects regarding how those records are to be kept.[264]

These obligations are primarily concerned with ensuring that employees receive their correct wages and entitlements.[265] Employers are only required to keep basic employee records for seven years on

---

[254] Submission to the Issues Paper: Maurice Blackburn, 3.
[255] Submission to the Issues Paper: Minderoo Tech and Policy Lab, University of Western Australia Law School, 28 citing *'QF' and Spotless Group Limited (Privacy)* [2019] AICmr 20, [49]. See also Submissions to the Issues Paper: Professor Kimberlee Weatherall, 4–5; The Allens Hub for Technology, Law and Innovation and Australian Society for Computers and Law, 5; Deloitte, 8.
[256] Submission to the Issues Paper: Minderoo Tech and Policy Lab, University of Western Australia Law School, 27–8.
[257] Submissions to the Issues Paper: OAIC, 62; HIV/AIDS Legal Centre, 3; Australian Communications Consumer Action Network, 10; Deloitte, 8; Centre for Media Transition, University of Technology Sydney, 10. See also Submissions to the Issues Paper: Law Council of Australia, 14; Law Institute of Victoria, 7.
[258] Submission to the Issues Paper: Gadens, 5. Cf Submissions to the Issues Paper: HIV/AIDS Legal Centre, 3; Reset Australia, 5.
[259] Submissions to the Issues Paper: Australian Chamber of Commerce and Industry, 2, 4–5; Ai Group, 11; AGL Energy Limited, 3; Nine, 9; Optus, 5.
[260] Submissions to the Issues Paper: Australian Chamber of Commerce and Industry, 4–5; Ai Group, 11.
[261] Submissions to the Issues Paper: Australian Chamber of Commerce and Industry, 3; Ai Group, 11.
[262] Submission to the Issues Paper: Australian Chamber of Commerce and Industry, 7–8.
[263] Submissions to the Issues Paper: Privacy108, 5; Legal Aid Queensland, 6; New South Wales Council for Civil Liberties, 5; Minderoo Tech and Policy Lab, University of Western Australia Law School, 27.
[264] Submission to the Issues Paper: Legal Aid Queensland, 6.
[265] Fair Work Ombudsman, 'Record-keeping & Pay slips' (Web Page, 2021).

matters such as leave, income and hours of work, as prescribed by the Fair Work Regulations. Employers must keep these prescribed employee records accurate and make them available for inspection and copying. However, there is no requirement to take reasonable steps to keep these records secure or to notify employees when they are mishandled or subject to a data breach.

Unlike the Fair Work Act, the model Work Health and Safety laws, which have been implemented by all states and territories except for Western Australia and Victoria, provide some protection of sensitive employee records in limited contexts. This includes records that monitor the health of employees working with hazardous chemicals, which must be kept confidential for 30 years and must not be disclosed without the relevant worker's written consent.[266] However, outside of these specific examples, the Work Health and Safety laws do not set out general obligations for employee records, despite importing the definition of 'employee record' from the Act.[267]

Submissions that favoured regulating the privacy of employee records, either under the Act or under a separate federal scheme on employment privacy,[268] regarded this as important to ensure the level of protection necessary to deal with the nature and volume of personal information employers now routinely collect.[269] The OAIC considered that employers' record-keeping requirements under other frameworks complement the Act and should enable employers to easily meet their compliance obligations under the APPs.[270]

Exemption necessary to administer the employment relationship

Ensuring employers can effectively manage their workplaces

Some businesses and employer representatives' submissions contended that removing the exemption would make it difficult for employers to administer the employment relationship.[271] This concern was often expressed in relation to particular APPs. For example, regarding APP 3.2, the Ai Group said it would be 'near impossible' for an employer to avoid the uncertainty that most of its collection of employees' personal information was not *reasonably necessary* for one or more of its functions or activities.[272] Ai Group also said that APP 3.3 (which applies to sensitive information) would be 'very difficult' to apply consistently with an employer's need to investigate instances of bullying or misconduct, but noted the possibility that such collection may be authorised by or under an Australian law, under APP 3.4.[273]

The burden of responding to access and correction requests

Several submissions noted that, notwithstanding the current exceptions under APP 12.3,[274] the application of APP 12 to employee records would make it difficult for employers to effectively conduct investigations and manage employees.[275] Ramsay Australia said this might jeopardise already complex interpersonal issues in the workplace.[276]

---

[266] Model Work Health and Safety Regulations pt 7.1 div 6.
[267] Model Work Health and Safety Act s 4.
[268] Submission to the Issues Paper: Maurice Blackburn, 4.
[269] Submissions to the Issues Paper: Office of the Information Commissioner Queensland, 2; Reset Australia, 5; Professor Kimberlee Weatherall, 4; Queensland University of Technology Faculty of Law, 17; Law Council of Australia, 16; Australian Privacy Foundation, 15; Australian Information Security Association, 12; Minderoo Tech and Policy Lab, University of Western Australia Law School, 27; Legal Aid Queensland, 6.
[270] Submission to the Issues Paper: OAIC, 63.
[271] Submissions to the Issues Paper: Ai Group, 12; Australian Chamber of Commerce and Industry, 10; Griffith University, 7; Ramsay Australia, 4; AGL Energy Limited, 3; Optus, 5; Nine, 9; Clubs Australia, 3.
[272] Submission to the Issues Paper: Ai Group, 12.
[273] Ibid.
[274] See, eg, ibid 13.
[275] Submissions to the Issues Paper: Ai Group, 13; Australian Chamber of Commerce and Industry, 4, 12; AGL Energy Limited, 3; Clubs Australia, 4; Ramsay Australia, 4.
[276] Submission to the Issues Paper: Ramsay Australia, 4.

Ai Group said that, unlike the employee records required to be kept under the Fair Work Act, records about employee performance and behaviour are often sensitive and personal in nature and should therefore not be able to be subject to an access request.[277] AGL said that a requirement to disclose evaluation material such as references and disciplinary and performance records might deter employers from undertaking frank assessments and investigations.[278] Other submissions added that without the reassurance of confidentiality, employees might be discouraged from engaging in full and frank disclosure – not only in the context of workplace investigations but also for more routine matters.[279] Concerns about employees accessing certain employee records were raised not only by submitters opposed to removing the exemption. Submitters who favoured narrowing the exemption recognised difficulties raised by this issue and suggested either a full or partial exemption to APP 12 for employers.[280]

Submissions expressed similar concerns about APP 13. For example, ACCI questioned whether, absent the employee records exemption, an employee dissatisfied with an outcome of an investigation or performance review could seek to have it 'corrected'.[281]

Should employees' consent be required to collect sensitive information

A large number of submissions expressed the need to take action to address the impact of the decision by the Full Bench of the Fair Work Commission in *Lee v Superior Wood.*[282] In that case it was held that the exemption did not apply to the employer's collection of sensitive information because the information was not yet contained in an employee record. Employers must therefore comply with APP 3 when collecting an employee's personal information before including it in their employee record. This requires obtaining the employee's consent in order to collect sensitive information.[283]

Submissions that favoured retaining the employee records exemption had differing views on what action should be taken in response to *Lee*. For example, the Ai Group said the exemption should apply to the collection of personal information and that the decision in *Lee* demonstrated both the 'folly' of removing the exemption and the need to ensure employers can flexibly impose reasonable administrative actions, such as taking temperatures in response to the COVID-19 pandemic.[284] However, AGL supported the decision and said that while the exemption should be retained it should not apply to collection, noting the importance of dissuading employers from collecting more personal information than is necessary for administering the employment relationship.[285]

Submissions in favour of narrowing the exemption also indicated a need for reasoned amendments following *Lee*, to make clear which APPs employers need to comply with. Electronic Frontiers Australia supported the exemption applying only to current employees where there is free, full and informed consent.[286] Gadens proposed narrowing the exemption by subjecting certain types of sensitive information about employees, such as their health and genetic information to the

---

[277] Submission to the Issues Paper: Ai Group, 13. See also Submission to the Issues Paper: Clubs Australia, 4.
[278] Submission to the Issues Paper: AGL Energy Limited, 3.
[279] Submissions to the Issues Paper: Australian Chamber of Commerce and Industry, 12; Ramsay Australia, 4; Clubs Australia, 4.
[280] Submissions to the Issues Paper: OAIC, 63; Salinger Privacy, 11; Deloitte, 9; Castan Centre for Human Rights Law – Monash University, 21.
[281] Submission to the Issues Paper: Australian Chamber of Commerce and Industry, 13.
[282] *Lee v Superior Wood Pty Ltd* [2019] FWC 2946 ('*Lee*'). Submissions to the Issues Paper: Griffith University, 7; Ai Group, 13; AGL Energy Limited, 3; CAIDE and MLS, 4; Gadens, 4; Electronic Frontiers Australia, 5.
[283] See Athena Koelmeyer and Nicola Josey, 'Consent, the Privacy Act and biometric scanners in the workplace' (2019) 57 *Law Society of NSW Journal* 76. See also OAIC, 'Coronavirus (COVID-19): Understanding your privacy obligations to your staff' (Web Page).
[284] Submission to the Issues Paper: Ai Group, 13.
[285] Submission to the Issues Paper: AGL Energy Limited, 3. See also Submission to the Issues Paper: Griffith University, 7.
[286] Submission to the Issues Paper: Electronic Frontiers Australia, 4–5.

protections in the Act and clarifying what constitutes genuine consent.[287] Other submissions presented *Lee* as evidence of the need to remove the exemption entirely and for all the privacy protections in the Act to apply.[288] The OAIC said the decision has likely created a greater compliance burden for employers to determine when the Act does or does not apply to their particular personal information-handling practices than if the APPs applied to all the personal information that an employer holds.[289]

Genuineness of employees' consent

As recognised in *Lee,* the capacity of employees to give genuine consent to the collection of their personal information, where failure to do so may result in disciplinary action, raises questions about whether consent is an appropriate mechanism in the context of the employment relationship. Guidance issued by the UK ICO states that consent will not usually be an appropriate basis on which to process personal information in the employment context as employees 'may feel compelled to consent, as they don't want to risk their job or be perceived as difficult'.[290]

Submissions in favour of retaining the exemption opposed requiring employees' consent to collect their personal information, stating that the nature of the employment relationship necessarily precluded seeking consent, particularly on an ongoing basis.[291] ACCI said that employees automatically consent to the handling of their personal information by employers, as implied by the employment contract and that employers should not be required to provide notification each time.[292] These submissions considered that information-handling practices of employers are in line with the public's expectations and need not be unnecessarily curtailed.[293]

Other submissions, which favoured removing or narrowing the exemption, acknowledged the problematic nature of requiring consent in the employment context because of the inherent power imbalance between employers and employees, in line with the *Lee* decision.[294] Submissions that suggested alternatives to consent acknowledged the need to enable employers to administer the employment relationship.[295] Some submissions suggested alternatives to the current exceptions for handling personal information, including in APP 3.3, such as where the collection of sensitive information is necessary to give effect to an employer's legitimate interests.[296]

Possible approaches to protecting employees' privacy

Remove the employee records exemption

Removing the exemption would require all APP entities to comply with the Act in relation to their personal information handling of employees and former employees. It would not affect most small business employers as most businesses with an annual turnover of $3 million or less are not covered by the Act. Submissions from employers and their representatives indicated that removing the exemption would make it difficult to administer the employment relationship, particularly with

---

[287] Submission to the Issues Paper: Gadens, 4–6.
[288] Submissions to the Issues Paper: OAIC, 63; Queensland Law Society, 4; Avant Mutual, 8; Law Council of Australia, 15.
[289] Submission to the Issues Paper: OAIC, 63.
[290] UK ICO, 'When is consent appropriate?', *Guide to the General Data Protection Regulation* (Web Page).
[291] Submissions to the Issues Paper: Griffith University, 7–8; Clubs Australia, 3.
[292] Submission to the Issues Paper: Australian Chamber of Commerce and Industry, 10.
[293] Submissions to the Issues Paper: Ai Group, 12–13; Clubs Australia, 4. See also Submissions to the Issues Paper: Gadens, 5; Financial Services Council, 13.
[294] Submissions to the Issues Paper: Privacy108, 6; Castan Centre for Human Rights Law – Monash University, 21; Gadens, 5 (with regard to sensitive information); Centre for Cyber Security Research and Innovation, 7; Minderoo Tech and Policy Lab, University of Western Australia Law School, 27–8; Australian Communications Consumer Action Network, 10; Data Synergies, 29.
[295] Submissions to the Issues Paper: Centre for Cyber Security Research and Innovation, 7; Gadens, 5; OAIC, 63; Castan Centre for Human Rights Law – Monash University, 21; Data Synergies, 29.
[296] Submissions to the Issues Paper: Australian Privacy Foundation, 16; Castan Centre for Human Rights Law – Monash University, 21; Data Synergies, 29; Centre for Cyber Security Research and Innovation, 7; Financial Services Council, 13.

respect to sensitive processes, such as disciplinary investigations and performance management if employees were able to access their personal information under APP 12.

Modify the employee records exemption

The exemption could be modified to allow better protection of employee records while retaining the flexibility employers need to administer the employment relationship. For example, a new standalone exception for employers could be introduced into APPs 3 and 6. Similar to the existing exemption, the new exception could apply to the collection, use and disclosure of an employee's personal and sensitive information by a current or former employer for any act or practice directly related to the employment relationship. This approach, which acknowledges the limitations of relying on consent in an employment context, could make it easier for employers to manage their workplaces by making clear that employees' consent would not be required to collect their sensitive information. This would restore the scope of the exemption to the interpretation that applied prior to the *Lee* decision and could allow for enhanced protection of employee privacy through the application of other APPs, such as APPs 8 and 11. The application of these APPs could help ensure employers take reasonable steps to protect employees' personal information from unauthorised access and disclosure and would apply the accountability principle to the disclosure of such information to overseas recipients.

The application of other APPs would require careful consideration of the unique nature of the employment context, to ensure that employers are exempted from having to comply with inappropriate or irrelevant obligations. For example, given the concerns about employers' ability to undertake sensitive managerial processes, appropriate amendments to APPs 12 and 13 could be made to balance employees' ability to access and seek correction of their personal information with countervailing considerations, such as the protection of other individuals' privacy.

Further, recognising submitters' concerns about employees being vulnerable to excessive or unreasonable collection of their sensitive information, additional protection could be considered in relation to employees' collection, use and disclosure of sensitive information. Proposal 10.1 that collection, use or disclosure of personal information must be fair and reasonable could be utilised in the employment context to provide specific, additional protection to sensitive information.

Enhance employee privacy protections in workplace relations legislation

Privacy protections could be extended to private sector employees through workplace relations legislation. If privacy protections applied to the handling of employees' personal information by employers covered by the Fair Work Act, employees of both large and small businesses that are not covered by the Privacy Act could be afforded privacy protection. It would also mean that private sector employees would be covered by different privacy standards to those which apply to Commonwealth public sector employees. While this situation already exists in relation to state and territory public sector employees that are covered by state and territory privacy legislation, it would contribute to further fragmentation of privacy protection across different legislative regimes. Including privacy protections in workplace relation legislation may also result in jurisdiction to investigate and determine privacy matters being conferred on the Fair Work Ombudsman and Commission rather than the Information Commissioner, which would represent a significant change.

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?

6. Political exemption

Registered political parties are exempted entirely from the Act.[297] A more limited exemption applies for acts or practices done for any purpose in connection with an election, a referendum, the participation in another aspect of the political process or facilitating acts or practices of a registered political party by political representatives and their affiliates and by political parties' affiliates.[298] The Issues Paper asked whether political acts and practices should continue to be exempted from the operation of some or all of the APPs.

Is the political exemption achieving its objective?

The objective of the political exemption is to encourage freedom of political communication and enhance the operation of the electoral and political process in Australia.[299] Nine Ltd stated that it 'enhances free and open communication and improves participation in and engagement with our political processes'.[300] The Cyber Security Cooperative Research Centre proposed retaining the exemption from the Act but removing relevant exemptions from the Do Not Call Register Act (DNCR Act) and spam rules.[301]

All other submissions that commented on the exemption considered that it is not achieving its objective and should be removed or narrowed in scope. These submissions came from various stakeholder groups, including security experts, privacy advocates, academics and universities, civil society and individuals.[302]

Potential for misuse of voters' personal information and voter manipulation

Some submissions recommended removing the exemption on the basis that it is no longer fit for purpose. They stated that the way in which data can be used to target and profile individuals has changed significantly since the introduction of the exemption in 2000, and has increased the need for transparency regarding how political parties handle personal information.[303] In its submission, the Castan Centre for Human Rights Law stated:

> *The unprecedented use of micro-targeted messaging in political communications in their manifold variations – ranging from the clearly deceptive or manipulative message to the confirmatory or engaging – requires a revaluation of the role of information privacy in political campaigns*.[304]

The Queensland Office of the Information Commissioner, Centre for Media Transition (UTS), Reset Australia and the Australian Privacy Foundation also expressed concerns about the potential for voter manipulation brought about by the exemption.[305]

---

[297] *Privacy Act* (n 2) s 6C.
[298] *Privacy Act* (n 2) s 7C.
[299] Privacy Amendment (Private Sector) Bill 2000 Second Reading Speech, 12 April 2000, 15752 ('Second Reading Speech, Private Sector Bill'); *Privacy Act Review Issues Paper*, 33.
[300] Submission to the Issues Paper: Nine, 9.
[301] Submission to the Issues Paper: Cyber Security Cooperative Research Centre, 7.
[302] Submissions to the Issues Paper: Reset Australia, 5; Castan Centre for Human Rights Law - Monash University, 29; Digital Rights Watch, 5; Australian Privacy Foundation, 16; Salinger Privacy, 12; OAIC, 66; Electronic Frontiers Australia, 5; Australian Communications Consumer Action Network, 10; Centre for Media Transition – University of Technology Sydney, 11; Office of the Information Commissioner Queensland, 3.
[303] Submissions to the Issues Paper: Salinger Privacy, 12; Digital Rights Watch, 5; Castan Centre for Human Rights Law - Monash University, 22-23; Australian Privacy Foundation, 16; New South Wales Council for Civil Liberties, 6.
[304] Submission to the Issues Paper: Castan Centre for Human Rights Law - Monash University, 27-28.
[305] Submissions to the Issues Paper: Office of the Information Commissioner Queensland, 3; Centre for Media Transition – University of Technology Sydney, 11; Reset Australia, 5; Australian Privacy Foundation, 16.

The Facebook-Cambridge Analytica matter was frequently raised in submissions which supported removing the exemption,[306] stating that it demonstrates the 'significant risks posed to the integrity of the electoral process when personal information is misused for political ends'.[307] The NSW Council for Civil Liberties noted its concerns about the potential for a similar incident to take place in Australia, stating that 'the activities of Cambridge Analytica, in which personal information was harvested without authorisation for political targeting, would be likely exempt if it were contracted to an Australian political party'.[308]

In the Facebook-Cambridge Analytica matter, individuals on Facebook took a personality test, the results of which (alongside data from their and their friends' Facebook accounts) were later matched with voter profiles in order to determine psychological patterns and to target messages during the 2016 presidential election.[309] The ultimate use of the information was not apparent at the point of collection.

On this issue, the UK ICO stated 'we are concerned about the way in which data was accessed from the Facebook platform and used for purposes it was not intended for or that data subject would not have reasonably expected'.[310] The UK ICO also noted that details around the sale of the data to third parties was not made clear to individuals, nor was the purposes for which it would eventually be processed and used (i.e. for the purposes of targeting messaging for the presidential election).[311]

Different standards for political parties reduces public confidence

Submissions also noted that, in addition to the risks to individuals' privacy, the exemption poses risks to public confidence in Australia's political system. Some suggested that removing the exemption – so that those who exercise or seek power in government adhere to the same standards required of the wider community – could help promote public confidence in Australia's political processes.[312]

The ALRC's 2008 report also expressed this view as part of its recommendation that the political exemption be removed.[313] A number of submissions supported the ALRC's reasoning for removing the exemption – including the Australian Information Security Association, Queensland Office of the Information Commissioner, the Centre for Cyber Security Research and Innovation at Deakin University and the Australian Privacy Foundation.[314]

Security of personal information held by political entities

Some submissions expressed concerns around the security of personal information in light of the exemption, including risks of cyber-attacks and foreign interference.[315] The NSW Council for Civil Liberties recommended that political parties be subject to security requirements under the Act.[316]

---

[306] Submissions to the Issues Paper: New South Wales Council for Civil Liberties, 6; Electronic Frontiers Australia, 5; Office of the Information Commissioner Queensland, 3; Centre for Media Transition – University of Technology Sydney, 11; Reset Australia, 5; Professor Kimberlee Weatherall, 4; OAIC, 65; Australian Communications Consumer Action Network, 10; Australian Privacy Foundation, 16.

[307] Submission to the Issues Paper: Office of the Information Commissioner Queensland, 3.

[308] Submission to the Issues Paper: New South Wales Council for Civil Liberties, 6.

[309] UK ICO, *Investigation into the use of data analytics in political campaigns – Investigation update* (11 July 2018) 17.

[310] Ibid 22.

[311] Ibid 21.

[312] ALRC Report 108 (n 53) 1428; Submissions to the Issues Paper: Office of the Information Commissioner Queensland, 3; Centre for Cyber Security Research and Innovation – Deakin University, 8; Australian Privacy Foundation, 16; Australian Information Security Association, 13; Calabash Solutions, 5.

[313] ALRC Report 108 (n 53) 1428.

[314] ALRC Report 108 (n 53) 1433; Submissions to the Issues Paper: Australian Information Security Association, 13; Office of the Information Commissioner Queensland, 3; Centre for Cyber Security Research and Innovation – Deakin University, 8; Australian Privacy Foundation, 16.

[315] Submissions to the Issues Paper: Palo Alto Networks, 3; Office of the Victorian Information Commissioner, 6.

[316] Submission to the Issues Paper: New South Wales Council for Civil Liberties, 7.

The Australian Privacy Foundation noted that it is difficult to see why political parties should not be subject to data security obligations, amongst other requirements of the Act.[317]

The approach in other jurisdictions

Other jurisdictions have varying models regarding the application of privacy or data protection laws to political parties. In the UK, political parties are subject to data protection legislation, which also recognises the importance of the activities of political parties which facilitate democracy. For example, where political parties in the UK wish to process personal data, they must identify a 'lawful basis' under the *Data Protection Act 2018* (UK) (DP Act) for processing.[318] One lawful basis is the processing of personal data that is necessary for the performance of a task carried out in the public interest.[319]

The DP Act provides further conditions that must be met to rely on this lawful basis to process personal data – including that the processing is *necessary* for an activity that supports or promotes democratic engagement.[320] Additional protections apply where political parties intend to process special category data (similar to 'sensitive information') which includes political opinions.[321]

Guidance from the UK ICO emphasises that political parties must be able to demonstrate the *necessity* of processing political opinion data specifically – that is, if the same political campaigning purpose can be achieved without processing political opinion data, then they cannot rely on this condition.[322]

Under the DP Act, political parties are subject to other data protection obligations, including individuals' rights to object to profiling for direct marketing purposes, access rights and security requirements.[323] Political parties must also have an appropriate policy document in place that sets out matters such as their compliance with data processing principles and policies on retention and erasure of personal data.[324]

In Canada, registered political parties are not subject to federal privacy laws. However, the *Canada Elections Act* S.C requires them to have personal information handling policies as part of registering as a political party.[325] This policy must include statements on the types of personal information the party collects, how the party protects personal information under its control, under what circumstances that personal information may be sold, and the party's practices concerning the collection and use of personal information created from online activity and its use of cookies, among other matters.[326]

Some Australian political parties have privacy statements or policies on their website indicating when they collect personal information, the types of information they collect (including information collected from an individual when they browse the party's website), and some of the ways in which

---

[317] Submission to the Issues Paper: Australian Privacy Foundation, 16.
[318] GDPR (n 26) art 9(2).
[319] GDPR (n 26) art 6(1)(e).
[320] *Data Protection Act 2018* (UK) (n 37) sch 1, pt 2, para (8)(b), (d)-(e).
[321] Under Article 9 of the GDPR, special category data is that revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. *Data Protection Act 2018* (UK) (n 37), sch 1, pt 2, para 22; see also UK ICO, *Guidance on political campaigning: Draft framework code for consultation* (October 2019) 45 ('*Guidance on political campaigning*').
[322] UK ICO, *Guidance on political campaigning* (n 321) 45.
[323] Ibid 7, 64.
[324] *Data Protection Act 2018* (UK) (n 37) sch 1, pt 4.
[325] *Canada Elections Act*, S.C 2000, c. 9, ss 385(2)(k), (4).
[326] Ibid s 385(2)(k).

they may use that information.[327] Some of these statements note that the party follows Australian best practice guidelines for privacy, or that the party's statement on privacy seeks to comply with the Act.[328]

In New Zealand, political parties are required to comply with the *Privacy Act 2020* (NZ). However, that Act does not apply to members of parliament in their official capacity.[329]

Questions

- What would be the impact, if any, on freedom of political communication and the operation of the electoral and political process in Australia if political parties were brought within the scope of the exemption that currently applies to political representatives and contractors, subcontractors and volunteers of political parties and political representatives?
- What would be the benefits and costs of applying some specific APPs to political parties and their affiliates?
    - For example, could political parties and their affiliates be required to have a privacy policy under APP 1 (including information on how individuals can make a complaint about a breach of any applicable APPs), or comply with security obligations under APP 11?

[327] Eg Australian Greens, *Privacy Policy* (Web Page); Australian Labor Party, *Privacy and Legals* (Web Page); Liberal Party of Australia, *Privacy* (Web Page); the National Party of Australia, *Privacy Policy and Disclaimer* (Web Page).
[328] Eg Australian Greens, *Privacy Policy* (Web Page); Australian Labor Party, *Privacy and Legals* (Web Page); Liberal Party of Australia, *Privacy* (Web Page).
[329] *Privacy Act 2020* (NZ) (n 29) s 8(b)(iv).

7. Journalism exemption

The journalism exemption currently exempts from the Act acts or practices engaged in by media organisations in the course of journalism, at a time when the media organisation is publicly committed to standards that deal with privacy that have been published by that organisation or a representative body.[330] The exemption does not apply to other activities of media organisations, such as advertising, subscriptions or competitions.[331]

The Issues Paper sought feedback on whether the journalism exemption appropriately balances the competing interests of privacy and freedom of expression and information, whether the scope of organisations covered should be altered and if some or all of the APPs should apply to any acts or practices of media organisations.

Does the journalism exemption appropriately balance competing interests?

The purpose of the journalism exemption is to balance the public interest in privacy protection with the public interest in allowing a free flow of information to the public through the media.[332] The majority of submissions that commented on this exemption acknowledged the unique position of journalism and the need for there to be special treatment of journalistic activities in relation to the protection of individuals' privacy.

Some submissions – mostly from media organisations – stated that the current scope of the exemption was appropriate. However, a number of submissions considered that its scope permits media organisations to intrude on individuals' privacy with little accountability and irrespective of whether or not the journalism is in the public interest.

Some submissions that argued the current exemption is too broad also supported the introduction of a statutory tort for invasions of privacy.[333] However, with the exception of a handful of case studies, very few submissions cited specific examples of invasions of privacy by media organisations.

There were also a small number of individual submitters that supported removing the exemption altogether to better protect privacy. Two submissions supported its removal on the basis that all exemptions should be removed from the Act.[334]

Scope of entities covered: What is a 'media organisation' and 'journalism'?

The exemption currently applies to a 'media organisation' which is defined as an organisation whose activities consist of, or include, the collection, preparation for dissemination or dissemination of the following material for the purpose of making it available to the public:

a) material having the character of news, current affairs, information or a documentary;
b) material consisting of commentary or opinion on, or analysis of, news, current affairs, information or a documentary.[335]

The term 'journalism' is not defined in the Act. Of those submissions that viewed the exemption as being too broad, some suggested narrowing it through changes to the definitions of 'journalism' and 'media organisation' in the Act. ElevenM and the Centre for Media Transition (UTS) raised concerns about the breadth of these definitions, and that they could result in unintended consequences – that is, entities not intended to be captured by the term 'media organisation' will fall within that

[330] *Privacy Act* (n 2) sub-s 7B(4).
[331] Submission to the Issues Paper: OAIC, 66.
[332] Second Reading Speech, Private Sector Bill (n 299) 15752.
[333] Submissions to the Issues Paper: Electronic Frontiers Australia, 5, 13; Michael Douglas – University of Western Australia, 1-3; Australian Privacy Foundation, 16-17, 37. Consideration of whether a statutory tort for invasions of privacy should be introduced is discussed further in Chapter 26.
[334] Submissions to the Issues Paper: Google, 4; Shogun Cybersecurity, 3.
[335] *Privacy Act* (n 2) sub-s 6(1).

definition, and will potentially seek to rely on the exemption in order to circumvent obligations in the Act.[336] Similarly, the Centre for Media Transition stated that the current exemption does not appropriately balance freedom of expression with the privacy of individuals – particularly given the proliferation of social media, and the potential expansion of who may be considered a 'media organisation' for the purposes of the exemption. They stated that the exemption should focus on professional journalistic activities, not the work of bloggers or other information disseminators.[337]

Submissions from some media organisations, including the ABC, Commercial Radio Australia, FreeTV and Nine, suggested that the concepts of 'journalism' or 'media organisation' (or both) could be amended to broaden the scope of the exemption.[338] However, other submissions from media organisations, including from Australia's Right to Know Coalition, the Guardian Australia, the New York Times and SBS, stated that the exemption strikes the right balance and supported retaining it in its current form.[339]

Scope of activities covered 'in the course of journalism'

Some submissions considered that the current scope of the exemption is not broad enough to ensure freedom of expression by the media. Nine's submission suggested amending the exemption to include 'acts or practices engaged in by media organisation in relation to news, artistic, entertainment and documentary content', noting that there is genuine public interest and artistic value in telling stories that would fall within these broader categories.[340] Nine cited its television series *Informer 3838*, a drama based on the story of Nicola Gobbo, as an example of the type of content which it considers is unclear as to whether the journalism exemption applies.[341]

Overseas data protection frameworks provide exemptions for journalism as well as other 'special purposes' in recognition of their role in supporting the right to freedom of expression and information.[342] For example, the GDPR provides for exemptions from certain data protection obligations for the 'special purposes' of journalism, or for the purposes of academic, artistic or literary expression.[343] Canada's *Personal Information Protection and Electronic Documents Act 2000* (PIPEDA) also exempts entities from the operation of that Act to the extent that the entity collects, uses or discloses personal information for journalistic, artistic or literary purposes.[344] Nine and FreeTV considered that broadening the exemption under the Act would more closely align Australia's approach with these international frameworks.[345]

Self-regulation of privacy standards by media organisations

In order to attract the exemption, a media organisation in the course of journalism must also be publicly committed to observe standards that deal with privacy, and publish those standards in writing.[346] This creates a privacy self-regulation model for media organisations where they are then bound by those standards rather than the standards in the Act.

---

[336] Submissions to the Issues Paper: ElevenM, 3; Cyber Security Cooperative Research Centre, 7; Centre for Media Transition – University of Technology Sydney, 12.
[337] Submissions to the Issues Paper: Centre for Media Transition – University of Technology Sydney, 12-13.
[338] Submissions to the Issues Paper: ABC, 5; Free TV, 16; Commercial Radio Australia, 3; Queensland Council for Civil Liberties, 5.
[339] Submissions to the Issues Paper: SBS, 5; The New York Times, 2; Australia's Right to Know Coalition, 1; The Guardian Australia, 7-8.
[340] Submission to the Issues Paper: Nine, 3.
[341] Ibid.
[342] GDPR (n 26) rec 153.
[343] GDPR (n 26) art 85(2).
[344] *PIPEDA* (n 28) sub-s 4(2)(c).
[345] Submissions to the Issues Paper: Nine, 3; Free TV, 16.
[346] *Privacy Act* (n 2) sub-s 7B(4).

The Law Council of Australia's submission expressed concern about the lack of accountability in this self-regulation model, raising that they are effectively free of any sanctions or real negative incentives under this arrangement. [347] Similarly, Privacy108 noted that relying on effective enforcement of media standards by self-regulatory bodies is a flawed approach, and that the current model has resulted in inadequate outcomes for Australians.[348] Some submissions noted that a media organisation need only 'publicly commit' to standards that deal with privacy, which could involve little more than a statement on a website and places no obligation on media organisations to have complaints processes in place for individuals.[349]

Alternative approaches to increasing privacy protections

While submissions recognised the importance of the public interest in allowing a free flow of information to the public through the media, a number of submitters expressed support for modifying the exemption to increase protection for individuals while continuing to fulfil its purpose.

Public interest requirement

Some submissions suggested introducing a public interest test into the journalism exemption, so that it would only apply where journalism is, on balance, in the public interest. If that requirement was not met, the Act would apply.

The DP Act, which imports the GDPR exemption for journalism, applies a public interest test to the exemption. That is, the exemption will only apply where there is a reasonable belief that the publication of the journalistic material would be in the public interest.[350] In determining whether publication would be in the public interest, consideration must be given to 'the special importance of the public interest in the freedom of expression and information'.[351]

In its 2008 report, the ALRC recommended introducing a definition of journalism including material in respect of which the public interest in disclosure outweighs the public interest in maintaining the level of privacy protection afforded under the APPs.[352]

In his submission, Michael Douglas of the University of Western Australia recommended a similar approach to that of the ALRC.[353] Mr Douglas commented:

> *The privilege is justified on the basis that media organisations engaged in 'journalism' serve the public interest by conducting their work. If media organisations do not serve the public interest, then the rationale for the exemption falls away*.[354]

The Arts Law Centre of Australia submitted that journalism should be defined to limit the scope of the exemption to protect information where there is a recognisable public interest in disclosure, noting that the media does not always report on matters of public interest.[355] Another submission noted that what is in the 'public interest' does not always correlate with that in which the public is interested.[356] The NSW Council for Civil Liberties also recommended a definition of journalism to

---

[347] Submissions to the Issues Paper: Law Council of Australia, 17; Privacy 108, 6-7.
[348] Submissions to the Issues Paper: Salinger Privacy, 13;
[349] Submissions to the Issues Paper: Centre for Media Transition – University of Technology Sydney, 13; Privacy108, 6-7.
[350] *Data Protection Act 2018* (UK) (n 37) sch 2, pt 5, sub-para 26(2).
[351] Ibid sch 2, pt 5, sub-para 26(4).
[352] ALRC Report 108 (n 53) 1452 (recommendation 42-1). Note: this definition proposed by the ALRC refers to model Unified Privacy Principles (UPPs), being the ALRC's recommended consolidation of the Information Privacy Principles and National Privacy Principles (Recommendation 18-2).
[353] Submission to the Issues Paper: Michael Douglas – University of Western Australia, 2.
[354] Ibid 1.
[355] Submission to the Issues Paper: Arts Law Centre of Australia, 5.
[356] Submission to the Issues Paper: Michael Douglas – University of Western Australia, 1. See also: ACCC, DPI report (n 2) 284.

limit the exemption to those acts and practices associated with a clear public interest in the freedom of expression.[357]

Salinger Privacy suggested a more limited exemption apply to media organisations for collection, use and disclosure for activities necessary to the conduct of investigative and public interest journalism.[358] Other submissions agreed with this approach,[359] which would apply the remaining APPs, such as security requirements under APP 11, to media organisations in the course of journalism.

Public interest tests are present in other areas of law, including defamation, freedom of information and administrative law.[360] These areas of law provide for a range of factors to be considered when determining whether a particular matter is in the public interest, including:

- the importance of freedom of expression in discussing issues of public interest[361]
- informing debate on a matter of public importance[362]
- the urgency of the matter for which the disclosure is made[363]
- the steps taken to verify the information which is being disclosed[364]
- whether the disclosure was made with malice[365]
- promoting integrity and accountability of the public sector[366]
- whether the disclosure would prejudice the administration of justice,[367] and
- whether the matter disclosed relates to the performance of public functions or activities.[368]

Security obligations

A number of submissions considered that APP 11 specifically should apply to media organisations. If security obligations were to apply to media organisations, they would be required to take reasonable steps to protect the personal information they hold from misuse, interference and loss; and unauthorised access, modification or disclosure.[369] They would also be subject to destruction requirements under APP 11.2 once they no longer required the personal information they had collected, used or disclosed in the course of journalism that fell within the exemption.[370]

The DP Act in the UK applies modified reporting obligations to media organisations in the context of its data breach notification scheme, removing the obligation to notify affected individuals of a data breach if the entity reasonably believes that doing so would be incompatible with the special purpose (such as journalism).[371] In such cases, entities must only notify the supervisory authority.[372] This recognises that it may not be appropriate for media organisations to alert individuals whom they are investigating to that fact via a data breach notification.

---

[357] Submission to the Issues Paper: New South Wales Council for Civil Liberties, 7.
[358] Submission to the Issues Paper: Salinger Privacy, 13.
[359] Submissions to the Issues Paper: Australian Privacy Foundation, 17; Australian Information Security Association, 13.
[360] *Defamation Amendment Act 2020* (NSW) ('*Defamation Act*'); *Freedom of Information Act 1982* (Cth) ('*FOI Act*'); *Public Interest Disclosure Act 2013* (Cth) ('*PID Act*').
[361] *Defamation Act* (n 360) sch 1, item 27, para 29A(3)(i).
[362] *FOI Act* (n 360) para 11B(3)(b).
[363] *Reynolds v Times Newspapers Ltd and Others* [1999] 3 WLR 1010, 1027: Urgency was one of the ten factors set out by Lord Nicholls against which the qualified privilege defence in defamation law should be determined.
[364] Ibid: This was another one of the ten factors set out by Lord Nicholls in this case.
[365] Defamation Amendment Bill 2020 (NSW), Explanatory Note, 9.
[366] *PID Act* (n 360) sub-para 26(3)(aa).
[367] Ibid sub-para 26(3)(d).
[368] *Defamation Act* (n 360) sch 1, item 27, sub-para 29A(3)(c).
[369] *Privacy Act* (n 2) sch 1, APP 11.1.
[370] Ibid sch 1, APP 11.2.
[371] GDPR (n 26) art 34; *Data Protection Act 2018* (UK) (n 37) sch 2, pt 5, sub-para 26(9)(c)(i).
[372] GDPR (n 26) art 33; *Data Protection Act 2018* (UK) (n 37) sch 2, pt 5, sub-para 26(9)(c).

Strengthening the self-regulation model

The Centre for Media Transition (UTS) suggested that media and news organisations should be subject to a single standards scheme that would apply across different platforms, and could be supported financially by digital platforms as distributors of news.[373] Submissions from the OAIC and Salinger Privacy suggested that media industry complaints handling bodies, such as the Australian Press Council (APC), could be recognised as an approved External Dispute Resolution (EDR) body under section 35A of the Act.[374] This would enable a greater level of oversight by the Information Commissioner.[375]

The DP Act contains a number of oversight measures in relation to the journalism exemption under that Act. For example, the Secretary of State must report to Parliament every three years on the use and effectiveness of the media's dispute resolution procedures in cases involving failures or alleged failures to comply with data protection legislation.[376] The UK Information Commissioner must also publish guidance about how to seek redress against media organisations where they have failed to comply with data protection legislation.[377]

Questions

- What further evidence is available, such as case studies and any quantitative evidence, to indicate that acts or practices engaged in by media organisations in the course of journalism are presently posing a risk to individuals' privacy?
- What impact would introducing a public interest requirement into the journalism exemption have on the free flow of information to the public through the media?
- What might be the positive or adverse consequences of applying security obligations under APP 11 to media organisations in the course of journalism?
- How could the self-regulation model for media organisations under the journalism exemption be improved?

[373] Submission to the Issues Paper: Centre for Media Transition – University of Technology Sydney, 14.
[374] Submissions to the Issues Paper: OAIC, 66; Salinger Privacy, 13.
[375] Submissions to the Issues Paper: OAIC, 66.
[376] *Data Protection Act 2018* (UK) (n 37) s 179.
[377] Ibid s 177.

Part 2: Protections

8. Notice of collection of personal information

The Issues Paper sought feedback on the ACCC's DPI report recommendations relating to notice and consent, which were supported by the government in principle.[378] The Issues Paper also sought input on how these mechanisms could be improved, whether notice and consent is an effective way for individuals to manage their personal information, and whether there should be more substantive regulation of permissible collections, uses and disclosures under the Act.

The current operation of APP 1 and APP 5

APP 1 requires APP entities to maintain a clearly expressed and up-to-date privacy policy that contains the matters listed in APP 1.4.[379] APP 5.1 requires that at the time of collection, or as soon as is practicable after collection, an APP entity must take such steps (if any) as are reasonable in the circumstances, to notify, or otherwise ensure that the relevant individual is aware of certain matters.[380] Under APP 5, an APP entity must notify an individual of the identity and contact details of the APP entity, the purposes for which the APP entity is collecting the personal information, and other persons or APP entities to whom the collecting entity normally discloses personal information, among other matters.[381]

The APP Guidelines acknowledge that it may not be reasonable to provide notice to an individual in certain circumstances, such as where:

- the individual is already aware of the APP 5 matters
- notification may pose a serious threat to life, health or safety
- notification would be inconsistent with other legal obligations, or
- it would be impracticable to do so.[382]

The role and importance of notice

A large number of submitters were of the view that notice is an important transparency mechanism in the Act.[383] Notice was considered a key component of any privacy reform (irrespective of the role of consent) as it is pivotal in communicating to individuals how their personal information is being handled. The OAIC noted that the transparency provided by privacy policies and notices enables individuals to decide whether 'to exercise control in how they deal with a service (such as adjusting privacy settings) or decide not to engage with the [service]' while also assisting regulators in holding entities to account.[384]

---

[378] Treasury, DPI response (n 18) 17.

[379] *Privacy Act* (n 2) sch 1, APPs 1.3, 1.4.

[380] *Privacy Act* (n 2) sch 1, APP 5. See also, Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill (Cth) 2012:

> The phrase 'reasonable in the circumstances' is an objective test that ensures that the specific circumstances of each case have to be considered when determining the reasonableness of the steps in question. This flexibility is necessary given the different types of APP entities and functions/activities that are to be regulated under the APPs. In many cases, it would be reasonable in the circumstances for an APP entity to provide the information outlined in APP 5.2.

[381] *Privacy Act* (n 2) sch 1, APP 5.2.

[382] OAIC, APP Guidelines (n 21) [5.7].

[383] Submissions to the Issues Paper: ANZ, 7; Atlassian, 4; Australian Financial Markets Association, 7; Australian Information Security Association, 14; Australian Privacy Foundation, 17; CAIDE and MLS, 5; Consumer Policy Research Centre, 6; CSIRO, 5; Deloitte, 10; Experian, 7; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 16; Financial Services Council, 14; Google, 4; Interactive Games and Entertainment Association, 10; Legal Aid Queensland, 8; OAIC, 69; Obesity Policy Coalition, 5; Office of the Victorian Information Commissioner, 6–7; Optus, 5; Salinger Privacy, 14.

[384] Submission to the Issues Paper: OAIC, 68.

Issues identified with APP 1 and APP 5

The DPI report expressed concern that APP entities currently have significant discretion under APP 5 as to whether individuals are notified about the collection of their personal information and how that notice is provided.[385] Submissions indicated particular concern about the heightened privacy risks to consumers stemming from the use and disclosure of personal information collected by third parties without the awareness of the individual.[386]

In order to increase the transparency of personal information handling and reduce information asymmetries between APP entities and individuals, the ACCC recommended that all collections should be accompanied by notice (unless the individual already has the information or there is an overriding legal or public interest reason), that notices should be concise, transparent and written in clear and plain language, and, where possible, any associated information burden could be reduced through the use of standardised icons or phrases.[387]

Some submitters considered that more clarity could be provided about when a notice is required and supported reforms or initiatives that would standardise notice provisions or provide for uniform phrases or icons to communicate privacy information.[388]

Proposals

APP 5 notices to be clear, current and understandable

A number of submitters argued that privacy notices currently provided by APP entities do little to enhance individuals' understanding of how their personal information will be handled. Long and complex privacy policies and notices were said to obscure rather than enhance transparency.[389]

Submitters were broadly supportive of introducing requirements to enhance the clarity of APP 5 notices,[390] and suggested that this could be addressed by expressly requiring in the Act that entities provide clear, current and understandable privacy notices.[391] Some submitters cautioned against introducing overly prescriptive notice requirements.[392] Facebook submitted that 'legal frameworks

---

[385] ACCC, DPI report (n 2) 461.

[386] Submissions to the Issues Paper: ACCC, 3; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 6; CAIDE and MLS, 7–8; Consumer Policy Research Centre, 6; Deloitte, 12–13; Dr Katharine Kemp, 12–13; New South Wales Council for Civil Liberties, 8; Obesity Policy Coalition, 6.

[387] ACCC, DPI report (n 2), recommendation 16(b).

[388] Submissions to the Issues Paper: The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 6; ANZ, 7–8; AusPayNet, 7; Australian Department of Health, 5; Australian Information Security Association, 14; Australian Privacy Foundation, 18; CAIDE and MLS, 6; Centre for Cyber Security Research and Innovation, 8; Consumer Policy Research Centre, 6; CSIRO, 6; Cyber Security Cooperative Research Centre, 8; Deloitte, 14–16; Dr Katharine Kemp, 15; Experian, 9; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 17; KPMG, 15; New South Wales Information and Privacy Commission, 3; OAIC, 74; Obesity Policy Coalition, 6; Queensland Law Society, 4; Royal Australian College of General Practitioners, 3; Salinger Privacy, 15; SBS, 7.

[389] Submissions to the Issues Paper: Australian Department of Health, 4; Consumer Policy Research Centre, 5; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 16; Financial Services Council, 14; Legal Aid Queensland, 8; Salinger Privacy, 14.

[390] See, eg, Submissions to the Issues Paper: OAIC, 73–4; Deloitte, 11; Consumer Policy Research Centre, 6; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 17; Experian, 7; Australian Information Security Association, 14; Australian Department of Health, 4; Data Synergies, 37; Royal Australian College of General Practitioners, 3; Cyber Security Cooperative Research Centre, 8; SBS, 6–7.

[391] Submitters supported adopting a requirement based on the terminology in Article 12(1) GDPR, which requires communications to the data subject to be presented in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language'. See, eg, Submissions to the Issues Paper: OAIC, 74; Deloitte, 11; Ramsay Healthcare, 5; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 17; Data Synergies, 37; Free TV Australia, 14; Royal Australian College of General Practitioners, 3; SBS, 6–7.

[392] Submissions to the Issues Paper: Microsoft Australia, 4; Facebook, 28; Interactive Games and Entertainment Association, 11.

should provide enough flexibility to permit, and indeed encourage, a range of design practices that may be appropriate across a variety of contexts'.[393]

The proposed requirement would bring the Act in alignment with international jurisdictions such as the EU and the UK, which maintain equivalent requirements in legislation.[394] The proposed clear notice requirement would be flexible enough to permit different approaches across government and different industry sectors, and could be supported by industry-specific codes or Commissioner-issued guidelines to further enhance individuals' engagement with, and comprehension of, privacy notices.[395]

This would build on the requirement in the OP code that APP 5 notices provided by social media services, data brokerage services and large online platforms must be 'clear, current and understandable', but would apply to all APP entities covered by the Act.[396]

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

Clarifying the interaction between privacy notices and privacy policies

Some submitters also considered whether the interaction between APP 1 and APP 5 should be clarified, and whether APP 5 privacy notices should be shortened and simplified to contain only relevant matters that individuals are most likely to be interested in, such as 'more obtrusive collection practices and uses'.[397] It was considered that a layered approach may assist individuals' understanding, whereby individuals receive notice of the most relevant and important matters at the point of collection in a clear and concise form,[398] and that entities have the flexibility to make such notices brief while offering additional details in supporting privacy policies to individuals who want further information. ANZ suggested that the Act should make explicit that the provision of a hyperlink to where individuals may find privacy information satisfies the obligation to ensure the individual has been made aware of the relevant matters, even though the individual may choose not to access it.[399]

The OAIC's submission considered the relationship between privacy policies required by APP 1 and privacy notices under APP 5, and noted that APP 1 privacy policies provide high-level information to the world at large about how an organisation generally handles personal information.[400] In contrast,

---

[393] Submission to the Issues Paper: Facebook, 29.

[394] GDPR (n 26) art 12 requires the provision of privacy information in 'concise, transparent, intelligible and easily accessible form, using clear and plain language'. Canada's proposed Consumer Privacy Protection Act would require privacy policies to be readily available and in 'plain language', and information accompanying consent requests must also be provided in 'plain language': Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, 2nd sess, 43rd Parl, 2020 ('Bill C-11'). Bill C-11 died on the Order Paper when the Canadian federal election was called on 15 August 2021. If the incoming government wishes to propose legislative changes to PIPEDA (n 28) a new bill will have to be introduced to the Parliament.

[395] Submission to the Issues Paper: OAIC, 73–4.

[396] Exposure Draft, OP Bill (n 1); Explanatory Paper, OP Bill (n 1). The OP code is also required to set out how notice will apply specifically in relation to children or other groups of people not capable of making their own privacy decisions – see further at chapter 13.

[397] Submissions to the Issues Paper: Queensland Law Society, 4. See also, OAIC, 70–1; Salinger Privacy, 15; Australian Department of Health, 4–5; Australian Privacy Foundation, 17; Data Synergies, 6.

[398] See, eg, Submissions to the Issues Paper: OAIC, 73; Deloitte, 14; Experian, 9–10; Centre for Cyber Security Research and Innovation, 8; New South Wales Information and Privacy Commission, 3; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 17; KPMG, 15; Australian Information Security Association, 14; Australian Financial Markets Association, 7; Data Synergies, 38; Cyber Security Cooperative Research Centre, 8; Optus, 5–6; AusPayNet, 7.

[399] Submission to the Issues Paper: ANZ, 7. See also, Data Synergies, 38–9.

[400] Submission to the Issues Paper: OAIC, 69.

the OAIC's view was that an APP 5 notice is designed to provide specific information relevant to a particular collection of personal information.[401]

The Act could be amended to shift some of the information that is currently required to be contained in an APP 5 notice into an APP entity's privacy policy. This would promote enhanced comprehension of privacy information as notices provided at the point of collection would be limited to the information that is most pertinent to an individual's decision regarding whether to provide their personal information to an entity. Specifically, a privacy notice would not include the matters set out in APP 5.2(c),(e),(i) and (j), which would be moved into the privacy policy. The privacy policy would also include a number of new matters, as set out in Chapter 20.

Limiting the information provided in notices may also promote the adoption of layered approaches to the provision of privacy information. This would encourage innovation by entities to structure their notices in a manner that provides individuals with the most crucial information at the time their personal information is collected while ensuring that additional information is easily accessible for individuals who wish to access further detail about how their information is handled at a later date.

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.

Standardisation of APP 5 notices

There was broad support for the DPI report's recommendation[402] to limit information burden through the use of standardised icons or phrases where possible.[403] The Centre for AI and Digital Ethics and Melbourne Law School (CAIDE and MLS) recommended 'a standard format for privacy notices that will allow consumers to develop expertise in reviewing and understanding the scope of collection policies'.[404]

Standardised information delivery has been used successfully in other regulatory contexts, including the use of standardised food nutrition tables, as well as the ongoing development of standardised consent taxonomies as part of the CDR standards.[405] International data protection laws also

[401] Submission to the Issues Paper: OAIC, 69.
[402] ACCC, DPI report (n 2) Recommendation 16(b).
[403] Submissions to the Issues Paper: OAIC, 74; ANZ, 7–8, Queensland Law Society, 4; Cyber Security Cooperative Research Centre, 8; Deloitte, 14–16; CAIDE and MLS, 6; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 6; SBS, 7; AusPayNet, 7; Experian, 9; Consumer Policy Research Centre, 6; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 17; Obesity Policy Coalition, 6; Dr Katharine Kemp, 15; Salinger Privacy, 15; Australian Information Security Association, 14; Australian Department of Health, 5; Australian Privacy Foundation, 18; Royal Australian College of General Practitioners, 3; Centre for Cyber Security Research and Innovation, 8; New South Wales Information and Privacy Commission, 3; KPMG, 15.
[404] Submission to the Issues Paper: CAIDE and MLS, 6.
[405] Data61, 'Consumer Experience', *Consumer Data Standards* (Web Page, April 2021) ('*Consumer Data Standards*').

contemplate the future development of standardised privacy notices or methods through which individuals may exercise privacy rights, including the GDPR[406] and California's CCPA.[407]

Some submitters considered that standardised notices or icons may oversimplify complex personal information handling processes, which may not be consistent between industry sectors or across government.[408] These submitters indicated that APP entities already have flexibility to notify individuals in a manner they consider to be effective, provided that it meets the principles of how notice should be provided.

Due to the wide range of contexts in which the Act applies, it is likely to be impractical to develop privacy notice templates, lexicon or icons that could be standardised across all APP entities.[409] For example, the collection notice methods of an online retailer, government agency, medical practitioner or CCTV operator are likely to vary depending on the context, and each entity is likely to collect, use and disclose personal information in different ways.

The development of standardised privacy notices, including standardisation of layouts, wording and icons may be a strong opportunity for reform on a sector-specific basis, such as through the OP code.[410] The OP Bill requires that the OP code must make provision for ensuring an individual is aware of the purposes for which an organisation collects, uses and discloses personal information, and must set out how an organisation is required to comply with this provision and existing requirements in APP 5. When meeting these requirements, the OP code developer could consider requiring the development of standardised privacy notices by organisations subject to the code, including standardised layouts, wording and icons. This approach would allow the OAIC and industry to work towards standardisation, which through appropriate use would allow an entity to use icons to comply with their APP 5 notice obligations. As noted in the DPI report, the design of effective information notices that limit 'information overload' will likely depend on comprehensive consumer testing.[411]

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.

Expanding the situations where notice is required

The DPI report recommended that all collections of personal information (whether directly from the consumer or indirectly as a third party) be accompanied by a privacy notice, unless the consumer already has the information or an overriding legal or a public interest reason applies.[412]

The Act does not expressly address the extent to which APP 5 notices are required for indirect collections of personal information. OAIC guidance states that 'the requirement to notify or ensure awareness of the APP 5 matters applies to all personal information 'collected' about an individual, either directly from the individual or from a third party'.[413]

Some submitters considered that the current requirement that an entity merely take 'such steps (if any) as reasonable in the circumstances'[414] leaves entities with 'significant discretion' about whether to provide notice, and expressed concern that significant privacy risks may result from

[406] GDPR (n 26) art 12(7).
[407] CCPA (n 27) § 1798.185(a)(4)(C).
[408] Submissions to the Issues Paper: Facebook, 30; Griffith University, 10; Optus, 6; Ramsay Healthcare, 5.
[409] Submission to the Issues Paper: Communications Alliance, 10.
[410] Exposure Draft, OP Bill (n 1); Explanatory Paper, OP Bill (n 1).
[411] ACCC, DPI report (n 2) 463.
[412] ACCC, DPI report (n 2) Recommendation 16(b).
[413] OAIC, APP Guidelines (n 21) [5.2].
[414] *Privacy Act* (n 2) sch 1 APP 5.1.

indirect collections that take place without an individual being notified.[415] Submitters' concerns were primarily related to the widespread sharing of personal information in the adtech ecosystem without an individual's knowledge.[416] The DPI report, in examining data practices in advertising services, cited 'an Australian study of medicine-related Android apps [which] found that "19 of the 24 apps shared data outside of the app to a total of 55 entities, owned by 46 parent companies" including personal information such as email addresses, medical conditions and drug lists'.[417]

It was proposed that collection notices should be required in a greater range of circumstances, including for indirect collections. Relevantly, the Office of the Victorian Information Commissioner submitted that:

> *A potential approach to strengthening notification in respect of personal information collected indirectly could be a model similar to Article 14 of the GDPR, which requires entities to provide notice to individuals whose information has been collected indirectly, unless one of several exceptions applies – for example, the provision of such information is impossible or would involve a disproportionate effort*.[418]

Some submitters cautioned that Recommendation 16(b) of the DPI report could place a greater burden on industry while also overwhelming individuals who may subsequently suffer from 'notice fatigue' and 'information overload'.[419] The OAIC recommended striking a balance between strengthened notice requirements and minimising potentially negative consequences of more frequent notifications such as notification fatigue.[420] In discussing the limitations of privacy notices, the OAIC noted that 'it is unreasonable to expect individuals to engage meaningfully with notices from the large (and likely increasing) number of APP entities seeking to handle their personal information'.[421]

Some submitters considered that despite potential difficulties associated with notifying individuals in circumstances where personal information has been collected indirectly (such as by a third party), the ACCC's recommendation to strengthen notice requirements is consistent with consumer expectations and more closely aligned to similar international requirements, such as the GDPR.[422]

While there is merit in enhancing transparency by placing a heavier obligation on APP entities to provide notice, some flexibility in the requirement to provide notice should be retained for situations where notice is unnecessary as the individual is already aware of the matters that would be notified and where providing notice would be impossible or would involve disproportionate effort, or may actually be harmful. Examples of such situations are set out in the APP Guidelines, including where notification may pose a serious threat to the life, health or safety of an individual or

---

[415] Submission to the Issues Paper: Deloitte, 13; Consumer Policy Research Centre, 6–7; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 17–18. See also Cyber Security Cooperative Research Centre, 8; Dr Katharine Kemp, 2, 12–13; ACCC, DPI report (n 2) 461.

[416] Submissions to the Issues Paper: Dr Katharine Kemp, 6, 13, 16; Salinger Privacy, 16–18; Cyber Security Cooperative Research Centre, 8. See also ICO, *Update Report into Adtech and Real Time Bidding* (Web Page, June 2019) 23.

[417] Willis and Bogle, 'Data sharing by popular health apps found to be 'routine', prompting calls for more transparency,' *ABC* (online, 22 March 2019) cited in ACCC, DPI report (n 2) 450.

[418] Submission to the Issues Paper: Office of the Victorian Information Commissioner, 7–8.

[419] Submission to the Issues Paper: Australian Industry Group, 14–15; Experian, 7; Facebook, 30. See also, Atlassian, 4.

[420] Submission to the Issues Paper: OAIC, 73. See also CSIRO, 5; Data Synergies, 38.

[421] Submission to the Issues Paper: OAIC, 71. See also Aleecia McDonald and Lorrie Cranor, 'The Cost of Reading Privacy Policies' (2008) 4(3) *A Journal of Law and Policy for the Information Society* 543, 562–5, where the authors estimated that the average time required for American internet users to read all privacy policies encountered in a year was 201 hours per year.

[422] Submissions to the Issues Paper: Deloitte, 13; Consumer Policy Research Centre, 6.

public health or safety, or where a law enforcement agency obtains personal information from a confidential source for the purpose of an investigation.[423]

Submitters indicated that the delivery of privacy notices may also be unnecessary where third party collections occur exclusively to facilitate another APP entity's purpose. Submitters noted that it is not uncommon for entities to engage specialist contractors to assist them with their business operations, where the 'purpose for which the personal information is being used has not materially changed and the risk of a consumer getting notification fatigue from receiving multiple notices is high'.[424] KPMG submitted that broadening the requirements to provide notice across a supply chain over and above the original notice would lead to a greater burden on individuals as well as notice fatigue.[425] However, the Australian Privacy Foundation proposed that where a third-party collection takes place there should also be a duty on the APP entity to require (by contract or otherwise) the third party to deliver the notice.[426]

The Review is seeking input on whether Proposal 8.4 is sufficiently flexible to allow an APP entity to not provide notice where it collects, uses or discloses personal information only on behalf of another APP entity that is responsible for determining the purposes and means of personal information handling, or whether it would be appropriate to introduce a specific exemption to notice requirements for this situation. Chapter 21 seeks feedback on whether introducing the concept of controllers and processors into the Act would be beneficial. If adopted, this distinction could clarify notice obligations for entities in these circumstances.[427]

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?

[423] OAIC, APP Guidelines (n 21) [5.7].
[424] Submission to the Issues Paper: Telstra, 8. Telstra noted, as examples, that entities may use printing houses to print customer bills or IT helpdesks to help resolve customer IT complaints. See also Submissions to the Issues Paper: Data Synergies, 38; Atlassian, 4.
[425] Submission to the Issues Paper: KPMG, 14. See also Submission to the Issues Paper: Atlassian, 4.
[426] Submission to the Issues Paper: Australian Privacy Foundation, 18.
[427] Submission to the Issues Paper: Atlassian, 4.

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

The Issues Paper sought feedback on the DPI report recommendations in relation to consent[428] and whether consent is an effective way for people to manage their personal information.

The Review received submissions on the role of consent in the Act from stakeholders across a range of sectors including academia, industry, technology companies, not-for-profits and peak bodies. There was general agreement from feedback received that consent is an important mechanism but is most effective when used in narrowly defined situations where individuals most need to exert control over their personal information.[429]

The current consent requirements

Consent is currently only required for a limited range of collections, uses and disclosures of personal information. Consent is generally needed for the collection of sensitive information, unless an exception applies.[430] Consent also functions as an exception permitting APP entities to use or disclose personal information for a secondary purpose.[431] Finally, consent may be relied on to authorise the use or disclosure of personal or sensitive information for the purposes of direct marketing in certain circumstances,[432] or as a basis for cross-border disclosures of personal information.[433]

The current definition of consent in the Act specifies that consent can be express or implied.[434] The Act provides no further clarification on the concept of consent. The APP Guidelines state that a number of conditions must exist for consent to be valid, including that consent be 'informed, voluntary, current and specific, and given with capacity' and provide the following guidance on implied consent:

> *Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity. An APP entity should not assume that an individual has consented to a collection, use or disclosure that appears to be advantageous to that person. Nor can an entity establish implied consent by asserting that if the individual knew about the benefits of the collection, use or disclosure, they would probably consent to it… An APP entity cannot infer consent simply because it provided an individual with notice of a proposed collection, use or disclosure of personal information. It will be difficult for an entity to establish that an individual's silence can be taken as consent.*[435]

Should consent be required in additional circumstances?

The Issues Paper sought views on whether it would be beneficial to require individuals' consent for any collection, use or disclosure unless necessary for the performance of a contract, legal

---

[428] ACCC, DPI report (n 2) Recommendation 16(c).

[429] Submissions to the Issues Paper: Salinger Privacy, 18; OAIC, 70–2, 76–7; Law Council of Australia, 17–18; Snap Inc, 3; Law Institute of Victoria, 8; Telstra Corporation Ltd and Telstra Health Pty Ltd, 9; New York Times, 2; Microsoft Australia, 3–4; Communications Alliance, 6–7; Australian Industry Group, 16-17; Ramsay Healthcare, 6; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 22; Association for Data-Driven Marketing and Advertising, 16–17; Experian, 11; Google, 7; New South Wales Council for Civil Liberties, 8; Privacy108, 11; GroundUp Consulting, 6; Optus, 7; Woolworths, 2; CSIRO, 6; CHOICE, 2–3; Queensland Law Society, 5–6; Queensland University of Technology Faculty of Law, 33; Interactive Games and Entertainment Association, 12; ANZ, 9; Data Synergies, 6, 39–40.

[430] *Privacy Act* (n 2) sch 1 APP 3.3, 3.4. See also cl 3.6(a) which permits agencies to collect personal information indirectly on the basis of consent.

[431] *Privacy Act* (n 2) sch 1 APP 6.1(a).

[432] *Privacy Act* (n 2) sch 1 APP 7.3, 7.4.

[433] *Privacy Act* (n 2) sch 1 APP 8.2.

[434] *Privacy Act* (n 2) s 6.

[435] OAIC, APP Guidelines (n 21) [B.37]–[B.39].

requirement, or public interest reason, as recommended in the DPI report. [436] Submitters considered that while consent is necessary in some cases, it should be relied upon as rarely as possible given limits to individuals' time and energy. Submitters overwhelmingly opposed moving to a position where consent has a more prominent role in authorising personal information handling under the Act.[437] Submitters' concerns included:

- that requiring the provision of consent in additional circumstances would lead to consent fatigue, where individuals are overwhelmed with the number of consent requests that they receive, are less able to effectively engage with those consents, and therefore are less likely to be providing effective consent[438]
- that it would be unnecessarily burdensome on APP entities to obtain consent in situations where an individual may not want or need to provide consent, particularly where a collection, use or disclosure of personal information would be reasonably expected by the individual or broader community[439]
- that consent places a burden on individuals to understand and consider complex data handling practices, unknown privacy harms that may materialise in the future and the many purposes for which their personal information may be handled, rather than allowing them to be confident that the purpose falls within appropriate confines (for example, that the collection, use or disclosure will not be harmful to the individual),[440] and
- consent is only meaningful where the individual has a voluntary choice; this is not the case where individuals feel resigned to consenting to the use of their information to access online services, as they do not consider there is any alternative.[441]

The New York Times submitted that consent should be necessary in some cases but ideally relied upon as rarely as possible as people have limited resources of time and energy to dedicate to understanding the specifics of a business's data handling processes, which 'should be treated with

---

[436] ACCC, DPI report (n 2) Recommendation 16(c).

[437] Submissions to the Issues Paper: Salinger Privacy, 18; OAIC, 70–2, 76–7; Law Council of Australia, 8, 17–18; Dr Kate Mathews Hunt, 9–10; Snap Inc, 3; Law Institute of Victoria, 8; New York Times, 2; Electronic Frontiers Australia, 8–9; Communications Alliance, 6; Australian Industry Group, 16; Ramsay Healthcare, 6; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 22; Telstra Corporation Ltd and Telstra Health Pty Ltd, 9; Association for Data-Driven Marketing and Advertising, 17; Experian, 11; ElevenM, 2; New South Wales Council for Civil Liberties, 8; Professor Kimberlee Weatherall, 6–8; Privacy108, 11; GroundUp Consulting, 6; Woolworths, 2; CSIRO, 6; CHOICE, 1–3; Queensland Law Society, 5–6; Queensland University of Technology Faculty of Law, 33; Interactive Games and Entertainment Association, 12; ANZ, 9; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 7; Facebook, 32–3; Data Synergies, 40.

[438] Submissions to the Issues Paper: OAIC, 70–72, 76; Snap Inc, 3; Law Council of Australia, 17; New York Times, 2; Electronic Frontiers Australia, 8; Communications Alliance, 6; Australian Industry Group, 16; Telstra Corporation Ltd and Telstra Health Pty Ltd, 9; Law Institute of Victoria, 8; Experian, 11; Google, 6; New South Wales Council for Civil Liberties, 8; Optus, 7; Uniting Church of Australia, 3; Woolworths, 2; CSIRO, 6; Humanising Machine Intelligence Project, Australian National University, 2; Interactive Games and Entertainment Association, 12–13; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 7; Facebook, 32–3; Data Synergies, 39–40.

[439] Submissions to the Issues Paper: Communications Alliance, 7; Australian Industry Group, 16; Ramsay Healthcare, 6; CSIRO, 6; Interactive Games and Entertainment Association, 12; OAIC, 71.

[440] Submissions to the Issues Paper: Salinger Privacy, 19; OAIC, 72; Consumer Policy Research Centre, 12; New York Times, 2; Electronic Frontiers Australia, 8; Office of the Victorian Information Commissioner, 8–9; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 21; New South Wales Information and Privacy Commission, 3; Association for Data-Driven Marketing and Advertising, 16–17; New South Wales Council for Civil Liberties, 8; Professor Kimberlee Weatherall, 6; Privacy108, 11; Consumer Policy Research Centre, 8; CHOICE, 2; Humanising Machine Intelligence Project, Australian National University, 2; Queensland University of Technology Faculty of Law, 33; Data Synergies, 39–40.

[441] Submissions to the Issues Paper: OAIC, 71; Salinger Privacy, 19; New York Times, 2; Electronic Frontiers Australia, 8; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 21; Law Institute of Victoria, 9; CAIDE and MLS, 7; New South Wales Council for Civil Liberties, 8; Uniting Church of Australia, 3; Queensland Law Society, 5–6.

respect and called upon sparingly.'[442] The OAIC recommended preserving the use of consent for high privacy risk situations, rather than routine personal information handling, and noted that requiring consent for reasonably expected personal information handling may reduce consent to a tick-box exercise, which will detract from the value of consent in higher-risk situations.[443]

Many submitters considered that it would be more effective to protect privacy by requiring that APP entities collect, use and disclose personal information fairly or within the reasonable expectations of individuals, by adopting the GDPR's 'legitimate interests' basis, or by prohibiting or restricting certain practices (see Chapters 10 and 11). This would avoid unnecessary regulatory burden associated with APP entities processing a large number of consent requests, while relieving individuals from the burden of receiving, comprehending and acting on those consents.

Under such an approach, consent could continue to be reserved for the collection, use and disclosure of sensitive information, which poses the highest privacy risk for individuals, and where an APP entity wishes to use or disclosure personal information for a purpose other than for which it was originally collected. Submitters also considered that enhancing individuals' ability to exercise ongoing control over their personal information through opt-out rights would be preferable to increased reliance on consent at the point of collection, as privacy risks may change over time (see Chapter 14).[444]

Some submitters supported the DPI report recommendation that the Act should offer greater protections for inferred information, particularly where inferred information includes sensitive information, such as information about an individual's health, religious belief, or political affiliations.[445] As considered in Chapter 2, consent will be required under APP 3.3 where sensitive information is inferred or generated. Submitters were also particularly concerned about the collection and use of sensitive information in the context of targeted advertising and micro-targeting of political messaging to individuals based on information about their specific behaviour and traits, discussed further at Chapter 16.

Proposals

Strengthening what is required to demonstrate consent

The Issues Paper sought input on what approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed. A large number of submitters supported clarifying the definition of consent in the Act to establish criteria for valid consent.[446] Submitters considered that existing guidance from the IC could be enshrined in the Act,[447] or that consent be defined as a clear affirmative act that is freely given, specific, current, unambiguous and informed.[448] Submitters expressed concern that, in seeking consent, some entities

[442] Submission to the Issues Paper: New York Times, 2.
[443] Submissions to the Issues Paper: OAIC, 70. See also Law Council of Australia, 18.
[444] See, eg, Submission to the Issues Paper: Humanising Machine Intelligence Project, Australian National University, 3, which said that 'the issues paper focuses quite narrowly on the collection of data, with less attention on its analysis and use. The latter, however, is where effects on consumers occur.'
[445] See ACCC, DPI report (n 2) Recommendation 17(4).
[446] Submissions to the Issues Paper: Salinger Privacy, 18; Legal Aid Queensland, 9; Cyber Security Cooperative Research Centre, 9; Obesity Policy Coalition, 6–7; Electronic Frontiers Australia, 7; Privcore, 3; Deloitte, 19–21; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 22; Centre for Cyber Security Research and Innovation, 9; Public Interest Advocacy Centre, 7; Australian Information Security Association, 16; ElevenM, 2; Centre for Media Transition, University of Technology Sydney, 17; AusPayNet, 8–9; Privacy108, 10; GroundUp Consulting, 6; Consumer Policy Research Centre, 7; Financial Services Council, 15; Atlassian, 5; ANZ, 10; Dr Katharine Kemp, 19; OAIC, 77; Australian Privacy Foundation, 20.
[447] OAIC, APP Guidelines (n 21) [B.43]–[B.51].
[448] Submissions to the Issues Paper: Dr Katharine Kemp, 19; OAIC, 76–7; Salinger Privacy, 18; Legal Aid Queensland, 9; Cyber Security Cooperative Research Centre, 9; Obesity Policy Coalition, 6–7; Electronic Frontiers Australia, 7; Privcore, 3; Deloitte, 19–21; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 22; Centre for Cyber Security Research and Innovation, 9; Public Interest Advocacy Centre, 7; Australian

may deliberately conceal the full range of their data handling practices or employ manipulative user interface design choices or 'dark patterns', to undermine consumer autonomy.[449] The Interactive Games and Entertainment Association submitted that the Act should provide regulated entities with a degree of flexibility as to consent mechanisms used, as some entities in the gaming industry 'may ask players to swipe a notice with their finger, press a particular button on a controller, or perform some other interaction to show that they give consent'.[450]

An enhanced definition of consent could provide additional safeguards so that where consent is used, it is likely to be more effective and enables individuals to make more informed decisions.[451] Furthermore, the additional requirements could align Australian privacy law more closely with the concept of consent as defined in the GDPR, which requires consent to be a 'freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data'.[452]

The OP code will require consent to be voluntary, informed, unambiguous, specific and current.[453] However, a number of these elements could also be introduced into the definition of consent in the Act, which would apply to all APP entities:

1) ***Voluntary*** – An individual must have a genuine opportunity to provide or withhold consent.[454] Guidance from the European Data Protection Board in relation to the GDPR's equivalent requirement notes that freely given consent implies 'real choice and control' for individuals, and that if 'consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given'.[455] The OAIC submitted that Commissioner-issued guidance could supplement this requirement to note that, depending on the circumstances, consent is unlikely to be voluntary 'when the provision of service is conditional on consent to personal information handling that is not necessary for the provision of the service, as per Article 7(4) of the GDPR'.[456]
2) ***Informed*** – An individual must be provided with sufficient information in an understandable form so that the individual is aware of the implications of providing or withholding consent.[457] APP entities should ensure that they use clear and plain language when presenting consents to individuals.[458]
3) ***Current*** – The purpose for which the personal information is being collected, used or disclosed must be sufficiently linked to the consent that an individual provided. Where the purpose for the collection, use or disclosure of personal information changes, consent should be obtained afresh. This is to be distinguished from periodic renewal of consent to the collection, use or disclosure of sensitive information, even where there is no material change to the purposes for use or disclosure, as contemplated by the OP code.

Information Security Association, 17; ElevenM, 2; Centre for Media Transition, University of Technology Sydney, 17; Privacy108, 10; GroundUp Consulting, 6; Consumer Policy Research Centre, 7; Financial Services Council, 15; Atlassian, 5; ANZ, 10; Dr Katharine Kemp, 19; Australian Privacy Foundation, 20.

[449] Submissions to the Issues Paper: Consumer Policy Research Centre, 8; OAIC, 72; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 28. See also Norwegian Consumer Council, *Deceived by Design* (June 2018).

[450] Submission to the Issues Paper: Interactive Games and Entertainment Association, 13.

[451] Submission to the Issues Paper: Deloitte, 19.

[452] GDPR (n 26) art 4(11).

[453] Exposure Draft, OP Bill (n 1); Explanatory Paper, OP Bill (n 1). The OP code is also required to set out how consent will apply specifically in relation to children or other groups of people not capable of making their own privacy decisions, with stricter requirements for social media platforms in relation to children and consent – see further at chapter 13.

[454] OAIC, APP Guidelines (n 21) [B.43]–[B.46].

[455] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679* (4 May 2020) 7 ('Guidelines 05/2020').

[456] Submissions to the Issues Paper: OAIC, 77. See also Dr Katharine Kemp, 20.

[457] OAIC, APP Guidelines (n 21) [B.47].

[458] See European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679* (n 455) 16.

4) ***Specific*** – The consent must be sufficiently precise as to the purpose for which the individual is providing consent. The APP Guidelines provide that 'an APP entity should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses'. The level of specificity required may depend on circumstances including the sensitivity of the personal information,[459] whether the proposed collection, use or disclosure is for a purpose that is essential or non-essential for the provision of a service,[460] and whether the collection, use or disclosure would be reasonably expected by the individual.
5) ***Unambiguous indication through clear action*** – Consent must take place through an active expression of the individual's choice. For example, in the online context, consent should take place through an opt-in mechanism, rather than processes that use default or preselected settings or opt-outs.[461] Recital 32 of the GDPR provides interpretative guidance for the definition of consent, and notes that '[s]ilence, pre-ticked boxes or inactivity should not therefore constitute consent'.[462]

The requirements that consent be voluntary and specific are directed at guarding against overly broad or 'bundled' consents. [463] The APP Guidelines[464] and the OAIC's submission note that 'broad or "bundled" consents have the potential to undermine the voluntary nature of consent'.[465] Deloitte submitted that the bundling of consents for essential and non-essential activities (such as marketing, tracking and certain disclosures to third parties) can undermine consumer trust, and is inconsistent with the voluntary nature of consent.

The Issues Paper sought feedback on whether entities should be required to refresh or renew an individual's consent on a periodic basis. The OP code will require organisations subject to the code that collect, use or disclose sensitive information to renew consent periodically, in addition to obtaining fresh consent when circumstances change.[466] While a number of submitters expressed concern regarding the periodic renewal of consent due to risks of consent fatigue and the regulatory burden involved,[467] further feedback is sought on whether such a requirement may be suitable to apply more broadly than to just organisations subject to the OP code, if limited to consent obtained for the collection of sensitive information.

The Issues Paper also sought feedback on whether APP entities should be required to expressly provide individuals with the option of withdrawing consent. The APP Guidelines state that an individual may withdraw their consent and this should be an easy and accessible process.[468] Chapter 14 considers whether an individual's ability to withdraw consent should be formalised and recognised in the Act through an ability to object to certain collections, uses and disclosures 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.

[459] OAIC, APP Guidelines (n 21) [B.48]–[B.51].
[460] Submission to the Issues Paper: Deloitte, 20.
[461] Submission to the Issues Paper: Salinger Privacy, 18.
[462] GDPR (n 26) rec 32.
[463] See generally European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679* (n 455) 14.
[464] OAIC, APP Guidelines (n 21) [B.43]–[B.46].
[465] Submission to the Issues Paper: OAIC, 77.
[466] Exposure Draft, OP Bill (n 1); Explanatory Paper, OP Bill (n 1).
[467] See, eg, Submissions to the Issues Paper: Ramsay Healthcare, 7; Fundraising Institute Australia, 9; Financial Planning Association of Australia, 4; CSIRO, 7; SBS, 7; Facebook, 37.
[468] OAIC, APP Guidelines (n 21) [B.51].

Case study
An APP entity offers a medication-tracking mobile application that allows individuals to record medications they have been prescribed and set dosage reminders. The entity asks new users to consent to the collection of their sensitive information, by providing them with a pre-checked box that states 'I consent to the collection of my health information for the provision of the services'.

The entity uses individuals' health information for a range of purposes, such as to provide the application's functionality, charging users and maintaining the services (including to address technical bugs and provide customer support). The entity also discloses individuals' health information to 'trusted partners', including health insurers and data brokers for the purposes of direct marketing.

The entity's consent is unlikely to be valid under the proposed definition. In particular, the consent is not sufficiently specific as to the fact that sensitive information will be disclosed for the purpose of direct marketing. The pre-checked consent box is also unlikely to constitute an unambiguous indication of the individual's choice through clear action.

Standardisation of consent requests

The ACCC's DPI report also recommended the use of standardised icons or phrases in consent requests to facilitate consumers' comprehension and decision-making.[469]

Development of standardised consent taxonomies has commenced as part of the development of the Consumer Data Right standards,[470] and a similar process could take place for the OP code. The OP code must set out how an organisation subject to the code is to comply with the requirements to obtain consent for the collection, use and disclosure of personal information under APP 3 and 6. As discussed above in relation to the standardisation of privacy notices, due to the wide range of contexts in which the Act applies, it is likely to be impractical to develop consent templates, icons or phrases across all sectors. However, the OP code is a strong opportunity for reform on a sector-specific basis.

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?

[469] ACCC, DPI report (n 2) Recommendation 16(c). See also Submission to the Issues Paper: Data Republic, 21.
[470] Data61, *Consumer Data Standards* (n 405).

10. Additional protections for collection, use and disclosure

The Issues Paper sought feedback on whether reforms should be considered to further regulate uses and disclosures of personal information, while ensuring that entities' legitimate personal information handling is not unduly impacted. In recommending broader reform of the Act, the DPI report recommended that consideration should be given to 'whether the Act should set a higher standard of privacy protection, such as by requiring all use and disclosure of personal information to be by fair and lawful means'.[471]

Currently, the protections within the APPs rely predominantly on a regulatory theory of privacy self-management.[472] The APPs require APP entities to notify individuals of the specific purposes for which their information will be handled. Individuals may use this information to consider the costs and benefits of the collection, use or disclosure of their information, engage with APP entities in a particular way, or provide consent in certain circumstances.[473]

While notice and consent still have an important role to play in the Act, many submissions considered that these principles should be supplemented with additional protections to ensure the fair and reasonable collection, use and disclosure of personal information.[474] The ANU Humanising Machine Intelligence Project submitted that for notice and consent to be effective, 'they must be scaffolded by robust institutional assurances, so that consumers can trust that their digital safety does not depend on their unfailing vigilance and the vigilance of their fellow Australians'.[475] The Law Council of Australia recommended including additional matters in the APPs to balance the rights of individuals and the responsibilities of APP entities, including by requiring the 'reasonableness and fairness of an act or practice of an APP entity in their management of personal information.'[476]

The current requirements for collecting, using and disclosing personal information

Under APP 3, entities are permitted to collect personal information where it is reasonably necessary for one or more of the entity's functions or activities.[477] In the case of public sector agencies, the collection must be reasonably necessary for, or directly related to, one or more of the agency's function or activities.[478] To collect sensitive information, an APP entity must also obtain an individual's consent or an exception must apply for the collection to occur.[479] APP 3 further stipulates that an entity must collect personal information only by lawful and fair means.[480]

An organisation's functions or activities may include current or proposed functions or activities, as well as those that the organisation carries out in support of its other functions and activities, such as human resources, corporate administration, property management and public relations activities.[481]

---

[471] ACCC, DPI report (n 2) Recommendation 17, 478.
[472] Submissions to the Issues Paper: OAIC, 9; Law Council of Australia, 7; Data Synergies, 37; Queensland University of Technology Faculty of Law, 34. See also Daniel Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880.
[473] Submissions to the Issues Paper: OAIC, 70–72; Law Council of Australia, 19; Data Synergies, 37; DIGI, 7; Queensland University of Technology Faculty of Law, 34. See also Solove (n 472) 1880.
[474] Submissions to the Issues Paper: OAIC, 83–8; Law Council of Australia, 5–6, 18–19; Adobe, 5; Consumer Policy Research Centre, 12; Salinger Privacy, 22–26; Public Interest Advocacy Centre, 8; Association for Data-Driven Marketing and Advertising, 9, 16; Australian Information Security Association, 20–1; ElevenM, 2; CAIDE and MLS, 6–7, 10; New South Wales Council for Civil Liberties, 9; Professor Kimberlee Weatherall, 7; CHOICE, 1, 5–6; Queensland University of Technology Faculty of Law, 36; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 7; Australian Communications Consumer Action Network, 12; Australian Privacy Foundation, 19; Data Synergies, 4. See also ACCC, DPI report (n 2) Recommendation 17(3).
[475] Submission to the Issues Paper: Humanising Machine Intelligence Project, Australian National University, 2.
[476] Submissions to the Issues Paper: Law Council of Australia, 5.
[477] *Privacy Act* (n 2) sch 1 APP 3.1–3.2.
[478] *Privacy Act* (n 2) sch 1 APP 3.1.
[479] *Privacy Act* (n 2) sch 1 APP 3.3–3.4.
[480] *Privacy Act* (n 2) sch 1 APP 3.5.
[481] OAIC, APP Guidelines (n 21) [3.13].

Under APP 6, personal information must be used or disclosed within the parameters of the purpose for which that personal information was collected (primary purpose). Any subsequent or new purpose (secondary purpose) is only permitted with the consent or the individual, or where an exception applies.[482]

Limitations of the current approach

The DPI report and submissions to the Issues Paper expressed concern that the current framework affords APP entities a significant degree of discretion in determining what collections of personal information are 'reasonably necessary' for their functions and activities under APP 3, including practices that may not meet consumer expectations.[483] Furthermore, the DPI report considered that under APP 6, 'there is no requirement for the 'primary purpose' to be a purpose that consumers are aware of, or a purpose that is necessary or beneficial to consumers.'[484]

The DPI report observed that some APP entities may list many broadly-expressed purposes for the collection of personal information in their privacy policy,[485] which may subsequently be interpreted as evidence of their primary purpose under APP 6.[486] The DPI report and the OAIC's submission also noted that under the APPs, entities are only required to *collect* personal information by fair and lawful means, and that there is no equivalent requirement for the *use and disclosure* of personal information to also be fair and lawful.[487] The ACCC concluded that, taken together, APP 3 and APP 6 enable entities to collect, use and disclose personal information for a broad range of primary purposes, without consent or without such personal information handling falling within consumers' reasonable expectations.[488]

The current framework places a large onus on the individual to 'read, assimilate and evaluate' privacy information [489] in privacy notices and policies, and then self-manage their privacy by choosing whether or not to engage with the entity, or to engage with the entity in a particular way (where this is possible). However, there is considerable evidence that individuals are overwhelmed by the amount of privacy information presented to them and that only a small percentage of individuals actually read the privacy policies of entities they engage with.[490] Submitters also noted

---

[482] *Privacy Act* (n 2) sch 1 APP 6.1–6.2.

[483] ACCC, DPI report (n 2) 438. See relatedly, Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 25–6; Humanising Machine Intelligence Project, Australian National University, 2; ANZ, 9; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 6; Dr Katharine Kemp, 17.

[484] ACCC, DPI report (n 2) 464. See relatedly, Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 25-26; Professor Kimberlee Weatherall, 7; CHOICE, 2.

[485] ACCC, DPI report (n 2) 438. See relatedly, Submissions to the Issues Paper: Oracle, 5; CHOICE, 2; Dr Katharine Kemp, 12; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 6.

[486] See, eg, *Flight Centre Travel Group (Privacy)* [2020] AICmr 57 (25 November 2020) [40] ('*Flight Centre Travel Group*'); *'DK' and Telstra Corporation Limited* [2014] AICmr 118 (30 October 2014) [44].

[487] ACCC, DPI report (n 2) 478. Submission to the Issues Paper: OAIC, 84.

[488] ACCC, DPI report (n 2) 438. See relatedly, Submissions to the Issues Paper: Professor Kimberlee Weatherall, 7.

[489] Submissions to the Issues Paper: Law Council of Australia, 19; OAIC, 72; Consumer Policy Research Centre, 11; Salinger Privacy, 21–22; Electronic Frontiers Australia, 8; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 16; Association for Data-Driven Marketing and Advertising, 15; Professor Kimberlee Weatherall, 6; CHOICE, 3, 6; DIGI, 7; Queensland University of Technology Faculty of Law, 33.

[490] OAIC, *2020 ACAP Survey* (n 51), 69–72. The 2020 ACAP survey revealed that only 31 per cent of participants normally read privacy policies, and just 20 per cent both read them and were confident they understood them. See also Aleecia McDonald and Lorrie Cranor, 'The Cost of Reading Privacy Policies' (2008) 4(3) *A Journal of Law and Policy for the Information Society* 543, 562–5. See also Submissions to the Issues Paper: Consumer Policy Research Centre, 12; CAIDE and MLS, 6; Oracle, 4; CHOICE, 2; DIGI, 10; Queensland Law Society, 4; Queensland University of Technology Faculty of Law, 33; Adobe, 4; Australian Communications Consumer Action Network, 11; Australian Privacy Foundation, 20.

that choosing not to engage with an entity may come at the cost of being excluded from accessing essential digital services.[491]

As the internet plays an increasingly central role in society, it becomes less likely that individuals will consider and digest all the privacy information they are presented with on a day-to-day basis – in short, 'there are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity'.[492] It was submitted that a notice and consent regulatory model should not be exclusively relied upon to ensure that consumers are protected.[493] The OAIC noted that '[t]he burden of understanding and consenting to complicated practices should not fall on individuals but must be supported by enhanced obligations for APP entities that promote fair and reasonable personal information handling and organisational accountability'.[494]

The current framework also places an emphasis on the exercise of individual control at the point of collection, which is often at the point at which an individual first engages with an APP entity. However, privacy risks typically emerge over time and it may be challenging for individuals to assess future unknown risks and conduct a cost-benefit assessment at that point in time.[495] The Centre for AI and Digital Ethics and Melbourne Law School considered that this limitation arises from the inevitable bounded rationality of individual decision making and assessments of future risks and harms, particularly those that are not monetised or concrete, as with privacy harms.[496]

CHOICE argued that rather than requiring an individual to understand how a product or service may be harmful for them, it is preferable to prevent the harm itself.[497] Submitters highlighted various acts and practices for which the Act should enable more robust review, including marketing to children or other vulnerable populations, certain applications of facial recognition technology and the automated processing of personal information from which other personal information, including sensitive information, is inferred.[498]

Proposal

Collection, use and disclosure of personal information must be fair and reasonable

Submitters considered that additional protections are needed to set minimum acceptable standards for how personal information is collected, used and disclosed, but had differing views on how this

[491] Submissions to the Issues Paper: Association for Data-Driven Marketing and Advertising, 16; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 21; New South Wales Council for Civil Liberties, 8; Queensland Law Society, 5; Dr Katharine Kemp, 2; Adobe, 4.
[492] Solove (n 472) 1881. See also Submissions to the Issues Paper: Consumer Policy Research Centre, 11; Electronic Frontiers Australia, 8; Queensland University of Technology Faculty of Law, 33; Adobe, 4.
[493] Submissions to the Issues Paper: Law Council of Australia, 7; Consumer Policy Research Centre, 12; Salinger Privacy, 21–2; Snap Inc, 3; Electronic Frontiers Australia, 8; Communications Alliance, 7; Office of the Victorian Information Commissioner, 9; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 16; New South Wales Information and Privacy Commission, 3; ElevenM, 1; Centre for Media Transition, University of Technology Sydney, 14; New South Wales Council for Civil Liberties, 8; Professor Kimberlee Weatherall, 7; Privacy108, 7; Humanising Machine Intelligence Project, Australian National University, 2; CHOICE, 1–3; DIGI, 7; Queensland Law Society, 5; Queensland University of Technology Faculty of Law, 33; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 7; Adobe, 4; Australian Privacy Foundation, 17; Data Synergies, 4. See also ASIC, *Disclosure: Why it shouldn't be the default* (Report, October 2019).
[494] Submission to the Issues Paper: OAIC, 72.
[495] Submissions to the Issues Paper: Consumer Policy Research Centre, 12; Salinger Privacy, 19; Electronic Frontiers Australia, 8; Office of the Victorian Information Commissioner, 8; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 21; Dr Katharine Kemp, 4. See relatedly Submission to the Issues Paper: Humanising Machine Intelligence Project, Australian National University, 3.
[496] Submission to the Issues Paper: CAIDE and MLS, 6. See also Submissions to the Issues Paper: Consumer Policy Research Centre, 12; Queensland University of Technology Faculty of Law, 34.
[497] Submissions to the Issues Paper: CHOICE, 2. See also Submissions to the Issues Paper: Consumer Policy Research Centre, 12; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 16; Electronic Frontiers Australia, 6, 8; New South Wales Council for Civil Liberties, 9; Professor Kimberlee Weatherall, 7.
[498] See, eg, Submissions to the Issues Paper: Salinger Privacy, 23; OAIC, 82.

could be achieved. Of those submissions who considered that consent should not be the primary basis for authorising the collection, use and disclosure of personal information, two alternatives were commonly raised:

1. A lawful basis for collection, use and disclosure modelled on the 'legitimate interest' test under Article 6(1)(f) GDPR,[499] or
2. A general requirement that entities do not undertake acts or practices in relation to an individual's personal information that would be unfair, cause harm, or be outside the reasonable expectations of an ordinary individual.[500]

As noted above, many industry stakeholders raised the GDPR's legitimate interest basis for processing personal data as a desirable basis for the handling of personal information in Australia. Article 6 of the GDPR provides six lawful bases for processing data, including where 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject'. When seeking to rely on the 'legitimate interests' basis for processing under the GDPR, an entity must balance its legitimate interest for which processing is necessary against the individual's interests, rights and freedoms.[501]

The Article 29 Working Party has noted that the basis may be incorrectly seen as an 'open door' to legitimise any personal data processing which does not fit into the other legal grounds of European data protection law, and that in certain circumstances, the test will operate to weigh in favour of the interests and fundamental rights of the data subjects to render a processing activity unlawful.[502] The legitimate interests of the entity may be interpreted broadly to include the interests of third parties or the public interest.[503] However the 'impact' to an individual's interests, rights and freedoms may be interpreted broadly in a commensurate manner.[504]

As the Act does not confer a right to privacy on individuals, but rather protects against arbitrary interferences with privacy as derived from Article 17 of the ICCPR, it may present difficulties to import a rights-based requirement.[505] The ACCC has claimed that 'there is considerable uncertainty and concern surrounding the relatively broad and flexible definition of the 'legitimate interests' basis for processing personal information under the GDPR.'[506]

Other submitters agreed with the DPI report's recommendation that a requirement for fair and lawful collections of personal information be extended to APP 6, [507] or considered that entities

---

[499] Submissions to the Issues Paper: Microsoft Australia, 3; Snap Inc., 3; Communications Alliance, 3; BSA|The Software Alliance, 6; Australian Industry Group, 17; Experian, 14, 19; Google, 7; DIGI, 7; Australian Financial Markets Association, 4; Australian Finance Industry Association, 7; Facebook, 32. See also GDPR (n 26) art 6(1)(f); UK ICO, *Legitimate Interests* (January 2021).

[500] Submissions to the Issues Paper: Law Council of Australia, 5, 18–19; OAIC, 83–8; Adobe, 5; Consumer Policy Research Centre, 12; Salinger Privacy, 22–6; Public Interest Advocacy Centre, 8; Association for Data-Driven Marketing and Advertising, 9, 16; Australian Information Security Association, 20–1; ElevenM, 2; CAIDE and MLS, 6–7, 10; New South Wales Council for Civil Liberties, 9; Professor Kimberlee Weatherall, 7; CHOICE, 1, 5–6; Queensland University of Technology Faculty of Law, 36; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 7; Australian Communications Consumer Action Network, 12; Australian Privacy Foundation, 19; Data Synergies, 4; Experian, 19; Uniting Church of Australia, 3. See also ACCC, DPI report (n 2) Recommendation 17(3).

[501] Article 29 Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (9 April 2014) 4 ('Opinion 06/2014'); UK ICO, *Legitimate Interests* (n 499).

[502] Article 29 Working Party, *Opinion 06/2014* (n 501) 5, 9–10.

[503] CJEU, Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'* (4 May 2017) [29]; Article 29 Working Party, *Opinion 06/2014* (n 501) 35.

[504] Article 29 Working Party, *Opinion 06/2014* (n 501) 37, 49.

[505] Radha M Pull ter Gunne, 'The Illusion of Control' (2020) 48(5) *Australian Business Law Review* 424.

[506] ACCC, DPI report (n 2) 466.

[507] Ibid Recommendation 17.

should only be permitted to collect, use or disclose personal information in a fair manner, within individuals' reasonable expectations, or in a manner that does not cause harm.[508] For example, the Centre for AI and Digital Ethics and Melbourne Law School recommended that additional rules should govern the collection, use and disclosure of personal information, 'including limits on practices that are not fair or inconsistent with individuals' reasonable expectations.'[509]

The Act could be amended so that APP entities' collection, use and disclosure of personal information must be fair and reasonable. The proposed test could apply to the existing APPs that regulate collection, use and disclosure, and include a number of legislated factors to assist entities in determining whether a particular collection, use or disclosure falls within acceptable parameters. Consideration of the factors would be contextual and depend on the circumstances.

A requirement on entities to act *fairly* exists currently within APP 3.5, which requires that APP entities collect personal information only by 'lawful and fair means'.[510] The APP Guidelines state that a 'fair means' of collection depends on the circumstances, and that it would usually be 'unfair to collect personal information covertly without the knowledge of the individual'.[511]

Professor Lee Bygrave has argued that the notion of fairness in data protection law requires entities to 'take account of the interests and reasonable expectations of data subjects', and handle personal information in a manner that 'does not, in the circumstances, intrude unreasonably upon the data subjects' privacy nor interfere unreasonably with their autonomy and integrity.'[512]

Guidance issued by the UK ICO notes that the GDPR's fairness principle[513] requires entities to 'handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.'[514] Similar fairness-based protections can be found in other Commonwealth legislation, for example, the unfair terms regime in the ACL.[515]

There are also existing principles within the Act that require an act or practice to fall within the *reasonable expectations* of the individual. This requirement is one exception that permits entities to use or disclose personal information for a secondary purpose, as well as to undertake direct marketing in certain circumstances.[516] Similar requirements appear in a number of international data protection laws, as illustrated on the following page.

---

[508] Submissions to the Issues Paper: Law Council of Australia, 5, 18–19; OAIC, 83–8; Consumer Policy Research Centre, 12; Salinger Privacy, 22–6; Public Interest Advocacy Centre, 8; Association for Data-Driven Marketing and Advertising, 9, 16; Australian Information Security Association, 20–21; ElevenM, 2; CAIDE and MLS, 6–7, 10; New South Wales Council for Civil Liberties, 9; Professor Kimberlee Weatherall, 7; CHOICE, 1, 5–6; Queensland University of Technology Faculty of Law, 36; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 7; Adobe, 5; Australian Communications Consumer Action Network, 12; Australian Privacy Foundation, 19; Data Synergies, 4. See also ACCC, DPI report (n 2) Recommendation 17(3).

[509] Submission to the Issues Paper: CAIDE and MLS, 6.

[510] *Privacy Act* (n 2) sch 1 APP 3.5.

[511] OAIC, APP Guidelines (n 21) [3.62].

[512] Lee Bygrave, 'Core Principles of Data Protection Law' (2001) 7(9) *Privacy Law and Policy Reporter* 169. See also Lee Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer, 2002) ch 5 ('*Data Protection Law*').

[513] GDPR (n 26) art 6(1).

[514] UK ICO, *Lawfulness, Fairness and Transparency* (January 2021).

[515] *CCA* (n 67) sch 2 ss 20–28.

[516] *Privacy Act* (n 2) sch 1 APP 6.2(a), 7.2(b).

Figure 10.1: Equivalent baseline protections in selected overseas data protection legislation

Jurisdiction	Law	Provision
Europe	General Data Protection Regulation	Article 5(1) – 'Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.'
United Kingdom	UK General Data Protection Regulation	Article 5(1) – 'Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.'
Canada	Personal Information Protection and Electronic Documents Act 2000 ('PIPEDA')	Section 5(3) – 'An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.'
Singapore	Personal Data Protection Act 2012	Section 18 – 'An organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances'
India	Personal Data Protection Bill 2019 (Bill no. 373 of 2019)	Clause 5 – 'Every person processing personal data of a data principal shall process such personal data— (a) in a fair and reasonable manner and ensure the privacy of the data principal…'

Entities that currently collect, use and disclose personal information in a way which meet the reasonable expectations of the individual and the community at large would likely satisfy this test. The new requirement would therefore only impose regulatory burden on those entities that handle personal information in a manner that is inconsistent with community expectations.

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

Factors relevant to the fair and reasonable requirement

The Act could set out factors to assist entities in assessing their collections, uses and disclosures of personal information. These factors could be supplemented with Commissioner-issued guidance and would be clarified through OAIC determinations and case law. Effective enforcement would therefore be crucial to further map the contours of a fair and reasonable requirement over time.[517]

The Review notes that similar guidance has been issued by the Office of the Privacy Commissioner of Canada (OPC Canada) for interpreting the 'appropriate purpose' test in section 5(3) of PIPEDA,[518] informed by past court decisions.[519]

[517] See Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 1 *Yearbook of European Law* 130, 183.
[518] *PIPEDA* (n 28) s 5(3).
[519] OPC Canada, *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)* (May 2018) ('*Guidance on inappropriate data practices*').

Furthermore, judicial consideration of the appropriate purpose test in Canada has set out factors for evaluating compliance with Section 5(3) PIPEDA, which include:

- the sensitivity of the personal information in question
- whether the organisation's purpose represents a legitimate business need
- whether the collection, use or disclosure effectively meets that need
- whether there are less invasive means of achieving the same ends, and
- whether the loss of privacy is proportional to the benefits.[520]

Canada's Bill C-11 proposed to codify these factors in legislation however the Bill died on the Order Paper in advance of the Canadian federal election in September 2021.[521]

1) Reasonable expectations

The first factor could be *whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances*.

The proposed factor would apply to collections under APP 3, as well as uses and disclosures for primary and secondary purposes under APP 6. What a reasonable individual would expect would be an objective test and would also consider individuals' collective interests in privacy.[522] The APP Guidelines note that 'the 'reasonably expects' test is an objective one that has regard to what a reasonable person, who is properly informed, would expect in the circumstances' and is 'a question of fact in each individual case'.[523]

It is likely that certain kinds of information would attract higher expectations from an objective reasonable individual, for example, sensitive information or IoT smart home data, the handling of which may require a higher standard of privacy protection. The test may also be interpreted to require a higher standard of privacy protection for vulnerable cohorts such as children. The Allens Hub and Australian Society for Computers and Law submitted that including in a privacy policy the 'ways in which personal information can be used should not be enough for the entity to be able to demonstrate individuals could have reasonably expected it.'[524]

2) The sensitivity and amount of personal information

The second factor could require consideration of *the sensitivity and amount of personal information being collected, used or disclosed*.

This factor would recognise that certain types of information, including sensitive information or information relating to an individual's vulnerabilities should be treated with a higher degree of care in order to ensure that the collection, use or disclosure is fair and reasonable.

This factor would also take into account the amount of personal information collected, used and disclosed, which could support the principle of personal information minimisation.[525] Privcore submitted that 'privacy risks, such as inappropriate use or disclosure, poor security, access and correction obligations can be reduced or avoided when a data minimisation approach is adopted.'[526]

---

[520] *Turner v Telus Communications Inc* [2005] FC 1601, [48].
[521] Bill C-11 (n 394).
[522] See Submissions to the Issues Paper: Centre for Media Transition, University of Technology Sydney, 4; Humanising Machine Intelligence Project, Australian National University, 2; Professor Kimberlee Weatherall, 6.
[523] OAIC, APP Guidelines (n 21) [6.20]. See also *Flight Centre Travel Group* (n 486) [58]–[65].
[524] Submission to the Issues Paper: The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 7.
[525] See Submissions to the Issues Paper: Consumer Policy Research Centre, 12; Dr Kate Mathews Hunt, 9; Professor Kimberlee Weatherall, 7; Humanising Machine Intelligence Project, Australian National University, 3.
[526] Submission to the Issues Paper: Privcore, 3.

3) Risk of adverse impact or harm

The third factor could require identification of *whether an individual is at a foreseeable risk of unjustified adverse impact or harm as a result of the collection, use or disclosure of their personal information*.

This element would bring the concept of privacy harms within the Act and would require consideration of potential adverse consequences to an individual or society arising from the processing of personal information. These might include:

- direct or indirect financial loss
- physical or psychological harm
- negative outcomes with respect to an individual's eligibility for rights, benefits or privileges in employment, credit and insurance, housing, education, professional certification or provision of health care and related services
- reputational harm, significant inconvenience or expenditure of time, and
- unwanted commercial communication.[527]

Overseas data protection regulators in Singapore[528] and the UK[529] have acknowledged that personal data handling that exposes individuals to harm or adverse impacts may contravene their appropriate purpose or fairness requirements, respectively.

4) Reasonably necessary to achieve functions and activities

The fourth factor could be *whether the collection, use or disclosure of personal information is reasonably necessary to achieve the functions and activities of the entity*.

The OAIC submitted that one factor to guide the interpretation of the fair and reasonable test could include whether an entity's purposes for personal information handling are reasonable and necessary.[530] The proposed wording aligns with the existing requirement in APP 3, which enables entities to collect personal information where it is reasonably necessary for one or more of the entity's functions or activities.[531] This may include current or proposed functions or activities.[532] Whether a collection, use or disclosure is 'reasonably necessary' for the organisation's functions and activities is an objective test, assessed from the perspective of a reasonable person who is properly informed.[533]

An alternative approach could be to require that a collection, use or disclosure be reasonably necessary to achieve the *legitimate interests* of the entity. Industry-based stakeholders commonly raised the GDPR's legitimate interest basis for processing personal data as a desirable basis for handling personal information in Australia.[534] However, if applied in Australia, a legitimate interests requirement would operate differently as one factor to be considered within a broader test.

---

[527] Data Synergies, *Privacy Harms: A paper for the Office of the Australian Information Commissioner* (June 2020) 43.
[528] Submission to the Issues Paper: OAIC, 86. See also UK ICO, *Lawfulness, Fairness and Transparency* (January 2021).
[529] Submission to the Issues Paper: OAIC, 86. See also Personal Data Protection Commission (SG), *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (February 2021).
[530] Submission to the Issues Paper: OAIC, 86. The OAIC submitted that the factor should consider whether the purpose in question was 'reasonable, necessary and proportionate', however, proportionality has been considered under the subsequent factor.
[531] *Privacy Act* (n 2) sch 1 APP 3.1–3.2.
[532] OAIC, APP Guidelines (n 21) [3.23].
[533] OAIC, APP Guidelines (n 21) [3.28].
[534] See, eg Submissions to the Issues Paper: Microsoft Australia, 3; Snap Inc., 3.

The term 'legitimate interests' has also been used in the context of the unconscionable conduct regime in the ACL,[535] and has been interpreted to involve an assessment of alternative available options to the entity and proportionality.[536]

5) Proportionality

The fifth factor could assess *whether the individual's loss of privacy is proportionate to the benefits of the collection, use or disclosure of their personal information*. As part of this, entities would consider:

a) whether the collection, use or disclosure intrudes to an unreasonable extent upon the personal affairs of the affected individual[537]
b) whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and[538]
c) any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.

The concept of proportionality is one which is used by Australian courts but is less commonly found in the express wording of Australian legislation.[539] While proportionality 'first entered the lexicon of Australian constitutional law as a test for characterising a statute as one falling within a constitutional head of power'[540] the concept has been employed by the courts when considering 'reasonably necessary' collections of personal information and contractual terms. In *Jurecek v Director, Transport Safety Victoria* Bell J applied the collection limitation principle in the *Information Privacy Act 2000* (Vic), noting that an evaluation of whether a collection of personal information is 'reasonably necessary' should include 'balancing, in a reasonably proportionate way, the nature and importance of any legitimate purpose and the extent of the interference.' This was said to be the case as the *Information Privacy Act 2000* (Vic) was intended 'to give effect in a particular context to the right to privacy stipulated in art 17 of the ICCPR' and because 'reasonable proportionality is a central component of that right.' [541] The *Jurecek* decision has since been cited with approval by the federal Privacy Commissioner in interpreting APP3 of the *Privacy Act*.[542] In assessing whether a respondent had engaged in unconscionable conduct under the ACL, Banks-Smith J noted that what is 'reasonably necessary' might also involve an analysis of the proportionality of the term against the potential loss that could be suffered.[543]

The OAIC interprets the 'lawful and fair' component of APP 3.5 as requiring a collection that is 'not unreasonably intrusive.'[544] The proposal formalises this requirement as an individual should be able to engage with services and products that do not unreasonably intrude on their personal affairs. In designing personal information handling practices, entities should be considering whether their approach is the least intrusive way to achieve the purpose for which the personal information is being handled.

---

[535] *CCA* (n 67) s 22(1)(b).
[536] *Australian Competition and Consumer Commission v Ashley & Martin Pty Ltd* [2019] FCA 1436, [59] ('*ACCC v Ashley & Martin*').
[537] Submissions to the Issues Paper: Salinger Privacy, 23; OAIC, 87.
[538] *Turner v Telus Communications Inc* (n 520) [48]; Bill C-11 (n 391); European Data Protection Supervisor, *Assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (December 2019).
[539] This may be compared to its use in EU law which has been influential in its adoption in the UK where proportionality tests feature in the UK *Data Protection Act 2018* (n 37) and other legislation such as the *Equality Act 2010*.
[540] The Hon TF Bathurst AC and Bronte Lambourne, 'On to Strasbourg or Back to Temple? The Future of European Law in Australia Post-Brexit' (2018) 92 *Australian Law Journal* 679.
[541] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285, [69]-[70] (Bell J).
[542] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021)* [2021] AICmr 50 (29 September 2021).
[543] *ACCC v Ashley & Martin* (n 533) [352].
[544] OAIC, APP Guidelines (n 21) [3.62].

6) Transparency

The sixth factor could consider *the transparency of the collection, use or disclosure of the personal information.* Professor Lee Bygrave contends that the concept of fairness in data protection law implies that personal information handling be 'evident to the data subject' and that fairness militates against surreptitious collection and deception of the data subject as to the nature and purposes of personal information handling.[545]

This factor is similar to Article 5(1) of GDPR, which expressly requires entities to process personal data in a transparent manner. Guidance issued from the UK ICO notes that transparency 'is about being clear, open and honest with people from the start about who you are, and how and why you use their personal data'.[546]

7) Best interests of the child

A final factor could recognise the special treatment which should attach to the personal information of children. If personal information relates to a child, an entity would need to consider '*whether the collection, use or disclosure of the personal information is in the best interests of the child.*' This factor is explored further in Chapter 13.

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.

Case study

An APP entity offers a weather application that collects users' precise geolocation data. Upon using the application for the first time, users are asked to consent 'to the use of your personal information in accordance with our privacy policy.'

The privacy policy of the weather application states that the entity collects personal information 'such as your name, email address, device identifiers and location information'. The privacy policy further states that personal information is used and disclosed for 'primary purposes, including to provide our services to you, provide location-specific weather updates and to share information with our partners and affiliates'. The listed purposes for using and disclosing location data in the privacy policy may form evidence of the weather application's primary purposes under APP 6.1.

The weather application sells users' precise geolocation data to third party data brokers. Under the existing APPs, the collection of the location data is likely to be reasonably necessary for the entity's functions and activities under APP 3.

[545] Bygrave, 'Core Principles of Data Protection Law' (n 512). See also Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (n 512) ch 5.
[546] UK ICO, *Lawfulness, Fairness and Transparency* (January 2021).

Proposals 10.1 and 10.2 would permit a more thorough analysis of the weather application's data handling practices. In relation to the *collection* of location data, considerations could include whether it would be more proportionate to collect location data that is less granular (and not capable of identifying an individual's address) but is still capable of identifying their city or region for the purposes of delivering location-specific weather updates.

In relation to the *disclosure* of precise geolocation data, consideration could be given to whether an individual would reasonably expect a weather application to sell their precise geolocation data to data brokers, who may subsequently on-sell that information to other unknown parties in Australia or internationally. The disclosure may not be reasonably expected due to the unique identifying nature of precise geolocation data, and capacity to identify an individual's home and work address through analysing an individual's movement patterns. The disclosure of this information to data brokers or onward disclosure to other unknown parties may subject individuals to risks of unjustified adverse impacts or harm. In sum, the sale of precise geolocation data by the weather application to data brokers is unlikely to be fair and reasonable in the circumstances.

Case study
A digital platform offers social media services. The digital platform collects personal information about individuals that use its services, including inferred interests, demographics, location and behaviours. This data is used to serve individuals with relevant content in order to maximise user engagement with the platform. The digital platform does not sell or disclose users' personal information, but permits advertisers to market to platform users based on specific traits.

The digital platform also actively infers users' moods and socio-economic status. The digital platform has received complaints that vulnerable individuals are receiving highly targeted content or advertisements relating to mental health, gambling and predatory loan services.

The profiling of user moods and socio-economic status is unlikely to be fair and reasonable in these circumstances. An individual is unlikely to reasonably expect that a social media platform would infer these particularly sensitive traits without their knowledge. Profiling based on such traits is unlikely to be a proportionate use of individuals' personal information, particularly whereby advertising revenue and engagement could be driven by non-sensitive traits that pose less of a risk of adverse impact or harm to the individual.

By contrast, if an entity offered specialised mental health therapy or financial coaching applications based on profiling of users' activity carried out transparently, and in the individuals' best interests, it could be more likely to meet the proposed fair and reasonable test.

Integration with existing APP 3 and APP 6 requirements

The Review is seeking feedback on what adjustments should be made to the existing requirements in APP 3 and APP 6 to accommodate an overarching requirement that collections, uses and disclosures be fair and reasonable in the circumstances.

In relation to APP 3, the Review is considering whether the proposed fair and reasonable test would replace the existing requirements in APP 3.1 and 3.2, as the test would require consideration of whether a collection of personal information is 'reasonably necessary to achieve the functions and activities of the entity.' The Review is also considering how the proposed overarching test interacts with the existing requirement in APP 3.5 that collections of personal information be by 'lawful and fair means'.[547] The APP Guidelines state that a 'fair means' of collection 'is one that does not involve

[547] *Privacy Act* (n 2) sch 1 APP 3.5.

intimidation or deception, and is not unreasonably intrusive'.[548] The proposed fair and reasonable test is not limited to the *means* of collection, but rather applies to both the *purpose* and *means* of collection. The existing requirement in APP 3.5 could therefore be subsumed into the overarching fair and reasonable test.

An alternative could be to limit the application of the fair and reasonable test to APP 6, to the effect that it only applies to uses and disclosures of personal information. This would be more closely aligned with the DPI report recommendation to 'require all uses and disclosures of personal information to be by fair and lawful means'.[549] However this would preclude an assessment of whether an entity's collection of personal information is fair and reasonable, meaning that, for example, the quantity of personal information collected by an entity would not be subject to scrutiny as to whether it was fair and reasonable.

The Review is also seeking feedback on how the fair and reasonable test would interact with the consent mechanisms in APPs 3.3 and 6.1(a). The OAIC submitted that the fair and reasonable test should 'qualify other requirements in the APPs, including whether an individual has consented to the act or practice'.[550] Such an approach would mirror the operation of the overarching fairness principle in GDPR.[551] In this regard, the European Data Protection Board notes that '[e]ven if the processing of personal data is based on consent of the data subject, this would not legitimise collection of data, which is not necessary in relation to a specified purpose of processing and be fundamentally unfair'.[552]

The Review is also considering how the proposal would be integrated with the existing requirements of APP 6. In particular, it is being considered if the assessment of whether 'the individual would reasonably expect the entity to use or disclose the information for the secondary purpose' should apply alongside the fair and reasonable test or be subsumed within it.

Finally, the Review is considering whether the secondary purpose exceptions in APP 6.2(b)-(e), as well as the sensitive information exceptions in APP 3.4, should be subject to the overarching fair and reasonable test. On balance, it is considered that such exceptions should *not* be made subject to the fair and reasonable test as 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.[553]

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?

[548] OAIC, APP Guidelines (n 21) [3.62].
[549] ACCC, DPI report (n 2) Recommendation 17.
[550] Submission to the Issues Paper: OAIC, 86.
[551] GDPR (n 26) art 5(1).
[552] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679* (n 455) 5.
[553] See, eg *Privacy Act* (n 2) ss 16A(1); sch 1, APP 3.4 (a), (d), 6.2(b),(e).

- 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)?

Additional requirements in APPs 3 and 6

Submitters to the Issues Paper also discussed possible additional amendments to APP 3 and APP 6 beyond the proposals canvassed in the previous section relating to notice, consent and collections, uses and disclosures.

Proposal – requirement on third party collections

As noted in Chapter 8, submitters were concerned about the prevalence of third party use and disclosure of personal information without the awareness of the individual. The OAIC's submission also highlighted instances of personal information being collected by third parties where it was apparent that it was originally collected by unfair or unlawful means, including where it was reasonably apparent that the information was published by the perpetrator of a data breach.[554]

The OAIC recommended that in addition to the existing requirement in APP 3.6 that organisations must collect personal information directly from an individual unless it is unreasonable or impracticable to do so, [555] an APP entity should also be required to 'take reasonable steps to satisfy itself that personal information that was not collected directly from an individual was originally collected in accordance with APP 3'.[556] 'As the rate and utility of data collection, transfer and use increases amongst organisations,'[557] such a requirement would seek to reduce the prevalence of use and disclosure of personal information obtained by unfair or unlawful means.

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.

Proposal – define primary and secondary purposes

Submitters also considered whether the concepts of primary and secondary purposes under APP 6 should be defined or further clarified.[558] The APP Guidelines provide that a primary purpose is the purpose for which an APP entity collects personal information and that:

> *How broadly a purpose can be described will depend on the circumstances and should be determined on a case-by-case basis. In cases of ambiguity, and with a view to protecting individual privacy, the primary purpose for collection, use or disclosure should be construed narrowly rather than expansively*.[559]

[554] Submission to the Issues Paper: OAIC, 44.
[555] *Privacy Act* (n 2) sch 1 APP 3.6.
[556] Submission to the Issues Paper: OAIC, 44.
[557] Submission to the Issues Paper: Deloitte, 13.
[558] Submissions to the Issues Paper: Salinger Privacy, 27–8; Australian Department of Health, 5; Facebook, 35; Australian Privacy Foundation, 22.
[559] OAIC, APP Guidelines (n 21) [B.101].

The APP Guidelines also clarify that a 'related' secondary purpose 'is one which is connected to or associated with the primary purpose' which must be 'more than a tenuous link'.[560] This has been interpreted to mean that the 'relationship between the purposes need only be one of association or connection'.[561] A 'directly related' secondary purpose is one that is 'closely associated with the primary purpose, even if it is not strictly necessary to achieve that primary purpose'.[562]

Salinger Privacy submitted that a primary purpose should be defined as the 'purpose of the original collection as notified to the individual' to ensure that the primary purpose is transparent, and cited California's CCPA as an example of data protection law that explicitly ties collection and use to transparency:

> *A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.*[563]

It was further contended that secondary uses and disclosures under APP 6 should be required to meet a threshold of being 'directly related to, and reasonably necessary to support, the primary purpose.'[564] This was based on the concern that the term 'related to' afford entities with a significant degree of discretion to determine that uses and disclosures which have only an indirect connection to the original purpose are authorised under APP 6. [565]

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. Secondary purposes that are 'directly related to' a primary purpose are more likely to be time-limited than secondary purposes which are merely 'related to' the primary purpose. This could have a downstream effect of strengthening the destruction requirements in APP 11.2.

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?

[560] Ibid [6.24].
[561] *'PB' and United Super Pty Ltd as Trustee for CBUS (Privacy*) [2018] AICmr 51, [64].
[562] OAIC, APP Guidelines (n 21) [6.26].
[563] *CCPA* (n 27) § 1798.100(b).
[564] Submission to the Issues Paper: Salinger Privacy, 27–8.
[565] Submission to the Issues Paper: Salinger Privacy, 28. See also Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 26; Australian Privacy Foundation, 22.

11. Restricted and prohibited practices

Different types of personal information handling present different risks to individuals. Some submitters proposed that certain collections, uses and disclosures of personal information are of a nature that need to either be more tightly regulated, or prohibited entirely. It was considered that such acts and practices may either pose a higher privacy risk to individuals, or may not meet the expectations of the Australian community.[566]

The Issues Paper noted overseas data protection frameworks that have considered the designation of prohibited acts and practices ('no-go zones'),[567] and considered whether there was a greater role for 'proceed with caution zones', or enhanced protections for certain categories of information, or acts or practices that pose a high risk to privacy.

A number of submitters supported the introduction of restricted practices, or 'proceed with caution zones' into the Act,[568] and some also considered that there is a role for prohibited acts and practices.[569]

Proposals

Restricted practices (proceed with caution zones)

Submitters proposed different mechanisms for restricting, but not prohibiting, certain high risk acts and practices. Some submitters were of the view that entities that engage in high risk acts and practices should be subject to additional organisational accountability obligations.[570] Others considered that individuals should be provided with additional opportunities to self-manage their privacy in relation to high risk personal information handling.[571]

The OAIC submitted that APP entities that engage in 'high-risk activities should be subject to additional organisational accountability obligations that require them to 'proceed with caution' to ensure that individuals are protected from harms arising from those practices'.[572] A number of submitters expressed support for a requirement that APP entities conduct Privacy Impact Assessments (PIAs) before commencing inherently 'high risk' projects.[573]

PIAs are a formal documented process for systematically identifying the privacy risks of a proposed project and setting out recommendations for managing, minimising, or eliminating those risks.[574] They are currently required under the Privacy (Australian Government Agencies – Governance) APP Code 2017 for government agencies that undertake 'high privacy risk projects,' which is defined

---

[566] Submissions to the Issues Paper: OAIC, 90; Consumer Policy Research Centre, 12–13; Office of the Victorian Information Commissioner, 9.

[567] See, eg, OPC Canada, *A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act* (Discussion Paper, May 2016). See also OPC Canada, *Guidance on inappropriate data practices* (n 519).

[568] Submissions to the Issues Paper: Experian, 11; OAIC, 90–2; Salinger Privacy, 27; Interactive Games and Entertainment Association, 15.

[569] Submissions to the Issues Paper: Consumer Policy Research Centre, 12–13; Salinger Privacy, 23–4; Obesity Policy Coalition, 9; Office of the Victorian Information Commissioner, 9; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 34–6; Public Interest Advocacy Centre, 8; Experian, 11; Australian Information Security Association, 20; Professor Kimberlee Weatherall, 7; Uniting Church of Australia, 3; Privacy108, 13; Humanising Machine Intelligence Project, Australian National University, 3; Adobe, 5–6; Australian Privacy Foundation, 25; Data Synergies, 4, 45.

[570] Submissions to the Issues Paper: OAIC, 90.

[571] See, eg, Submission to the Issues Paper: Salinger Privacy, 24, considering whether explicit consent should be required for the collection, use and disclosure of location data, potentially by expanding the definition of sensitive information.

[572] Submission to the Issues Paper: OAIC, 90.

[573] Submissions to the Issues Paper: Salinger Privacy, 27; Privcore, 4; ElevenM, 2; Data Synergies, 4.

[574] OAIC, *When do agencies need to conduct a privacy impact assessment?*; OAIC, *Guide to undertaking privacy impact assessments*; UK ICO, *Data Protection Impact Assessments* (January 2021).

as personal information handling that is 'likely to have a significant impact on the privacy of individuals.'[575]

Data protection impact assessments (DPIAs) are also required under the GDPR for prescribed forms of personal data processing, including the large scale processing of sensitive data, the large scale and systemic monitoring of a publicly accessible area, and personal data processing that is likely to result in a high risk to individuals.[576] European supervisory authorities are also required to publish lists of processing activities for which DPIAs are mandatory.[577] For example, the UK ICO has also issued guidelines that require a DPIA to be conducted where an entity uses profiling or special category data to decide on access to services, and the use of biometric or genetic data in certain situations, among other situations.[578]

However, submitters expressed concerns about entities adopting a compliance mentality when undertaking PIAs such that the object of the exercise, to ensure privacy is built into the design of the project at its outset, is not realised.[579]

In light of these concerns, the Review is considering whether entities that engage in certain specified high risk practices (restricted practices) should be required to undertake additional organisational accountability measures to adequately identify and mitigate privacy risks in a flexible and scalable way.[580] Depending on the level of risk, an entity may need to conduct a formal PIA. Entities could be required to keep records of the process to demonstrate compliance with the Act for assessment by the Information Commissioner, if required.

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.

***'Large scale' test sourced from GDPR Article 35. Commissioner-issued guidance could provide further clarification on what is likely to constitute a 'large scale' for each type of personal information handling.*

[575] Privacy (Australian Government Agencies – Governance) APP Code 2017 s 12 ('Australian Government Agencies Privacy Code').
[576] *GDPR* (n 26) art 35.
[577] Ibid.
[578] UK ICO, *Data Protection Impact Assessments* (n 574).
[579] Submissions to the Issues Paper: Data Synergies, 4; Australian Privacy Foundation, 41–2.
[580] Submission to the Issues Paper: OAIC, 88. The OAIC recommended that APP 1 should require 'entities to take steps as are reasonable in the circumstances to implement practices, procedures and systems which will mitigate the risk of unfair and unreasonable information handling practices as a result of the entity's handling of personal information'.

An alternative approach put forward by submitters would be to increase individuals' opportunity to control their personal information in relation to restricted practices. As noted in the Issues Paper, this is already a feature of Australian privacy law through the requirement to obtain consent for the collection of sensitive information, as well as existing opt-out rights for direct marketing. However, these could be expanded to reflect emerging privacy risks in the digital age.

For example, Salinger Privacy submitted that consent should be required for the collection, use and disclosure of precise geolocation data by expanding the definition of sensitive information.[581]

The restricted practices proposed above could form a starting point for such a requirement, but would require adjustment to focus less on an organisational risk threshold that triggers the requirement. A number of mechanisms through which individuals could exercise control in relation to high-risk personal information handling could be explored, including consent through an expansion of the definition of sensitive information (see Chapter 2), absolute opt-out rights (see Chapter 14) or the provision of explicit notice about the high-risk practice.

11.1 – 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.

Prohibited practices ('no-go zones')

A number of submitters supported the introduction of prohibited practices into Australia's privacy law framework. It was considered that 'no-go zones' could be introduced either through legislation,[582] or Commissioner-issued guidance[583] that interprets an overarching requirement of fair and reasonable personal information handling.[584]

Submitters proposed a number of possible prohibited practices, including profiling and behavioural advertising knowingly directed at children,[585] the scraping of personal information from online platforms,[586] the tracking and sharing of mental health information other than by the individual's own health service providers,[587] or the use of information about an individual's emotional stress, mental or physical health or financial vulnerability that is shown to cause harm or discrimination.[588] The Office of the Privacy Commissioner of Canada has issued guidance on practices considered to be no-go zones.[589] Notable examples for consideration include entities requiring passwords to social media accounts to be provided for the purposes of employee screening and automated processing of personal information undertaken for the purpose of unlawful discriminatory treatment.[590]

---

[581] Submission to the Issues Paper: Salinger Privacy, 24, 26. See also Submission to the Issues Paper: Australian Communications Consumer Action Network, 12.
[582] Submissions to the Issues Paper: Australian Privacy Foundation, 25; Humanising Machine Intelligence Project, Australian National University, 3; Adobe, 8; Data Synergies, 4.
[583] Submissions to the Issues Paper: Data Synergies, 4; Salinger Privacy, 23; Public Interest Advocacy Centre, 8; Professor Kimberlee Weatherall, 8; Adobe, 5–6.
[584] Submissions to the Issues Paper: OAIC, 90–1; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 36; Professor Kimberlee Weatherall, 8; Consumer Policy Research Centre, 12–13.
[585] Submissions to the Issues Paper: Data Synergies, 4; OAIC, 91; Salinger Privacy, 23; Obesity Policy Coalition, 9.
[586] Submissions to the Issues Paper: OAIC, 91; Salinger Privacy, 26; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 30; Australian Medical Association, 9.
[587] Submission to the Issues Paper: Salinger Privacy, 24.
[588] Submission to the Issues Paper: Consumer Policy Research Centre, 12.
[589] OPC Canada, *Guidance on inappropriate data practices* (n 519).
[590] Submissions to the Issues Paper: Office of the Victorian Information Commissioner, 9; Experian, 9.

The Review is seeking additional feedback on whether prohibited practices should be introduced into Australia's privacy law framework, and which practices could be designated as being prohibited.

Any prohibited practice would need to be carefully calibrated and appropriately targeted, to avoid unintended blanket prohibitions that may proscribe beneficial or legitimate practices.[591] For example, a blanket prohibition on the online tracking and profiling of children may be undesirable as it could interfere with the development of services that may be beneficial for children and pose little privacy risk, such as music streaming services that provide personalised music recommendations based on the profiling of a child's past listening activity and predicted music interests. On this basis, an optimal implementation of prohibited practices could take place through Commissioner-issued guidance interpreting the proposed overarching fair and reasonable test (Chapter 10), as is the approach taken by the Office of the Privacy Commissioner of Canada.[592]

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?

[591] Submission to the Issues Paper: OAIC, 91; Consumer Policy Research Centre, 13; Interactive Games and Entertainment Association, 15.
[592] OPC Canada, *Guidance on inappropriate data practices* (n 519).

12. Pro-privacy default settings

The Issues Paper noted the DPI report recommendation that default settings enabling data processing for a purpose other than the performance of a contract should be preselected to 'off.' [593] The DPI report argued that such a requirement would prevent entities from using defaults to nudge users to select more intrusive data collection settings.[594]

Several submitters were in favour of a requirement to implement pro-privacy default settings.[595] Deloitte submitted results from the Deloitte 2020 Privacy Index, noting that 93% of consumers expect a service to provide them with an upfront option to opt-in to non-essential data handling practices, rather than having to opt-out of these practices.[596] While some submissions recognised that pro-privacy defaults may improve privacy protections, others argued that default settings may limit entities' ability to provide an optimal service if privacy settings are required to be set to maximum by default. For example, the Interactive Games and Entertainment Association submitted that pro-privacy defaults may have unintended consequences in the video games sector. This could include frustration for users, by requiring them to manually change their settings to access expected features such as selecting a server based on location, having a visible user profile within a game, finding and playing with their friends, and sharing content.[597] Some submitters considered that pro-privacy defaults may be inappropriate in certain sectors, such as healthcare or research, but may be beneficial to apply specifically to online platforms.[598]

Proposal

The Review is seeking feedback on whether regulated entities should be required to: (1) enable pro-privacy settings by default, or (2) make privacy settings easily accessible to individuals.

Option 1 would effectively require individuals to opt-in to certain personal information handling practices that are turned off by default. Some submitters considered whether such a default requirement should only be required for *certain* collections, uses and disclosures of personal information, such as sensitive information.[599] To this end, the UK ICO has created an Age Appropriate Design Code, which applies to digital services in the UK that are likely to be used by children.[600] The Age Appropriate Design Code encourages entities to implement 'high privacy' settings by default unless the entity can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child, or whether the processing is required for an entity's 'core or most basic service.' [601] The Code requires a number of default privacy settings, including that:

- geolocation options should be switched off by default, and entities should provide an obvious sign for children when location tracking is active

---

[593] ACCC, DPI report (n 2) 468.
[594] Ibid.
[595] Submissions to the Issues Paper: OAIC, 79; Dr Kate Mathews Hunt, 9; Salinger Privacy, 27; Shaun Chung and Rohan Shukla, 15; Cyber Security Cooperative Research Centre, 9; Legal Aid Queensland, 11; Electronic Frontiers Australia, 9; Deloitte, 22; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 28; Centre for Cyber Security Research and Innovation, 10; Experian, 15; Australian Information Security Association, 18; CAIDE and MLS, 9; Privacy108, 11; Consumer Policy Research Centre, 9; Australian Communications Consumer Action Network, 12.
[596] Submission to the Issues Paper: Deloitte, 22.
[597] Submission to the Issues Paper: Interactive Games and Entertainment Association, 13–4. See also Submission to the Issues Paper: Snap Inc., 4.
[598] Submissions to the Issues Paper: Department of Health of Western Australia, 6–7; CSIRO, 7.
[599] Submission to the Issues Paper: Griffith University, 13.
[600] UK ICO, *Age appropriate design: a code of practice for online services* (Web Page, September 2020) ('*Age appropriate design code*').
[601] Ibid ch 7 (Default settings).

- children's personal data should only be visible or accessible to other users of the service if the child amends their settings to allow this
- any optional processing of personal data, including any uses designed to personalise the service, have to be individually selected and activated by the child
- any settings which allow third parties to process personal data have to be activated by the child, and
- users should have the option to change settings permanently or just for the current use.

Submitters also proposed other broad thresholds that could trigger privacy default settings. For example, they suggested that high-privacy default settings be required for any personal information handling for a purpose other than for the performance of a contract,[602] for personal information handling that is not needed to enable the provision of the product or service,[603] or not necessary for delivering the APP entity's primary purpose.[604] The Review notes that the *Online Safety Act 2021* (Cth) ('Online Safety Act') contains a power for the Minister to determine basic online safety expectations for social media services, relevant electronic services and designated internet services, which could include privacy and safety settings by default.[605]

Option 2 would not require privacy settings to be set at a particular level by default, but would require entities to provide the individual with an easy and unambiguous way to select all settings to the most restrictive through a single click option. The OAIC noted that this option could incentivise entities to design consumer friendly and easy to use privacy controls, and place the responsibility on these entities to provide clear notices that persuade individuals as to why positively electing to change these default settings is in their best interests.[606]

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.

Questions

- Should pro-privacy default settings be enabled by default, or should requirements be limited to ensuring that privacy settings are clear and easy to access?
- If pro-privacy default settings are enabled by default, which types of personal information handling practices should be disabled by default?

[602] Submission to the Issues Paper: Legal Aid Queensland, 11. See also ACCC, DPI report (n 2) 468.
[603] Submissions to the Issues Paper: OAIC, 79; Cyber Security Cooperative Research Centre, 9.
[604] Submission to the Issues Paper: Optus, 8.
[605] See, *Online Safety Act 2021* (Cth) s 45 ('*Online Safety Act*'). See also Explanatory Memorandum, Online Safety Bill 2021 (Cth) 30; 'Safety by Design', *Office of the eSafety Commissioner*. On August 8 2021, the Department of Infrastructure, Transport, Regional Development and Communication released the Draft Basic Online Safety Expectations Determination 2021 for consultation. It provides that electronic services must take reasonable steps to ensure that end-users are able to use the service in a safe manner and notes that reasonable steps which could be taken in relation to children could include ensuring that the default privacy and safety setting of the children's service are set to the most restrictive level.
[606] Submission to the Issues Paper: OAIC, 79.

13. Children and vulnerable individuals

Children's privacy

The Act does not contain any express requirements regarding children's privacy. The Issues Paper sought feedback on whether the Act requires privacy protections for children in addition to those that will be developed through the OP code.[607]

Risks to privacy and potential harms for children

Submissions were broadly in favour of enhanced privacy protections for children in light of their particular vulnerability.[608] Submitters noted that children are increasingly engaging with technology, online platforms, mobile applications, IoT connected toys and social media, and expressed concern that entities may regularly share children's data for advertising purposes, or engage in harmful tracking, profiling of, or targeted marketing to children.[609] The DPI report noted that younger children may lack the technical, critical and social skills to engage with the internet in a safe and beneficial manner.[610]

Reset Australia submitted that some entities may collect 'thousands of data points' from children, which could include location, gender, interests, hobbies, moods, mental health and relationship status. This personal information can be used to identify moments when children are particularly vulnerable in order to more effectively target and engage them.[611] The Castan Centre for Human Rights cited evidence that while some children may recognise the risks of oversharing personal information online, they are likely to be less aware of the risks of online tracking.[612]

Online Privacy Bill

The OP Bill proposes a number of amendments to the Act to provide additional protections for children and vulnerable individuals.[613] The OP Bill proposes to define a 'child' in the Act as an individual 'who has not reached 18 years of age.' It will require that an OP code be developed which will introduce specific requirements[614] for how social media services, data brokerage services and large online platforms with at least 2.5 million end-users in Australia handle personal information, including stricter requirements for how they provide notice and seek consent from their users, and to stop using or disclosing an individual's personal information upon request. The OP code must then set out how all OP organisations will meet these requirements in relation to children and vulnerable persons.

In addition, the OP code will introduce stricter requirements for social media services to target the particular risks that social media services pose to children. Social media services will need to:

- take all reasonable steps to verify the age of individuals who use social media services

---

[607] Exposure Draft, OP Bill (n 1).
[608] Submissions to the Issues Paper: OAIC; Castan Centre for Human Rights Law – Monash University; Reset Australia; Data Synergies; Salinger Privacy; Australian Council on Children and the Media; Privacy108; Obesity Policy Coalition; Google; Snap Inc.; ACCC; Department of Health of Western Australia; Centre for Cyber Security Research and Innovation; Australian Information Security Association; Australian Communications Consumer Action Network; Fundraising Institute Australia; Guardian Australia; ABC; Deloitte; Royal Australian College of General Practitioners; Digital Rights Watch, Access Now, Centre for Responsible Technology Australia, Electronic Frontiers Australia, Fastmail and Reset Australia (joint submission); Uniting Church in Australia.
[609] Submissions to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 31; OAIC, 80, 84, 91; Privacy108, 11; Salinger Privacy, 23; Obesity Policy Coalition, 2–3.
[610] ACCC, DPI report (n 2) 448.
[611] Submission to the Issues Paper: Reset Australia, 7–8. See also Darren Davison, 'Facebook targets 'insecure' kids', *The Australian* (online, May 2017).
[612] Submission to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 32.
[613] Exposure Draft, OP Bill (n 1).
[614] Ibid sub-cl 26KC(5).

- ensure that the collection, use or disclosure of a child's personal information is fair and reasonable in the circumstances, with the best interests of the child being the primary consideration when determining what is fair and reasonable, and
- obtain parental or guardian consent before collecting, using or disclosing the personal information of a child who is under the age of 16, and take all reasonable steps to verify the consent. [615]

As children's personal information may be collected, used and disclosed in ways which may pose privacy risks to children by APP entities which may not be covered by the OP code, the Review is seeking feedback on the extent to which these requirements should apply more broadly.

Defining a child and determining capacity to consent

The Act currently does not make special provision for privacy protections that apply to persons under the age of 18, nor does it stipulate an age at which an individual has capacity to consent to their personal information being collected, used or disclosed.

As noted above, the OP Bill will define a child as an individual under the age of 18. Upon the registration of the OP code by the IC, social media services will be required to comply with specific protections in relation to children, including a requirement to obtain parental or guardian consent before collecting, using or disclosing the personal information of a child under 16.

The OAIC provides the following guidance on children and young people:

> *An APP entity handling the personal information of an individual under the age of 18 must decide if the individual has capacity to consent on a case-by-case basis. As a general rule, an individual under the age of 18 has the capacity to consent if they have the maturity to understand what's being proposed. If they lack maturity it may be appropriate for a parent or guardian to consent on their behalf. If it's not practical for an APP entity to assess the capacity of individuals on a case-by-case basis, as a general rule, an APP entity may assume an individual over the age of 15 has capacity, unless they're unsure*.[616]

The current OAIC guidance reflects the ALRC Report 108 recommendation that an assessment about the individual's capacity should be undertaken, but where impracticable, an individual aged 15 or over is presumed to be capable of giving consent, making a request, or exercising a right of access.[617]

Overseas approaches to children and capacity

Some overseas privacy laws have adopted separate age thresholds for when parental consent is required and when additional privacy protections will apply. For example, in the UK, only children aged 13 or over are able to provide their own consent,[618] and the recently introduced UK Age Appropriate Design Code includes standards to enhance protection of children up to the age of 18 when using digital services.[619] In the US, the Children's Online Privacy Protection Act ('COPPA') requires parental consent for children under the age of 13 years.[620] However, submitters noted that a major weakness of the COPPA framework is that it does not require entities to adopt age-

[615] Ibid sub-cl 26KC(6).
[616] OAIC, 'Children and Young People' (Web Page). See also OAIC, APP Guidelines (n 21) [B.56]–[B.58].
[617] ALRC Report 108 (n 53) [68.126].
[618] UK Department for Digital, Culture, Media & Sport, *General Data Protection Regulation Keeling Schedule* (13 December 2018) 10, Article 8(1) ('*General Data Protection Regulation Keeling Schedule*').
[619] UK ICO, *Age appropriate design code* (n 600) 17.
[620] *Children's Online Privacy Protection Act*, 15 USC §§ 6501-6506, 312.2 (1998) ('COPPA').

appropriate protocols for personal information collected from teenagers aged 13 and over, who may also require additional protection.[621]

Defining a child as a person under the age of 18 years

Some submitters to the Issues Paper sought clarity on how a child or minor would be defined for the purposes of child-specific privacy protections.[622] Some submissions proposed that child-specific privacy protections should apply up to the age of 18 years old.[623]

Defining a child as an individual under 18 years of age in the Act will allow for the application of child-specific privacy protections. This position would be consistent with the Online Safety Act[624], the UK Age Appropriate Design Code and Ireland's *Data Protection Act 2018*.[625]

Determining when a child has capacity to consent

The DPI report recommended strengthening the Act to require consent to be obtained from a parent or guardian for the collection of a child's personal information, but did not propose an age under which such a requirement should apply.[626] A number of submissions supported requiring entities to obtain parent or guardian consent to collect a child's information, although stakeholders were divided on whether capacity should be assumed at a defined age or determined on a case-by-case basis.[627] Some suggested that a 'bright-line' age limit be specified, noting the following age thresholds:

- 13 years of age,[628] in alignment with COPPA[629] and the UK GDPR[630]
- 14 years of age, when a child may take responsibility for their My Health Record[631]
- 15 years of age,[632] as per existing OAIC guidelines
- 16 years of age,[633] in alignment with the default age threshold under GDPR;[634] or
- 18 years of age.[635]

Other submitters opposed rigid age limits or 'one-size-fits-all' approaches on the basis that children have varying levels of maturity, and that an individualised assessment of capacity is consistent with available research on developmental psychology.[636] It was proposed that the Gillick competency test[637] could be adopted into Australian privacy law, which requires a case-by-case analysis of a

---

[621] Submission to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 35. It was acknowledged that the Federal Trade Commission encourages operators to do so, however the lack of legislative protections for teenagers was observed as a weakness of the framework.
[622] Submission to the Issues Paper: Communications Alliance, 8.
[623] Submissions to the Issues Paper: Obesity Policy Coalition, 3; Reset Australia, 8–9.
[624] *Online Safety Act* (n 605) s 5.
[625] *Data Protection Act 2018* (Irl) s 29. See also, Data Protection Commission Ireland, *Fundamentals for a child-oriented approach to data processing* (December 2020) 6 ('*Fundamentals for a child-oriented approach to data processing*').
[626] ACCC, DPI report (n 2) 456, 464–70, Recommendation 16(c). See also ALRC Report 108 (n 53) [68.126].
[627] Submissions to the Issues Paper: ACCC, 35–6; Google, 7; Snap Inc., 4; Department of Health of Western Australia, 7; Centre for Cyber Security Research and Innovation, 10; Australian Information Security Association, 18; Australian Communications Consumer Action Network, 13–14; Reset Australia, 8–9.
[628] Submissions to the Issues Paper: Google, 8; Snap Inc., 4; Centre for Cyber Security Research and Innovation, 10.
[629] COPPA 15 USC §§ 6501-6506 (1998).
[630] *General Data Protection Regulation Keeling Schedule* (n 618).
[631] Submission to the Issues Paper: Australian Medical Association, 8.
[632] Submission to the Issues Paper: Australian Council on Children and the Media, 2.
[633] Submissions to the Issues Paper: Australian Communications Consumer Action Network, 13–4; see also, Data Synergies, 44–5.
[634] GDPR (n 26) art 8(1).
[635] Submissions to the Issues Paper: Fundraising Institute Australia, 8; Reset Australia, 8–9; Obesity Policy Coalition, 3.
[636] Submissions to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 32; CSIRO, 7; Department of Justice and Community Safety, Victoria, 5; Australian Medical Association, 8.
[637] See *Secretary of the Department of Health and Community Services v JWB and SMB* (1992) 175 CLR 189.

minor's capacity to consent in terms of maturity and intelligence.[638] Others submitters questioned whether it may be appropriate to determine the validity of consent based on the character of the data, the uses the data is put to and the relationship between child and entity.[639]

Proposal – a parent or guardian's consent must be obtained where a child is under the age of 16

While defining a child as an individual below the age of 18 will allow for additional protections to apply across both the early childhood and teenage years, the current uncertainty regarding whether a child has capacity to consent to the collection, use or disclosure of their personal information could be addressed by adopting a specific age threshold at which capacity may be assumed.

The Castan Centre for Human Rights observed that a rigid age limit, as adopted in COPPA, provides clarity as companies can more easily establish whether a child is of a certain age than whether the child is of sufficient maturity to make their own privacy decisions, and that an individualised assessment of capacity leaves risks for children if there is a failure to correctly identify a lack of capacity.[640] Establishing capacity on a case-by-case basis is likely to be particularly problematic in online settings.

16 years of age is proposed in the OP Bill as the threshold under which social media services must obtain the consent of a parent or guardian, reflecting the particular risks social media services pose to children.[641] Some submissions to the Review supported 16 years of age as an age threshold that would promote a privacy protective outcome for children.[642] This would also be consistent with the default position under GDPR which applies in some countries in the EU including Germany and the Netherlands.[643]

However, other submitters suggested that a guardian's consent should only be required in the case of young children, as many teenagers may have developed the maturity, experience and understanding to consent on their own.[644] A lower age threshold may also recognise children's increasing need for independence and privacy from their parents or guardians as they mature, and that mature minors are less likely to consult their parents before signing up to an online service, or may not wish to reveal certain information to their parent or guardian.[645]

Specifying an age in the Act at which a child is assumed to have capacity to make privacy decisions would also determine when a child could exercise privacy requests independently of their parents, including access, correction, objection or erasure requests. However, the Act would continue to recognise situations where it is not appropriate for a parent or guardian to exercise requests on behalf of a child under the age of 16, such as where access would pose a serious risk to the life, health or safety of any individual, including the child. The Australian Medical Association noted that doctors must exercise judgment about disclosing a child's medical records to non-custodial parents in situations where there may be abuse or domestic violence.[646] Parental authority would be subject

[638] Submissions to the Issues Paper: Griffith University, 13; MIGA, 7; Shaun Chung and Rohan Shukla, 16; Australian Information Security Association, 18; Department of Justice and Community Safety, Victoria, 5.
[639] Submissions to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 33; IGEA, 14–15.
[640] Submission to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 30, 32.
[641] Exposure Draft, OP Bill (n 1), sub-cl 26KC(6).
[642] Submissions to the Issues Paper: Australian Communications Consumer Action Network, 13–4; see also, Data Synergies, 44–5.
[643] GDPR (n 26) art 8(1). Note however that the GDPR permits member states to derogate from this position in domestic law and provide a lower age threshold, provided that the lower age threshold is not below 13 years of age. Several EU member states have opted for a lower age threshold than 16 years, including the United Kingdom (pre-Brexit), France, Denmark, Spain and Sweden.
[644] Submission to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 39.
[645] Submission to the Issues Paper: MIGA, 7.
[646] Submission to the Issues Paper: Australian Medical Association, 8.

to the existing limitations contained in the respective APPs, for example, the grounds to refuse access under APPs 12.2 and 12.3.[647]

While a case-by-case assessment of a child's capacity is likely to be impractical in an online context, as well as in other contexts where an entity's engagement with a child is brief, it may be appropriate in situations where the entity has a relationship with the child and has historically relied on an individualised approach to assessing capacity, such as in the healthcare sector.[648] On this basis, the Review is seeking feedback on whether entities should be able to assess capacity on an individualised basis where it is practical to do so, as is permitted under existing OAIC guidance.[649]

13.1 Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16. The review is seeking additional feedback on whether APP entities should be permitted to assess capacity on an individualised basis where it is practical to do so.

Feedback is also sought on the circumstances in which parent or guardian consent must be obtained:

- **Option 1 – All collections of personal information**
  Parent or guardian consent to be required before collecting, using or disclosing personal information of the child under the age of 16.
- **Option 2 – Where consent is currently required under the Act**
  Parent or guardian consent to be required in respect of a child under the age of 16 in situations where the Act currently requires consent, including before the collection of sensitive information or as an available mechanism to undertake a secondary use or disclosure of personal information.

The assumed age of capacity would also determine when a child may exercise privacy requests independently of their parents, including access, correction or erasure requests.

Age and consent verification

The DPI report also recommended that an enforceable code of practice for digital platforms introduce requirements to verify that consent is given or authorised by the child's guardian.[650] Some submitters also proposed a requirement that service or product providers must determine the age of users they deal with, on the basis that age verification is necessary to ensure that entities are practically able to take steps to apply child-specific protections.[651]

Age and consent verification requirements are a feature of overseas data protection laws. The GDPR requires controllers to make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.[652] COPPA imposes an obligation on entities to obtain 'verifiable parental consent' before any collection, use, or disclosure, which may include consent forms to be signed by the parent, the use of a credit card or online payment system, the use of a toll-free phone number, or verification of government-issued identification.[653] The UK Age Appropriate Design Code prompts entities to take 'a risk-based approach to recognising the age of individual users and to either establish age with a level of certainty that is appropriate to the risks to child that arise from data processing, or apply the standards in that code to all service users instead.[654]

[647] *Privacy Act* (n 2) sch 1 APPs 12.2, 12.3.
[648] Submissions to the Issues Paper: MIGA, 7; Australian Medical Association, 8.
[649] OAIC, 'Children and Young People' (Web Page).
[650] ACCC, DPI report (n 2) 481–92.
[651] Submission to the Issues Paper: Uniting Church of Australia, 4.
[652] GDPR (n 26) art 8(2).
[653] COPPA 15 USC §§ 6501-6506, 312.5(a) (1998).
[654] UK ICO, *Age appropriate design code* (n 600).

The OP code will require social media services to take all reasonable steps to verify a user's age and parental consent. Details as to what constitutes 'all reasonable steps' could be provided in the OP code or Commissioner-issued guidelines, and may include consideration of available technologies, the privacy risks posed by a particular service and the security and privacy interests of users.[655]

Simplified privacy notices

The DPI report recommended that privacy notices be written at a level that can be readily understood by the minimum age of the permitted digital platform user.[656] A number of submitters supported the introduction of such a requirement, suggesting that privacy notices are currently difficult for children to understand, which can result in a lack of comprehension of online data processes and a lack of informed consent.[657]

Some submitters considered that the use of visual and graphical communication (including infographics or standardised icons) should be promoted, as some children are unlikely to engage with purely written privacy information.[658] Similar requirements have been introduced in the UK Age Appropriate Design Code, which encourages entities to use diagrams, cartoons, graphics, video and audio content rather than relying solely on written communications. [659] The OP code will need to make specific provision for ensuring that collection notices for children are clear and understandable, current and timely.[660]

Proposal

The proposed changes to the APP 5 notice obligations discussed in Chapter 8 would require privacy notices to be clear, current and understandable. This could be emphasised in cases where the information is addressed specifically to a child. The proposed requirement would help children's understanding of potential privacy and safety issues that may flow from certain types of personal information handling, and support the provision of informed consent where it is required from a mature minor. The proposed wording is modelled on Article 12(1) GDPR,[661] to implement the substance of the DPI report's recommendation in a technology neutral way. It would also align with the existing principles-based requirements in the Act that afford APP entities with a degree of flexibility in determining how to deliver an understandable privacy notice to children.

Visual or graphical communication could be used by an entity to ensure that its privacy notice is intelligible to children. Visual and graphical communication in privacy notices could also be encouraged in Commissioner-issued guidelines, or the OP code.

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

Limits on collections, uses and disclosures of children's personal information

Some submitters highlighted the limitations of seeking parental consent as a mechanism to protect children's privacy, noting some parents' lack of digital literacy, the impracticality of obtaining parental consent in online settings, and that some children are unlikely to seek the approval of their

---

[655] House of Representatives Standing Committee on Social Policy and Legal Affairs, Parliament of Australia, *Protecting the age of innocence: Report of the inquiry into age verification for online wagering and online pornography* (Report, February 2020), Ch 2.

[656] ACCC, DPI report (n 2) 456, 461–3 Recommendation 16(b).

[657] Submissions to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 41; Communications Alliance, 8; Centre for Media Transition, 16; Obesity Policy Coalition, 5–6.

[658] Submissions to the Issues Paper: Reset Australia, 8; Australian Council on Children and the Media, 3; Communications Alliance, 8.

[659] UK ICO, *Age appropriate design code* (n 600) 37–42.

[660] Exposure Draft, OP Bill (n 1), s 26KC(5).

[661] GDPR (n 26) art 12(1) provides that privacy information must be presented 'to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child'.

parents before signing up to a service.[662] These submitters considered that notice and consent requirements should be supplemented with substantive regulation of allowed and disallowed practices in relation to children.[663]

Fair and reasonable personal information handling and the best interests of the child

Some submitters considered that an overarching requirement to ensure the fair and reasonable handling of personal information would provide a degree of protection to children.[664] The proposed fair and reasonable test (Chapter 10) would permit the IC to determine whether the collection, use or disclosure of a child's personal information was inappropriate in the circumstances. In particular, it is proposed that the test include a factor regarding 'whether the collection, use or disclosure of the personal information is in the best interests of the child.'

The OP code will require social media services to ensure that the collection, use or disclosure of a child's personal information is fair and reasonable in the circumstances. In determining whether the collection, use or disclosure is fair and reasonable in the circumstances, the best interests of the child must be the primary consideration.[665]

The concept of the best interests of the child derives from the United Nations Convention on the Rights of the Child,[666] which has been adopted as a primary consideration in both the UK Age Appropriate Design Code and the Irish Data Protection Commission's Draft Fundamentals for a Child-Oriented Approach to Data Processing.[667] It requires entities to consider whether, throughout the handling of a child's personal information, a child's physical, psychological and emotional wellbeing is protected.[668]

The UK ICO has noted that taking account of the best interests of the child does not mean that entities cannot pursue their commercial or other interests, but where any conflict arises, it is unlikely that the commercial interests of an organisation will outweigh a child's right to privacy.[669] The Article 29 Working Party has further noted that in certain circumstances, the best interests of the child will necessitate a deviation from the protection of privacy, such as where the disclosure of personal information may be required from a teacher to a social worker in order to protect the child, either physically or psychologically.[670]

The fair and reasonable test may therefore be interpreted to limit certain acts and practices that are detrimental to a child's best interests and wellbeing, for example:

- online tracking, behavioural monitoring and profiling of children
- the disclosure of a child's personal information to a third party which exposes the child to potential safety or privacy risks, and
- the sale of a child's personal information.

---

[662] Submissions to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 35–6; The New York Times, 3; ABC, 6.
[663] Submissions to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 38; OAIC, 91; Salinger Privacy, 23; Australian Communications Consumer Action Network, 12; Guardian Australia, 15; Privacy108, 11; Obesity Policy Coalition, 2, 9; Australian Council on Children and the Media, 4.
[664] Submissions to the Issues Paper: Salinger Privacy, 23; Australian Communications Consumer Action Network, 12.
[665] Exposure Draft, OP Bill (n 1), sub-cl 26KC(6).
[666] *United Nations Convention on the Rights of the Child,* art 3.
[667] UK ICO, *Age appropriate design code* (n 600) 24; Data Protection Commission Ireland, *Fundamentals for a child-oriented approach to data processing* (n 625) 3, 13.
[668] See Committee on the Rights of the Children, *General Comment No 14: The right of the child to have his or her best interests taken as a primary consideration*, 62nd sess, UN Doc CRC/C/GC/14 (29 May 2013) 4; UK ICO, *Age appropriate design code* (n 600) 25.
[669] UK ICO, *Age appropriate design code* (n 600) 24, 26.
[670] Article 29 Data Protection Working Party, *Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)* (11 February 2009) 5–6.

In Canada, the Canadian Privacy Commissioner applied the 'appropriate purpose' test in section 5(3) PIPEDA to find that a reasonable person would not consider it appropriate for a youth-specific social media network to pre-select settings for its users that pushed users towards public disclosure of sensitive personal information.[671] This was particularly so 'given the special circumstances surrounding youth users and privacy' and the 'movement toward safer social networking for youth'.[672]

Prohibited acts and practices and privacy default settings

Some submitters proposed that certain acts or practices be prohibited in relation to children, in particular, profiling, tracking, online behavioural monitoring and advertising targeted at children.[673] For example, Ireland's *Data Protection Act 2018* expressly prohibits the processing of a child's personal data 'for the purposes of direct marketing, profiling or micro-targeting'.[674]

It was further proposed that the OAIC could issue guidance on child-specific 'no-go-zones'[675] which would not meet the requirements of the fair and reasonable test, similar to the Canadian Privacy Commissioner's guidance based on court interpretations of section 5(3) PIPEDA.[676]

Other submitters to the Review were supportive of the development of a children's privacy code,[677] such as the UK's Age Appropriate Design Code.[678] The DPI report also recommended that an enforceable code of practice for digital platforms introduce requirements to verify the provision of guardian consent, as well as restrict the collection, use or disclosure of children's personal information for targeted advertising or online profiling purposes and to minimise the collection, use and disclosure of children's personal information.[679] The Castan Centre for Human Rights suggested that the digital platform code could include 'key features of the UK Age Appropriate Design Code, thereby addressing children's desire for increased transparency, accessibility and flexibility in their dealings with online service providers'.[680]

The UK Age Appropriate Design Code sets out 15 standards of age-appropriate design, and focuses on providing default settings to ensure that children have the best possible access to online services whilst minimising data collection and use, by default. [681] It encourages entities to implement 'high privacy' settings by default unless the entity can demonstrate a compelling reason for a different default setting.[682]

The default privacy settings include that:

- geolocation options should be switched off by default, and entities should provide an obvious sign for children when location tracking is active
- children's personal data should only be visible or accessible to other users of the service if the child amends their settings to allow this

---

[671] *PIPEDA* (n 28) s 5(3).
[672] OPC Canada, *PIPEDA Report of Findings #2012-001* [92] – [102].
[673] Submissions to the Issues Paper: OAIC, 91–2; Australian Council on Children and the Media, 2; Obesity Policy Coalition, 8–9; Privacy108, 11.
[674] *Data Protection Act 2018* (Irl) s 30.
[675] Submissions to the Issues Paper: Salinger Privacy, 23; Guardian Australia, 15; Obesity Policy Coalition, 9.
[676] OPC Canada, *Guidance on inappropriate data practices* (n 519).
[677] Submissions to the Issues Paper: ABC, 5–6; Deloitte, 24; Royal Australian College of General Practitioners, 3.
[678] Submissions to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 39; Guardian Australia, 15; Reset Australia, 8; Digital Rights Watch, Access Now, Centre for Responsible Technology Australia, Electronic Frontiers Australia, Fastmail, Reset Australia (joint submission), 3.
[679] ACCC, DPI report (n 2) 481–92, Recommendation 18.
[680] Submission to the Issues Paper: Castan Centre for Human Rights Law – Monash University, 43.
[681] UK ICO, *Age appropriate design code* (n 600).
[682] Ibid 7.

- any optional uses of personal data, including any uses designed to personalise the service, have to be individually selected and activated by the child
- any settings which allow third parties to use personal data have to be activated by the child, and
- users should have the option to change settings permanently or just for the current use.

As discussed in Chapter 12, privacy default settings were supported by a number of submissions,[683] including some that specifically called for their application to children.[684] The Online Safety Act contains a power for the Minister to determine basic online safety expectations for social media services, relevant electronic services and designated internet services, which could include privacy and safety settings by default.[685]

The UK Age Appropriate Design Code also specifies that entities should not use children's personal data in ways that have been shown to be detrimental to their wellbeing and to collect only the minimum amount of personal data needed to provide elements of a service in which a child is actively and knowingly engaged.[686]

As noted above, the OP code will require social media services to ensure that the collection, use or disclosure of a child's personal information is fair and reasonable in the circumstances and that in determining whether the collection, use or disclosure is fair and reasonable in the circumstances, the best interests of the child must be the primary consideration.[687]

In developing the OP code, the code developer may consider including requirements similar to the UK's Age Appropriate Design Code in order to provide social media services with greater specificity as to what information handling practices will, and will not, constitute fair and reasonable collection, use and disclosure of children's personal information.

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?

[683] See, eg, Submissions to the Issues Paper: Legal Aid Queensland, 7; Deloitte, 22; Griffith University, 13; ID Exchange, 11; OAIC, 99–102; Australian Privacy Foundation, 24; Data Synergies, 44.
[684] Submissions to the Issues Paper: The New York Times, 3; Australian Council on Children and the Media, 4.
[685] See, *Online Safety Act* (n 605) s 45. See also Explanatory Memorandum, Online Safety Bill 2021 (Cth) 30; 'Safety by Design', *Office of the eSafety Commissioner*. On August 8 2021, the Department of Infrastructure, Transport, Regional Development and Communication released the Draft Basic Online Safety Expectations Determination 2021 for consultation. It provides that electronic services must take reasonable steps to ensure that end-users are able to use the service in a safe manner and notes that reasonable steps which could be taken in relation to children could include ensuring that the default privacy and safety setting of the children's service are set to the most restrictive level.
[686] UK ICO, *Age appropriate design code* (n 600).
[687] Exposure Draft, OP Bill (n 1), sub-cl 26KC(6).

Vulnerable individuals

In response to questions posed in the Issues Paper about children's privacy, some submitters said there was a need to consider additional or different privacy protections for other individuals with vulnerabilities, including adults experiencing temporary or permanent incapacity for reasons such as disability, illness and injury.[688]

Third party representatives

The Act permits third parties acting with consent

The Act enables individuals to make certain decisions, such as providing consent to the collection of their personal information, or requesting its correction. Nothing in the Act prevents an individual from nominating a third party to assist or make those decisions for them. For example, an individual could nominate their spouse or partner to request access to their personal information on their behalf under APP 12.

In its Report 108, the ALRC recommended the Act explicitly recognise third parties acting with the consent of the individual.[689] It said that introducing the concept of 'nominee' and providing for nominee arrangements would be consistent with the Act's emphasis on individual autonomy.

The Act permits third parties acting with legal authority

Individuals experiencing limited or lost capacity or communicative difficulty may not be able to make such nominations. In these circumstances, the authority of third parties is recognised in other ways. Generally, where a third party is legally appointed as a substitute decision maker, an APP entity should recognise this arrangement. In regard to the collection, use or disclosure of personal information, the 'required or authorised by or under an Australian law' exception should authorise substitute decision makers established by other laws. The onus is on the APP entity to verify the authority of third party decision makers.

The ALRC considered it was unnecessary to explicitly recognise formal arrangements as the relevant laws that give effect to legal appointments determine the extent to which third parties can substitute decisions under the Act. Providing an additional hurdle to recognition would add unnecessary complexity to the existing patchwork of state and territory laws.[690]

The Act recognises 'responsible persons' in limited circumstances

Outside of formal arrangements, the Act recognises relatives, friends and next-of-kin as 'responsible persons' in limited circumstances. For example, a health service provider may disclose health information about an individual to their responsible person where: the individual is incapable of giving or communicating consent and the disclosure is necessary to provide care or treatment, or for compassionate reasons.[691] The onus is on the provider to assess an individual's capacity and ensure the third party meets the definition of responsible person.[692]

The ALRC cautioned against the automatic and general recognition of informal care arrangements. Of particular concern was the unacceptable risk of interference with the privacy of an individual who cannot give consent and may not be aware that a third party is making decisions under the Act on their behalf.

---

[688] Submissions to the Issues Paper: Law Institute of Victoria, 9; Legal Aid Queensland, 7; Guardian Australia, 15; Salinger Privacy, 23.
[689] ALRC Report 108 (n 53) [70.101]–[70.102].
[690] Ibid [70.64].
[691] *Privacy Act* (n 2) s 16B(5). The concept of 'responsible person' is also applied in the context of emergency declarations: at s 80P.
[692] Ibid s 6AA.

Report 108 also considered whether to include a presumption of capacity in the Act, accompanied by a mechanism for assessing capacity. The ALRC concluded these measures were not appropriate because: 1) the presumption already exists at common law and 2) assessments of capacity are better dealt with in specialised legislation. It also acknowledged that assessing capacity is a complex task and imposing such a requirement on APP entities would be overly burdensome.[693] Submissions to that inquiry also raised concerns that capacity is contextual and a 'finding' of incapacity under the Act might impact assessments of capacity under other laws and for other purposes.

On balance, where the Act does not currently prevent third parties acting with consent or with legal authority, no changes are required to explicitly recognise these representative arrangements.

The proposed fair and reasonable test, discussed in Chapter 10, would require an APP entity to consider an individual's circumstances when collecting, using or disclosing their personal information. One factor relevant to the test would be whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the information handling. Further, the proposal to make notices clearer, shorter and less complex, as discussed in Chapter 8, would assist individuals experiencing incapacity to better understand relevant information so that they can make informed decisions.

The OP Bill provides that the OP code must require organisations bound by the code to address specific protections for individuals physically or legally incapable of giving consent. Further consideration of how the Act and APPs should apply to particular groups of people, including any additional or different protections for vulnerable adults, could be undertaken as part of developing the OP code.

[693] ALRC Report 108 (n 53) [70.49].

14. Right to object and portability

The Issues Paper did not expressly seek feedback on whether individuals should be able to request that entities cease collecting, using or disclosing their personal information. In the context of consent, feedback was sought on whether entities should be required to provide individuals with the option of withdrawing consent.

Individuals' ability to opt-out or withdraw consent

Under the Act, the point at which an individual has the best opportunity to control their personal information is the point at which it is collected. Where sensitive information is solicited, an individual may refuse to give consent. Where personal information is solicited, an individual may decide not to provide their information, which may have the effect that the individual's interaction or transaction with the APP entity goes no further.

The APPs are silent on whether consent may be withdrawn. Current OAIC guidance states that an individual may withdraw their consent and that this should be an easy and accessible process.[694] The guidance also notes that there may be possible consequences should consent be withdrawn, for example, an APP entity may no longer be able to provide the service to an individual.[695]

There is currently no mechanism under the Act to enable individuals to request that an APP entity no longer use or disclose personal information which the APP already holds. The OP code provides that organisations subject to the OP code will be required to take such steps (if any) as are reasonable in the circumstances to not use or disclose, or to not further use or disclose, an individual's personal information upon request from that individual.[696] The requirement would not prevent secondary uses or disclosures that are currently permitted under the Privacy Act, specifically uses or discloses that:

- are authorised or required by or under another Commonwealth, State or Territory law or court or tribunal order
- are reasonably necessary to assist a law enforcement body undertake an enforcement-related activity, or
- occur during a 'permitted general situation' or a 'permitted health situation', for example, in response to a serious threat to individual or public health or safety.[697]

Should individuals have more ongoing control over their personal information?

In the context of considering the efficacy of the notice and consent framework, some submissions indicated that enhancing individuals' ability to exercise ongoing control over their personal information is preferable to increasing reliance on consent at the point of collection, as privacy risks may change over time.[698]

A number of submissions highlighted the right to object under the GDPR[699] and proposed that an equivalent mechanism should be considered in the Australian context.[700] The 2020 ACAP Survey indicated that 77 per cent of respondents were supportive of having a right to object to certain data

[694] OAIC, APP Guidelines (n 21) [B.51]; OAIC, *Consent to the handling of personal information* (Web Page, 2020).
[695] OAIC, *Consent to the handling of personal information* (n 694).
[696] Exposure Draft, OP Bill (n 1); Explanatory Paper, OP Bill (n 1) 10.
[697] Explanatory Paper, OP Bill (n 1), 10.
[698] See, eg, Submission to the Issues Paper: Humanising Machine Intelligence Project, Australian National University, 3, who argued that 'the issues paper focuses quite narrowly on the collection of data, with less attention on its analysis and use. The latter, however, is where effects on consumers occur.'
[699] GDPR (n 26) art 21; UK ICO, 'Right to Object', *Guide to the General Data Protection Regulation* (January 2021) ('Right to Object').
[700] Submissions to the Issues Paper: OAIC, 54–5; Office of the Information Commissioner Queensland, 3; Australian Information Security Association, 23; CAIDE and MLS, 8; Rights in Records by Design, 2–3; Reset Australia, 7; Humanising Machine Intelligence Project, Australian National University, 3.

practices (for example, selling of personal information) while still being able to access and use the service.[701] The Centre for AI and Digital Ethics and Melbourne Law School noted that a right to object would not constitute a veto over appropriate data usage, but would help to limit continued processing where compelling legitimate grounds for that processing cannot be demonstrated.[702] The OAIC's submission noted that a right to object would complement a right to erasure by allowing an individual to stop certain types of data use or disclosure without necessarily requiring the erasure of their personal information, which is important where individuals wish to continue using a service.[703]

Some submitters considered that an option to withdraw consent should be formalised in statute,[704] as this would act as a check on APP entity conduct[705] and provide additional control and transparency over personal information handling processes.[706] The OAIC considered that APP entities should also be required to notify an individual of their right to withdraw consent, where consent has been obtained.[707] MIGA expressed concern about the ability for individuals to withdraw consent in the healthcare sector, arguing that it may impede the provision of appropriate healthcare.[708] Some industry stakeholders observed that where an individual does not provide consent, an entity's commercial model may no longer be viable,[709] stating that it may be a reasonable commercial response to restrict access to a service or certain functions within the service.[710] The ACMA noted that withdrawal of consent is framed differently across the Privacy Act, Spam Act and DNCR Act, which may be confusing for consumers and industry.[711]

International approaches to opt outs and objection rights

The GDPR's right to object enables individuals to request that entities no longer process personal data in certain circumstances.[712] It is available where personal data has been processed for the purpose of direct marketing, or for an entity's 'legitimate interests' or a 'public task'[713] and the entity cannot demonstrate a 'compelling reason' to continue processing.[714] The right to object is generally not absolute, except in relation to individuals' ability to cease the processing of personal data for the purpose of direct marketing.[715]

Other overseas jurisdictions also provide data subjects with specific opt-out rights in relation to certain practices. For example, California's CCPA provides individuals with a right to request that a business cease selling their personal information to third parties, and requires businesses to provide a 'clear and conspicuous link' on their webpage entitled 'Do Not Sell My Personal Information'.[716] The 2023 CPRA amendments to the CCPA will introduce a new right to restrict the use and disclosure

[701] OAIC, 2020 ACAP Survey (n 51) 67.
[702] Submission to the Issues Paper: CAIDE and MLS, 8.
[703] Submission to the Issues Paper: OAIC, 54.
[704] Submissions to the Issues Paper: OAIC, 80; Consumer Policy Research Centre, 7, 12; Dr Kate Mathews Hunt, 11; Australian Privacy Foundation, 25; Legal Aid Queensland, 12; Snap Inc, 4; Deloitte, 26; Cyber Security Cooperative Research Centre, 9; Gadens, 10; HIV/AIDS Legal Centre, 7; AusPayNet, 11; Australian Financial Markets Association, 11.
[705] Submission to the Issues Paper: AusPayNet, 11.
[706] Submission to the Issues Paper: Deloitte, 26.
[707] Submission to the Issues Paper: OAIC, 79.
[708] Submission to the Issues Paper: MIGA, 8.
[709] Submissions to the Issues Paper: Illion, 4; Google, 7.
[710] Submission to the Issues Paper: Illion, 4.
[711] Submission to the Issues Paper: Australian Communications and Media Authority, 5.
[712] GDPR (n 26) art 21.
[713] Ibid arts 6(1)(e)-(f).
[714] UK ICO, Right to Object (n 699).
[715] Ibid.
[716] CCPA (n 27) § 1798.135(a)(1).

of sensitive information to those which are necessary to perform services or provide goods that are reasonably expected by an average consumer.[717]

Under the GDPR, individuals have a specific right to withdraw consent, though the act of withdrawing consent does not retrospectively affect the lawfulness of past processing based on consent.[718] The GDPR requires that it 'shall be as easy to withdraw as to give consent',[719] and that individuals must be informed of their right to do so.[720] Singapore's *Personal Data Protection Act* and also permits individuals to withdraw consent as would have Canada's Bill C-11. Upon receiving a request to withdraw consent, entities must inform the individual of any likely consequences of withdrawal.[721] Upon receiving a request, the entity must cease collecting, using or disclosing the personal information, unless otherwise required or authorised by Singaporean law,[722] or under the 'reasonable terms' of a contract.[723]

Proposal

Objecting to collection, use or disclosure

Building on the OP code requirement that covered organisations must cease using or disclosing personal information upon request, the Act could be amended to enable individuals to object or withdraw consent to the collection, use or disclosure of personal information by any APP entity under the Act. Where an individual objects or withdraws consent to the collection, use or disclosure of their personal information, an entity would be required to take reasonable steps to stop collecting personal information from that individual or to stop further using or disclosing that personal information. The entity would be required to inform the individual of the consequences of the objection.

One consequence may be that an entity is unable to offer an individual a product or service or continue to provide the individual with a product or service if the collection, use or disclosure of the individual's personal information is necessary to provide the product or service. However the fair and reasonable test would apply to assess the collection, use or disclosure of personal information in those circumstances. This could involve consideration of the amount and sensitivity of the personal information collected and whether its use was reasonably necessary to achieve the functions and activities of the entity such that the individual could not be offered the service without it. It may also involve consideration of whether the individual's loss of privacy as a result of the collection, use or disclosure is proportionate to the benefit of the service.

Similar to the OP code, the requirement that an entity take *reasonable steps* to stop collecting, using or disclosing personal information on request would allow for continued collection, use or disclosure in certain circumstances, such as where further collection, use or disclosure is required:

- to complete a transaction or give effect to a contract
- to provide a service or product the individual has requested
- due to the application of an Australian law, court or tribunal order
- due to a permitted general or health situation, or
- to assist a law enforcement body undertake an enforcement-related activity.

[717] CPRA (n 120) § 1798.121.
[718] GDPR (n 26) art 7(3).
[719] Ibid.
[720] Ibid art 13(2).
[721] *Personal Data Protection Act 2012* (SG) s 16(1), (2); Bill C-11 (n 394) sub-cl 17(2).
[722] *Personal Data Protection Act 2012* (SG) ss 16(4), 25; Bill C-11 (n 394) sub-cl 17(1).
[723] Bill C-11 (n 394) sub-cl 17(1).

An ability to object or withdraw consent would enable individuals to exercise control as the use or disclosure of their personal information takes place, and as privacy risks emerge over time.[724] The ability to withdraw consent is a feature of the Consumer Data Right.[725]

Where an individual objects or withdraws consent to the collection, use or disclosure of their personal information and the entity stops collecting, using or disclosing that personal information, depending on the circumstances, this may enliven the obligation in APP 11.2 to destroy or de-identify (or anonymise as proposed in Chapter 2) the relevant personal information. However the intent of an individual objecting to the collection, use or disclosure would not be to necessarily require erasure of personal information. As is contemplated by the GDPR's right to object, the ability to object to data processing applies to specific purposes for which personal information can be used.[726] This is distinct from the right to erasure which applies to the personal information itself.

As an objection may be exercised in relation to specific purposes for using personal information (for example, direct marketing), the destruction or de-identification obligation would not be enlivened if the entity was required to retain the information for other purposes, including to provide other aspects of the service, internal record keeping requirements in connection with providing the service, or legal retention requirements. Nevertheless, if a right to object is introduced, a successful objection could be grounds for a further erasure request as is the case under Article 17(1)(c) of the GDPR. This is discussed further in Chapter 15. In light of submitter concerns regarding the privacy risks of technology which collects and uses personal information for the purpose of targeted marketing, the Act could also be amended so that individuals would have an unqualified ability to object to direct marketing. That is, an entity would be required to stop collecting, using or disclosing the personal information, not just take reasonable steps to do so. This proposal is discussed in greater detail in Chapter 16.

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.

Personal information portability

A small number of submitters suggested that a personal information portability right should be introduced, similar to the data portability right that exists in Article 20 GDPR,[727] or that individuals should otherwise be permitted to download their data, subject to public policy exceptions.[728] Australia has taken a sectoral approach to data portability through the Consumer Data Right (CDR),[729] which currently applies to certain entities in the banking sector, and is due to apply to the energy and telecommunication sectors, with an intent to expand the scheme on a sector-by-sector basis over time.[730] Introducing personal information portability in the Act may duplicate aspects of the CDR scheme and create unnecessary regulatory complexity.

[724] Submissions to the Issues Paper: Salinger Privacy, 19; Electronic Frontiers Australia, 8.
[725] *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) sub-r 4.11(3)(g) ('*CDR Rules*').
[726] See, Jef Ausloos, *The Right to Erasure in EU Data Protection Law* (Oxford University Press, 2020) 212. Ausloos states that: '[t]his distinction is crucial in a modern-day context, where the same personal data is often processed for an incalculable number of purposes. The right to object only prevents further processing for one or more delineated purposes, whereas the right to erasure prevents processing of any kind as the data can no longer be stored by the controller.'
[727] Submissions to the Issues Paper: Australian Information Security Association, 23; Digital Rights Watch, 4; Reset Australia, 7; Oracle, 4, 20–3.
[728] Submissions to the Issues Paper: Google, 10; Dr Kate Mathews Hunt, 12.
[729] *CCA* (n 67) pt IVD.
[730] Treasury, *Consumer Data Right Overview* (9 May 2018) 3–4.

15. Right to erasure of personal information

The Issues Paper sought feedback on whether a right to erasure should be introduced into the Act, including how to achieve greater individual control of personal information through a right to erasure without negatively impacting other public interests.

The DPI report recommended that APP entities be required to erase an individual's personal information on request, unless the retention of information is necessary for the performance of a contract to which the individual is a party, is required under law, or is otherwise necessary for an overriding public interest reason.[731] The government's response to the DPI report stated that the Review would need to consider potential freedom of speech concerns, challenges during law enforcement and national security investigations, and practical difficulties for industry that could flow from a legal obligation to erase personal information on request.[732]

Submissions to the Issues Paper expressed a high level of interest in the right to erasure, with a large number of submissions supporting and opposing such a right. Submissions that supported a right to erasure came from industry (including technology companies), academics, not-for-profits, peak bodies, state and federal privacy commissioners and some public sector agencies. Submitters that were supportive generally acknowledged that a right to erasure should not be absolute in application, and should be qualified by exceptions for circumstances in which the interests of the APP entity, or the public interest, outweigh an individual's privacy interests.[733] Submissions that identified challenges with introducing a right to erasure included some public sector agencies[734] and stakeholders from the telecommunications, healthcare and financial services sectors.[735] Many submitters that opposed the right to erasure expressed concern about its potential application in specific circumstances.

Benefits of introducing a right to erasure

Submissions that supported a right to erasure considered it would provide individuals with greater control over their information, place consumers in a stronger bargaining position relative to digital platforms and enable meaningful consent withdrawal or deletion of personal information where it is being used for a different purpose to what was originally agreed.[736] It was considered that erasure rights could protect children from data practices that enable a 'digital footprint' to be collated on them that extends beyond the age of majority and that deletion should be made easier for sensitive information or information that relates to consumer vulnerabilities, such as income levels, ethnic background, or whether they have a disability or serious illness,[737] particularly where this has been inferred by digital platforms.

---

[731] ACCC, DPI report (n 2) 35.
[732] Treasury, DPI response (n 18) 17.
[733] Submissions to the Issues Paper: Law Council of Australia, 20–1; Centre for Cyber Security Research and Innovation, 11; Centre for Media Transition, University of Technology Sydney, 19; Cyber Security Cooperative Research Centre, 10; Deloitte, 28–9; Experian, 22; Information Technology Industry Council, 2–3; Legal Aid Queensland, 13; Office of the Information Commissioner Queensland, 3–4; Palo Alto Networks, 3–4.
[734] Submissions to the Issues Paper: Department of Health of Western Australia, 9; National Archives of Australia, 6–8.
[735] Submissions to the Issues Paper: Communications Alliance, 10; Optus, 11–12; Telstra Corporation Ltd and Telstra Health Pty Ltd, 10; Australian Institute of Health and Welfare, 3; Australian Medical Association, 10; Avant Mutual, 13–14; MIGA (Supplementary Submission), 2–3; Ramsay Healthcare, 9; Australian Banking Association, 7; Australian Financial Markets Association, 12–13; Financial Planning Association, 4; Financial Services Council, 17–18; Fintech Australia, 12; Insurance Council of Australia, 5; KPMG, 7, 20.
[736] Submissions to the Issues Paper: Australian Department of Health, 10; CAIDE and MLS, 8; Centre for Media Transition, University of Technology Sydney, 18–19; Consumer Policy Research Centre, 9–10; Oracle, 15. See also ACCC, DPI report (n 2) 471.
[737] Submissions to the Issues Paper: Australian Council on Children and the Media, 2, 4; Consumer Policy Research Centre, 9–10.

These submissions pointed to the existing erasure rights in Europe's GDPR and California's CCPA, and the exceptions in those respective data protection laws, as a model for Australia.[738] Submitters also observed that equivalent rights to erasure currently exist in a number of data protection laws in the Asia-Pacific region, including Japan, South Korea, Thailand, Taiwan and Indonesia.[739] Some submitters suggested that the GDPR has demonstrated that erasure rights do not impose unreasonable regulatory or financial burdens on data processors.[740] However, the regulatory burden would likely be higher for entities processing complex erasure requests, such as the deletion of technical vehicle-generated data from connected vehicles (discussed further below).[741]

The joint submission of the Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law submitted that by aligning with overseas approaches, Australian courts and regulators may benefit from emerging comparative jurisprudence that considers the complexities and balancing of interests inherent in an erasure request.[742] Some submitters noted that the ability to make an erasure request is available under Australia's CDR[743] and My Health Record[744] schemes.[745]

Deloitte's Media Consumer Survey 2021 indicated strong support among participants for additional measures to enable consumers to delete their data, with 79 per cent of respondents saying they would either be 'likely' or 'very likely' to use a right to erasure.[746] The most commonly cited reasons for wishing to erase personal information included receiving too many marketing communications, not wanting an entity to hold onto personal information after they stop dealing with the entity, and not trusting the entity to use personal information responsibly.[747] The OAIC submitted that entities already have an obligation under APP 11.2 to destroy or de-identify personal information, and that the processes and procedures they have in place to comply with this obligation should ease the compliance burden of a right to erasure.[748]

Challenges of introducing a right to erasure

Some submitters considered that the deletion of records could make it difficult to prove that an interaction with an individual had taken place,[749] which could make the resolution of customer

[738] Submissions to the Issues Paper: Atlassian, 5; Australian Information Security Association, 23; Centre for Cyber Security Research and Innovation, 11; Centre for Media Transition, University of Technology Sydney, 18–19; Digital Rights Watch, 4; Dr Kate Mathews Hunt, 12; Electronic Frontiers Australia, 11; elevenM, 3; Facebook, 3; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 33; HIV/AIDS Legal Centre, 7; ID Exchange, 12; James Scheibner (ETH Zurich) and Dianne Nicol (University of Tasmania), 5–6; Office of the Information Commissioner Queensland, 3–4; Obesity Policy Coalition, 10; Palo Alto Networks, 3; SBS, 8; Shaun Chung and Rohan Shukla, 19; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 8.

[739] Submissions to the Issues Paper: Deloitte, 27–9; James Scheibner (ETH Zurich) and Dianne Nicol (University of Tasmania), 5–6.

[740] Submissions to the Issues Paper: Centre for Media Transition, University of Technology Sydney, 18–19; Dr Kate Mathews Hunt, 12.

[741] Submissions to the Issues Paper: Federal Chamber of Automotive Industries, 20.

[742] Submission to the Issues Paper: The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 8. See also David Erdos and Krzysztof Garstka, 'The 'right to be forgotten' online within G20 statutory data protection frameworks' (2020) 10(4) *International Data Privacy Law* 1, for a discussion of the balancing of interests required to support an erasure right. The authors argue that rights to erasure are a 'qualified right which can be limited or even extinguished when there are compelling legitimate reasons justifying the continued dissemination of personal data. In principle, such a right must be supported by relatively flexible substantive norms that can be interpreted contextually'.

[743] *CDR Rules* (n 725) sub-div 4.3.4.

[744] *My Health Records Act 2012* (Cth) sub-s 17(3) s 51 ('*MHR Act*').

[745] Submissions to the Issues Paper: CSIRO, 8–9; OAIC, 52; Privacy108, 14; SBS, 8.

[746] Deloitte, *Deloitte Australian Privacy Index 2021* (Report, 2021) 11.

[747] Ibid.

[748] Submission to the Issues Paper: OAIC, 53.

[749] Submission to the Issues Paper: Business Council of Australia, 5.

complaints challenging post-deletion.[750] Some submitters suggested that the need for a right to erasure was negated by the existing retention limitation requirements in APP 11.2.[751] However, a right to erasure would differ from APP 11.2, which involves an entity determining if destruction of personal information should occur, as opposed to an individual instigating the deletion of personal information.

Some submitters noted that it may be technically impracticable to undertake deletion of certain records,[752] for example, IT backup tapes that are technically incapable of deleting a single person's data,[753] removal of one person from CCTV footage,[754] or telecommunications network data.[755] Submitters expressed concern about the costs of complying with a right to erasure,[756] and considered that deletion should not be required for data that has an incidental link to an individual or where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the consumer's privacy or community expectations.[757]

Some submitters considered that erasure should not be required where information must be retained to safeguard public interests such as freedom of speech, freedom of the media and national security.[758] Submitters also considered that erasure rights should not impede the functions of investigative or law enforcement activities, nor enable individuals to erase data that reveals involvement in serious criminal activity.[759]

Proposals

Introduce a right to request erasure on certain grounds

The Review is still considering the benefits and challenges of permitting erasure requests under the Act. In light of competing stakeholder views about the benefits and challenges of introducing a right to erasure, the Review is seeking further feedback on the most appropriate means of introducing a right to erasure that would provide individuals with greater control over their personal information without negatively impacting other public interests.

Deloitte's submission suggested that consideration should be given to establishing defined circumstances for a right to erasure, in order to strike an appropriate balance between individual protections, the interests of APP entities and the broader public interest.[760] Some submitters considered that a right to erasure should be underpinned by withdrawal of consent.[761] A number of submissions pointed to defined circumstances in which the deletion of an individual's personal information could be warranted, including the deletion of children's personal information, sensitive

[750] Submissions to the Issues Paper: Australian Finance Industry Association, 5–6; Financial Planning Association, 4, Insurance Council of Australia, 5.
[751] Submissions to the Issues Paper: AGL, 4; Interactive Games and Entertainment Association, 17–18; KPMG, 7; Telstra Corporation Ltd and Telstra Health Pty Ltd, 10; United States Chamber of Commerce, 5–6.
[752] Submissions to the Issues Paper: Australian Finance Industry Association, 5-6; Facebook, 43; Law Institute of Victoria, 11–12.
[753] Submissions to the Issues Paper: Business Council of Australia, 5; CSIRO, 8-9.
[754] Submissions to the Issues Paper: Law Council of Australia, 20–1; Law Institute of Victoria, 11–12; Shopping Centre Council of Australia, 1.
[755] Submission to the Issues Paper: Telstra Corporation Ltd and Telstra Health Pty Ltd, 10.
[756] Submissions to the Issues Paper: CSIRO, 8–9.
[757] Submissions to the Issues Paper: BSA|The Software Alliance, 7; CSIRO, 8–9; Federal Chamber of Automotive Industries, 20; Law Council of Australia, 20–1; Optus, 11–12.
[758] Submissions to the Issues Paper: ABC, 6; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 8; Cyber Security Cooperative Research Centre, 4, 10; Information Technology Industry Council, 2–3.
[759] Submissions to the Issues Paper: Data Republic, 14; Financial Services Council, 17–18; Uniting Church of Australia, 5.
[760] Submission to the Issues Paper: Deloitte, 29.
[761] Submissions to the Issues Paper: Dr Chris Culnane and Associate Professor Ben Rubinstein, 18; Experian, 22; Griffith University, 15; Law Council of Australia, 20–1.

information, or information relating to an individual's vulnerabilities.[762] Some submitters indicated that a right to erasure should be applied to certain sectors, such as to digital platforms.[763]

The GDPR right to erasure, which is limited to six non-cumulative grounds, could be used as a model for a right to erasure in Australia.[764] The Act could be amended so that an individual could make a request for erasure of personal information where one of the following grounds applied:

- 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, or
- the personal information relates to a child and erasure is requested by the child, parent or authorised guardian, subject to Proposal 13.1.

This would be subject to exceptions that are discussed further under Proposal 15.2 below. This option is modelled on the positive grounds that underpin the GDPR right to erasure in Article 17(1). It would seek to permit erasure of personal information that poses the greatest privacy risks to individuals (including sensitive information or the personal information of a child) and where personal information should otherwise be destroyed. In doing so, the proposal would attempt to achieve a balance with public interests that may necessitate the retention of personal information in certain circumstances, as well as mitigate the risk of personal information being erased that may be relevant to a subsequent law enforcement or intelligence investigation. The proposal might also operate to increase the efficacy of APP 11.2 where personal information is not destroyed or de-identified as required,[765] by enabling an individual to initiate this process at their request.

15.1 An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions at 15.2, below:

- the personal information must be destroyed or de-identified under APP 11.2
- the personal information is sensitive information
- an individual has successfully objected to personal information handling through the right to object (see Chapter 14)
- the personal information has been collected, used or disclosed unlawfully
- the entity is required by or under an Australian law, or a court/tribunal order, to destroy the information, and
- the personal information relates to a child and erasure is requested by a child, parent or authorised guardian.

Exceptions to a right to erasure

The ACCC recommended that exceptions to any right to erasure should apply where the retention of information is necessary for the performance of a contract to which the consumer is a party, is

[762] Submissions to the Issues Paper: Australian Council on Children and the Media, 2, 4; Castan Centre for Human Rights Law – Monash University, 37; Consumer Policy Research Centre, 9–10; Obesity Policy Coalition, 10; Privacy108, 14.
[763] Submission to the Issues Paper: Oracle, 15.
[764] See GDPR (n 26) art 17(1). The six grounds are: (1) personal data is no longer necessary in relation to the purposes for which they were collected or processed; (2) the data subject withdraws consent and there is no other legal ground for processing; (3) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing; (4) the personal data has been unlawfully processed; (5) compliance with a legal obligation in Union or Member State law; and (6) the personal data has been collected from a child in relation to the offer of information society services referred to in Article 8(1).
[765] Ausloos, *The Right to Erasure in EU Data Protection Law* (n 726) 235.

required under law, or is otherwise necessary for an overriding public interest reason.[766] Submitters identified these circumstances and a number of other situations where the public interest or the interests of an APP entity in retaining personal information should prevail over an individual's interest in seeking erasure.

The Review is seeking feedback on what exceptions may be appropriate for a right to erasure in the Act to address concerns in relation to freedom of speech, challenges during law enforcement and national security investigations, and practical difficulties for industry.[767] The following possible exceptions respond to the major concerns expressed in submissions. A number of additional possible exceptions are set out at the conclusion of this section.

Personal information is required for a transaction or contract

In line with the DPI recommendation, submitters considered that an exception should apply where personal information must be retained to complete a transaction, or for the performance of a contract.[768] This would avoid the practical difficulty that would arise if an individual lodged an erasure request before a business transaction was complete – for example, an individual who orders goods online and submits an erasure request to the e-commerce merchant before the order is dispatched. At a minimum, the entity would need to retain the customer's contact details and address to ensure that their order could be delivered. Exceptions to this effect apply in California and were also proposed in the Canadian Bill C-11.[769]

Erasure is technically impractical or would constitute an unreasonable burden

Submitters expressed concern about the application of a right to erasure where deletion may be technically impractical or impossible.[770] It was also suggested that erasure should not be required where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the consumer's privacy or community expectations, or where the link to an individual is incidental.[771] SBS noted that under the CDR, the duty on regulated entities following a successful erasure request is to only conduct deletion 'to the extent reasonably practicable'.[772]

Japan's *Act on the Protection of Personal Information 2003* contains an exception to this effect, such that erasure is not required if the entity would incur significant expense, where it is difficult to erase the retained personal data and where 'necessary alternative action is taken to protect a principal's rights and interests'.[773]

Erasure would hinder law enforcement

Some submitters considered that exceptions may be required to ensure that a right to erasure does not hinder law enforcement operations by allowing the deletion of personal information that could

---

[766] ACCC DPI report (n 2) 35.
[767] Treasury, DPI response (n 18) 17.
[768] ACCC DPI report (n 2) 470. Submissions to the Issues Paper: AusPayNet, 12; Calabash Solutions, 9; CAIDE and MLS, 8; Information Technology Industry Council, 2–3; Legal Aid Queensland, 13; Optus, 11–12.
[769] CCPA (n 27) § 1798.105(d)(1). The exception applies where personal information must be retained to: [c]omplete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer. See also Bill C-11 (n 394) sub-cl 55(1)(b).
[770] Submissions to the Issues Paper: Business Council of Australia, 5; CSIRO, 8–9; Federal Chamber of Automotive Industries, 20; Law Council of Australia, 20–1; Law Institute of Victoria, 11–12; Telstra Corporation Ltd and Telstra Health Pty Ltd, 10.
[771] Submissions to the Issues Paper: BSA|The Software Alliance, 7; Federal Chamber of Automotive Industries, 20; Law Council of Australia, 20–21; Optus, 11–12. For example, certain types of telecommunications network data.
[772] See *CDR Rules* (n 725) sub-r 1.18. See also Submissions to the Issues Paper: AGL, 4; CSIRO, 8–9.
[773] Act on the Protection of Personal Information 2003 (Japan) Art 30(2), *translated* Personal Information Protection Commission Japan.

be evidence of the commission of a crime.[774] The Uniting Church expressed concern that individuals should not be able to request the erasure of data that may reveal an individual's involvement in serious criminal activity, such as online child sexual abuse, human trafficking, illicit drug trafficking, money laundering, tax evasion, bribery and fraud, and was supportive of the mandatory metadata retention scheme as a risk mitigation measure.[775]

An alternative approach could be an exception based on the existing APP 12.3(i), which would apply where an APP entity reasonably believes that erasure would be likely to prejudice one or more enforcement-related activities conducted by, or on behalf of, an enforcement body.[776] The Interactive Games and Entertainment Association suggested that a law enforcement public interest exemption may be problematic if there had been no approach from law enforcement at the time of an erasure request, and queried whether the onus would be on the APP entity to pre-emptively assess all of the individual's chat logs to identify potential evidence of child grooming.[777]

In addition, an exception to erasure for joint personal information may alleviate the impacts on law enforcement. Such an exception would be based on APP 12.3(b) and would prevent the erasure of information that relates to multiple individuals, such as photographs posted on a social media page. An indirect consequence of such an exception may be to reduce the incidence of erasure of chat logs or online messages that may reveal involvement in online criminal activity, such as illicit drug trafficking.

Public interest and freedom of expression

As indicated in the government response to the DPI report, there are likely to be other key public interest reasons to retain information in certain circumstances. It was also acknowledged by submitters that there may be public interest reasons to retain personal information for reasons such as freedom of speech and freedom of the media.[778]

The Queensland Office of the Information Commissioner considered that an appropriate balance must be struck with other competing rights and interests, including freedom of expression and the freedom to seek and receive information as defined in other human rights instruments.[779] Nine submitted that defamation laws currently provide remedy for false or damaging published materials and that there is a public interest in maintaining and making available an accurate historical record.[780]

While overseas data protection laws typically contain exceptions for legally enshrined rights such as freedom of expression and freedom of information,[781] Australian law only recognises the freedom of political communication as a constraint on legislative and executive power.[782] Therefore, a possible erasure exception for personal information that may constitute an exercise of freedom of speech or

---

[774] Submissions to the Issues Paper: Data Republic, 14; Uniting Church of Australia, 5.
[775] Submission to the Issues Paper: Uniting Church of Australia, 5. See *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth)**.** An obligation to retain data under a mandatory retention scheme could be grounds to refuse erasure under a separate exception for an act or practice required by or under an Australian law.
[776] *Privacy Act* (n 2) sch 1 APP 12.3(i).
[777] Submission to the Issues Paper: Interactive Games and Entertainment Association, 17–18.
[778] Submissions to the Issues Paper: ABC, 6; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 8; Calabash Solutions, 9; Centre for Media Transition, University of Technology Sydney, 18–19; Cyber Security Cooperative Research Centre, 4, 10; Information Technology Industry Council, 2–3; Law Institute of Victoria, 11–12; Legal Aid Queensland, 13; Office of the Information Commissioner Queensland, 3–4; Privacy108, 14; SBS, 8. See also ALRC, *Serious Invasions of Privacy in the Digital Era* (Report No 123, June 2014) ('*ALRC Report 123*').
[779] Submission to the Issues Paper: Office of the Information Commissioner Queensland, 4.
[780] Submission to the Issues Paper: Nine, 8.
[781] See, eg, GDPR (n 26) art 17(3)(b); *CCPA* (n 27) § 1798.105(d).
[782] *Theophanous v Herald & Weekly Times Ltd* (1994) 182 CLR 104, 168; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 561.

freedom of expression could be modelled on the public interest test in the FOI Act, which seeks to balance competing interests in determining whether individuals should be granted access to government-held documents.[783]

An adapted exception for the purposes of an erasure request could consider whether 'erasure of the personal information in the circumstances would, on balance, be contrary to the public interest'.[784] Reconciling the competing interests of privacy, freedom of expression and the retention of information in the public interest would be determined on a case-by-case basis. Factors to provide guidance on determining what was in the public interest could include whether erasure or retention of personal information would:

- promote the objects of the Act
- inform the public, or enable debate on a matter of public importance
- constitute an unreasonable limitation on the expression of a legitimate view or opinion, or
- inhibit the handling of personal information for archival, research or statistical purposes, journalistic purposes; or for academic, artistic or literary expression in the public interest. [785]

A public interest test would require IC determinations and the development of case law to further clarify the circumstances in which it would be in the public interest to reject an erasure request. Commissioner-issued guidance could also provide clarity for APP entities.

Personal information in a generally available publication and search results

Given that some individuals wishing to make erasure requests are likely to be concerned about publicly available personal information, the Review is also considering whether such a right should apply to the de-indexing of search results on a search engine, to the extent that the construction of a search index involves a collection of personal information.

Existing APPs that afford individuals with rights in relation to their personal information only apply in relation to personal information that is 'held' by an APP entity.[786] An APP entity 'holds' personal information where it has possession or control of a 'record', which is defined to exclude generally available publications.[787] If personal information in a generally available publication is not considered to be 'held' by an entity, it may limit the ability of individuals to request erasure of search results or other personal information published online. This issue is also relevant in the context of correction rights under APP 13 (see Chapter 18).

This broader concept of a right to be forgotten is recognised in the EU and can require search engines to de-index results that may appear from a search of a particular individual's name, where the indexed links are 'inadequate, irrelevant or no longer relevant, or excessive'.[788] The right is not absolute and must be balanced with other recognised European human rights, including the freedom of expression and the interest of the public in having the information.[789]

Google's submission, while supportive of a limited right to erase data that is provided to an organisation by product or service users, sought to distinguish this from requests to de-index or

---

[783] See *Freedom of Information Act* (n 360) sub-ss 11A(5), 11B(3).
[784] See ibid sub-s 11A(5).
[785] See ibid sub-s 11B(3); GDPR (n 26) arts 17(3)(d), 85, 89; *Data Protection Act 2018* (UK) (n 37) sch 2, pt 5, s 26.
[786] *Privacy Act* (n 2) sch 1 APPs 12.1, 13.1.
[787] *Privacy Act* (n 2) s 6.
[788] *Google Spain SL and Google Inc v Agencia Espanola de Proteccion de Datos*, Court of Justice of the European Union, Case C-131/12, 13 May 2014.
[789] Yann Padova, 'Is the right to be forgotten a universal, regional or 'global' right?' (2019) 9(1) *International Data Privacy Law* 15, 16; *Google Spain SL v Agencia Espanola de Proteccion de Datos*, Court of Justice of the European Union, Case C-131/12, 13 May 2014 [81].

delist search engine results.[790] Google considered that the balancing of individual privacy rights with the interests of other third party publishers is complex, and that the European right to be forgotten places these 'hard, important questions in the hands of a private tech company' with little in the way of guidance for decision-making.[791] Google also submitted that any public interest questions relating to the removal or delisting of search results should be made by an appropriate and independent judicial or regulatory authority.

Possible further exceptions

Submissions raised a number of other concerns regarding requests to erase personal information. These concerns could potentially be addressed through the following additional exceptions:

- where the personal information sought to be erased is contained in a Commonwealth record[792] – to ensure compliance by agencies with their record management obligations, including under the *Archives Act 1983* (Cth) (Archives Act)[793]
- where the entity is required to retain the information by or under an Australian law, or court/tribunal order[794] – to address concerns that retention may be required to comply with other legal requirements[795]
- where a request is 'frivolous or vexatious', consistent with APP 12[796]
- where erasure would have an unreasonable impact on the personal information of another individual – to address concerns that it may be inappropriate or impractical to erase joint personal information, such as phone call records or multiplayer video game history[797]
- where erasure would pose a serious threat to the life, health or safety of any individual, or to public health and safety[798]
- where personal information is required for the purposes of occupational medicine or for the management of health or social care systems or services – to address concerns that deletion of medical records should not be permitted[799]
- where the information is required for archival, research or statistical purposes in the public interest – to address concerns about information that is required for archival, research or statistical purposes, such as the maintenance of university registers of award qualifications and/or student misconduct, and[800]

---

[790] Submission to the Issues Paper: Google, 9.
[791] Ibid.
[792] Submissions to the Issues Paper: Australian Department of Health, 10; Office of the Information Commissioner Queensland, 3-4.
[793] See, eg, *Privacy Act* (n 2) sch 1 APP 11.2(c).
[794] See, eg, *Privacy Act* (n 2) sch 1 APP 11.2(d).
[795] Submissions to the Issues Paper: ANZ, 14; AusPayNet, 12; Australian Finance Industry Association, 5–6; Business Council of Australia, 5; Calabash Solutions, 9; Consumer Policy Research Centre, 9–10; Federal Chamber of Automotive Industries, 20; Information Technology Industry Council, 2–3; Legal Aid Queensland, 13; OAIC, 52, Office of the Information Commissioner Queensland, 3–4; SBS, 8.
[796] Submission to the Issues Paper: OAIC, 53.
[797] Submissions to the Issues Paper: AusPayNet, 12; BSA|The Software Alliance, 7; Interactive Games and Entertainment Association, 17–18; Law Council of Australia, 20–1; Law Institute of Victoria, 11–12; Optus, 11–12; Telstra Corporation Ltd and Telstra Health Pty Ltd , 10. See, eg, *Privacy Act* (n 2) sch 1 APP 12.3(b); Bill C-11 (n 394) sub-cl 55(1)(a).
[798] Submissions to the Issues Paper: Business Council of Australia, 5; Cyber Security Cooperative Research Centre, 4, 10; Deloitte, 27–9; Murdoch Children's Research Institute, 2. See, eg, *Privacy Act* (n 2) sch 1 APP 12.3(a); GDPR art 17(3)(c).
[799] Submissions to the Issues Paper: Avant Mutual, 13–14; Business Council of Australia, 5; Department of Health of Western Australia, 9; Ramsay Healthcare, 9. See, eg, GDPR art 17(3)(c).
[800] Submissions to the Issues Paper: Deloitte, 27–9; Griffith University, 15; Information Technology Industry Council, 2–3; James Scheibner (ETH Zurich) and Dianne Nicol (University of Tasmania), 5–6; Murdoch Children's Research Institute, 2; OAIC, 53; Office of the Information Commissioner Queensland, 3–4; Privacy108, 14. See, eg, GDPR art 17(3)(d).

- where the information relates to existing or anticipated legal proceedings between the entity and the individual – to address concerns information may be required for exercising or defending legal rights in future possible litigation.[801]

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.

Introduce a process for responding to erasure requests

The OAIC submitted that an APP entity should be required to respond to an erasure request within an appropriate time frame as is currently required in relation to access requests under APP 12.[802] The Review is seeking feedback on whether an entity should also be required to provide reasons for refusal if an exception applies, as is currently required under APP 12, unless unreasonable to do so.[803]

The Review is also considering the circumstances under which a child, parent or authorised guardian should be permitted to request erasure of a child's personal information. This is further explored in Chapter 13, which considers when an adult may lodge a request under the Act (including access and correction requests) on behalf of a child.

It was also submitted that if a distinction between data controllers and processors is introduced into the Act, the onus should be on the controller to receive and action deletion requests, and to ensure processors comply with the deletion request.[804] Optus submitted that entities should be able to transfer reasonable costs of actioning the request to the individual if it is overly complex.[805]

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?

[801] Submissions to the Issues Paper: AusPayNet, 12; Bennett + Co, 2; Business Council of Australia, 5.
[802] Submission to the Issues Paper: OAIC, 53. See *Privacy Act* (n 2) sch 1 APP 12.4.
[803] *Privacy Act* (n 2) sch 1 APP 12.9.
[804] Submissions to the Issues Paper: BSA|The Software Alliance, 7; Information Technology Industry Council, 2–3.
[805] Submission to the Issues Paper: Optus, 12.

16. Direct marketing, targeted advertising and profiling

The Issues Paper asked submitters to consider whether the Act strikes the right balance between the protection of privacy and the handling of personal information for the purpose of direct marketing, and whether protections for individuals could be improved.

The DPI report's recommendation 16(c) considered that 'real and informed consents should always be required where the consumer's personal information is used or disclosed for a purpose that is not in accordance with the consumer's own interests, such as where it is used or disclosed for targeted advertising purposes',[806] and that consumers who prefer to provide their personal information for targeted advertising purposes should be required to actively make this selection.[807]

What is direct marketing, targeted advertising and profiling?

Direct marketing is not defined in the Act. OAIC guidance states that it 'involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services'.[808] Direct marketing can include non-personal marketing communicated directly to an individual through the use of personal information such as their name and address.

The direct marketing of greatest concern to submitters was personalised targeted advertising, also known as behavioural advertising. Personalised targeted advertising is the displaying of online advertisements targeted to specific individuals based on their attributes, characteristics or interests, which are inferred from their previous web browsing activity or other data.[809] It is often reliant on an expansive range of technologies that track an individual's activities across the internet and on electronic devices, such as cookies, pixel tags, device/browser fingerprinting, mobile device tracking and cross-device tracking.[810]

Targeted advertising can also rely on the tracking of individuals' behaviour and activity in offline contexts. For example, personal information collected by IoT voice assistants, virtual reality and augmented reality tools is also increasingly being used for targeted advertising.[811] Targeted marketing which involves the use or disclosure of personal information about a reasonably identifiable individual is covered by the Act.[812]

Targeted advertising is often dependent on the use of a processing technique known as 'profiling'. The GDPR defines profiling as the processing of personal data to 'evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.[813] However, it is important to note that profiling is used for a wide range of purposes outside of advertising, including the personalisation of services, assessing eligibility for financial products or predicting the likelihood that certain medical treatments will be successful.[814]

Targeted advertising has become increasingly integral to business' marketing strategies in recent years as it allows businesses to direct their advertising at the consumers most likely to purchase their goods and services. The ACCC's *Digital Advertising Services Inquiry* interim report (Ad tech

[806] ACCC, DPI report (n 2) 465.
[807] Ibid 468.
[808] OAIC, APP Guidelines (n 21).
[809] ACCC, *Digital Advertising Services Inquiry* (Interim Report, December 2020) 50 ('*Adtech Inquiry Interim Report*').
[810] ACCC, DPI report (n 2) 130, 387–8; Brian Chen, 'Fingerprinting' to Track Us Online Is on the Rise: Here's What to Do', *New York Times* (online, 3 July 2019).
[811] ACCC, *Digital Platforms Services Inquiry* (Interim Report, September 2020) 88–9, 96–100.
[812] OAIC, APP Guidelines (n 21) 7.11.
[813] GDPR (n 26) art 4.
[814] See Submission to the Issues Paper: Financial Services Council, 5; UK ICO, *What is automated decision-making and profiling?* (Web Page, January 2021).

Inquiry interim report) noted that digital advertising expenditure in Australia reached $9.1 billion in the 2019-20 financial year.[815]

Customer loyalty schemes

Customer loyalty schemes collect information about members in order to generate consumer insights that are often used for targeted advertising.[816] Membership of a customer loyalty scheme is voluntary and generally provided at no monetary cost to the consumer. In exchange for participating in a customer loyalty scheme, members are offered benefits such as discounts, rewards and other promotions.[817]

Customer loyalty schemes collect information about members including their demographic data, transaction history, interests, preferences, consumption patterns, buying behaviours and habits.[818] In addition, loyalty schemes may purchase or gain access to datasets held by data brokers which can allow loyalty schemes to infer information about a member's lifestyle, interests and social attitudes.[819] Some schemes generate additional revenue by selling de-identified insight reports to third parties and by advertising to members on behalf of third parties.[820]

In its *Customer Loyalty Schemes* report, the ACCC expressed concern about customer loyalty schemes collecting, using and disclosing information in ways that do not meet the expectations of consumers, including by seeking broad consents from consumers, making vague disclosures to consumers about the collection, use and disclosure of their information, providing consumers with limited insight and control over the sharing of their information with unknown third parties and providing a limited ability for consumers to opt out of targeted advertising delivered by third parties.[821] Submitters to the Issues Paper expressed similar concerns,[822] noting that consumers do not have the option to decline the collection or use of their personal information where it is not necessary for the provision of the customer loyalty scheme.[823]

Some submitters were particularly concerned with a practice identified in the ACCC report in which customer loyalty schemes continued to track the purchasing behaviour and transaction activities of members even if they did not scan their loyalty card, by automatically linking any payment card used by the member to their profile.[824] By linking payment cards to a member's profile, a customer loyalty scheme could collect, use and disclose the same information as if the member had actively used their loyalty card – without the need to compensate the member with the usual reward.[825] Dr Katherine Kemp's submission noted that a member of a customer loyalty scheme may believe they have avoided tracking by choosing not to use their loyalty card, unaware that they are tracked through their payment cards.[826] The ACCC recommended that customer loyalty schemes should end the practice of automatically linking members' payment cards to their loyalty scheme profile,[827] and Salinger Privacy suggested this type of tracking should be strictly prohibited.[828]

---

[815] ACCC, *Adtech Inquiry Interim Report* (n 809) 9.
[816] ACCC, *Customer Loyalty Schemes* (Final Report, December 2019) 45.
[817] Ibid 47.
[818] Ibid 45-47.
[819] Ibid 48-52.
[820] Ibid 45.
[821] Ibid 82.
[822] Submissions to the Issues Paper: Dr Katherine Kemp, 17-18; Salinger Privacy, 27; Allens Hub for Technology, Law and Innovation, 6-7.
[823] Submissions to the Issues Paper: Dr Katherine Kemp, 17-18; Allens Hub for Technology, Law and Innovation, 6-7.
[824] ACCC, *Customer Loyalty Schemes* (n 816) 65; Submissions to the Issues Paper: Dr Katherine Kemp, 19; Salinger Privacy, 27.
[825] ACCC, *Customer Loyalty Schemes* (n 816) 65
[826] Submission to the Issues Paper: Dr Katherine Kemp, 19.
[827] ACCC, *Customer Loyalty Schemes* (n 816) 67.
[828] Submission to the Issues Paper: Salinger Privacy, 27.

While the ACCC noted in its *Customer Loyalty Schemes* report that a number of schemes had either made, or committed to make, improvements to their information handling practices during the course of the ACCC's review, it expressed concerns about loyalty schemes collecting, using and disclosing personal information in ways that did not meet the expectations of consumers.[829]

Regulation of direct marketing, targeted advertising and profiling

The Act currently specifically regulates organisations' use and disclosure of personal information for the purpose of direct marketing under APP 7. APP 7 prohibits organisations from using or disclosing personal information for the purpose of direct marketing unless the organisation collected the information from the individual and the individual would reasonably expect their personal information to be used or disclosed for that purpose.[830] If an individual would not reasonably expect the use or disclosure of their personal information for direct marketing, or the personal information was collected from a third party, consent must be obtained unless impracticable to do so.[831] Organisations may not use or disclose sensitive information for the purpose of direct marketing unless the individual has provided consent.[832]

The consent requirements in APP 7 depend on whether or not the organisation has collected the personal information directly from the individual. This reflects the intent that more stringent obligations should apply to organisations using the personal information of individuals who are not existing customers.[833] In all cases, the organisation must provide a simple means by which the individual may easily request not to receive direct marketing communications from the organisation.

APP 7 does not apply to the extent that the *Spam Act* or *DNCR Act* apply.[834] The OAIC noted that in practice, APP 7 therefore generally only applies to:[835]

- direct marketing calls or faxes where the number is not listed on the Do Not Call Register, or the call is made by a registered charity
- direct marketing by mail and door-to-door direct marketing, and
- online marketing (including on websites and mobile apps) which involve the use or disclosure of personal information about a reasonably identifiable individual to target that marketing.[836]

Issues identified with the regulation of direct marketing

Privacy risks and potential harms

Submissions raised concerns about the adequacy of the current regulation of direct marketing in the Act, in light of the privacy risks to individuals as a result of profiling and targeted marketing. The UK ICO's 'Update Report into Ad tech and Real Time Bidding' (RTB report) highlighted that 'the creation of detailed profiles, which are repeatedly augmented with information about actions that individuals take on the web, is disproportionate, intrusive and unfair in the context of the processing of personal data for the purposes of delivering targeted advertising'.[837]

---

[829] ACCC, *Customer Loyalty Schemes* (n 816) 84.
[830] *Privacy Act* (n 2) sch 1 APP 7.2.
[831] Ibid sch 1 APP 7.3.
[832] Ibid sch 1 APP 7.4.
[833] Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012 (n 139) 81.
[834] *Privacy Act* (n 2) sch 1 APP 7.8.
[835] Submission to the Issues Paper: OAIC, 45.
[836] OAIC, APP Guidelines (n 21) [7.9]–[7.12]. The APP Guidelines state that direct marketing may include 'displaying an advertisement on a social media site that an individual is logged into, using personal information, including data collected by cookies relating to websites the individual has viewed.'
[837] UK ICO, Update Report into Adtech and Real Time Bidding (Report, 20 June 2019) 20 ('RTB Report').

Dr Kemp's submission cited the RTB report finding that, 'the transfer of consumer's personal data to numerous third parties in the ad tech supply chain gives rise to a very significant risk that the data will be improperly stored and used, particularly since the original collector of the data no longer has control over it'.[838] Salinger Privacy's submission cited the Norwegian Consumer Council's study of ten popular mobile applications, including dating apps and menstrual cycle trackers, which were found to transmit data to at least 135 different third parties for targeted advertising.[839]

Submissions cited other potential harms including targeting of inappropriate content at children,[840] profiling of political views to enable misinformation to be directed at vulnerable individuals,[841] and predictions about product eligibility based on socioeconomic status.[842] The Ad tech Inquiry interim report highlighted heightened risks as a result of the increased reliance that consumers have placed on digital markets due to the COVID-19 pandemic.[843] The ACCC has noted a steady increase in scams involving online private messaging, social media and search services.[844] From 2018 to 2019, the number of complaints increased by almost 32%, with $38.5 million of losses being reported in 2019, compared to $23.5 million in 2018.[845]

Lack of transparency

Submissions expressed concern about a lack of transparency in relation to profiling and targeted advertising.[846] Dr Kemp's submission stated that:

> *Firms often claim consumers have received notice of the use of their data for additional purposes relating to marketing or commercial data sharing arrangements on the basis of vague, open-ended terms in privacy policies. The relevant terms are commonly phrased in a way that consumers cannot determine the actual use of the personal data and the entities to whom that data will be disclosed*.[847]

Oracle noted that Google's privacy policy uses a wide definition of 'services' that includes advertising technology services.[848] The DPI report noted that privacy policies reviewed for that report tended to describe online tracking technologies as being used for product improvement or user convenience rather than for advertising purposes.[849] The RTB report also highlighted a lack of transparency in the ad tech industry in its conclusion that 'the profiles created about individuals are extremely detailed and are repeatedly shared among hundreds of organisations for any one bid request, all without the individuals' knowledge'.[850]

Concerns about validity of consent

Dr Kemp further considered that consumers' consent to the use of their personal information for marketing purposes should not be regarded as voluntary where the consent sought is expressed in broad terms and is bundled with the primary purposes for personal information handling. These

---

[838] Submission to the Issues Paper: Dr Katharine Kemp, 12.
[839] Submission to the Issues Paper: Salinger Privacy, 30.
[840] Submission to the Issues Paper: Reset Australia, 7–8.
[841] Submissions to the Issues Paper: Salinger Privacy, 30–2; Digital Rights Watch, 6.
[842] Submission to the Issues Paper: Consumer Policy Research Centre, 30 (Attachment 1). See also ACCC, ACCC, *Adtech Inquiry Interim Report* (n 809) 78-79.
[843] ACCC, *Adtech Inquiry Interim Report* (n 809) 79 citing Consumer Policy Research Centre: 'Unfair trading practices in digital markets – evidence and regulatory gaps', *Research and policy briefing*, December 2020.
[844] ACCC, *Adtech Inquiry Interim Report* (n 809) 56.
[845] Ibid.
[846] Submission to the Issues Paper: Guardian Australia, 3; CAIDE and MLS, 3; Humanising Machine Intelligence Project, Australian National University, 2; Legal Aid Queensland, 12; Obesity Policy Coalition, 2-3; Salinger Privacy, 16–18; Dr Katharine Kemp, 6.
[847] Submission to the Issues Paper: Dr Katharine Kemp, 12.
[848] Submission to the Issues Paper: Oracle, 5–6.
[849] ACCC, DPI report (n 2) 412.
[850] UK ICO, RTB Report (n 837) 23.

consents were then said to 'snowball as third parties in the ad tech supply chain in turn rely on these broad permissions as consent for their own data practices.[851] The Ad tech Inquiry interim report noted that only seven per cent of those surveyed in Deloitte's 2020 Australian Privacy Index stated that they had a 'very good understanding' of how their personal information is used after they provide consent.[852]

Such concerns are exacerbated by market practices referred to as 'dark patterns' that use design features to 'deceive, steer or manipulate users' into behaviour that is contrary to their intentions, such as an intentionally complicated unsubscribe mechanism.[853] In this regard, the Review notes that the Austrian Data Protection Authority is currently reviewing a complaint regarding the validity of user consent to tracking by Google's Android Advertising ID.[854]

Individuals' ability to exercise control

Submissions also raised concerns about individuals' inability to exercise control in relation to the collection, use and disclosure of their information for direct marketing. Despite the requirement for organisations to provide individuals with a simple means to request not to receive marketing communications, submissions indicated that opting out currently requires complex, time-consuming and repeated actions on the part of the consumer which cannot guarantee a complete avoidance of tracking for marketing purposes.[855] This submitter feedback aligned with the DPI report finding that most digital platforms do not enable a user to opt-out of targeted marketing entirely.[856]

Submitters also highlighted that APP 7 does not regulate the *collection* of personal information for direct marketing purposes and therefore does not permit an individual to opt out of having their online behaviour tracked and personal information collected for direct marketing purposes. Instead, it is limited to opting out of *receiving* marketing communications.[857] There is also no requirement in APP 7 to permit individuals to opt-out of their personal information being used or disclosed for direct marketing purposes.[858]

Coverage of the Act

Some submissions were concerned that many forms of profiling and behavioural advertising are not clearly covered by the Act[859] due to the increasing use of technical information as a replacement for traditional identifiers such as names.[860] Profiling for targeted advertising is often reliant on the collection and aggregation of non-personal technical information that can be combined to identify individuals with a high degree of accuracy. For example, the Ad tech Inquiry interim report cited findings that between 61 and 87 per cent of individuals in the United States were able to be identified by a combination of ZIP code, birth date and gender.[861]

---

[851] Submission to the Issues Review: Dr Katharine Kemp, 16.
[852] ACCC, *Adtech Inquiry Interim Report* (n 809) 52 citing Deloitte, Australian Privacy Index 2020 (Report, 2020) 7.
[853] Federal Trade Commission, *Statement of Commissioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning, Inc Commission File Number 1723186* (Web Page, 2 September 2020) 1.
[854] ACCC, *Adtech Inquiry Interim Report* (n 809) 53.
[855] Submissions to the Issues Paper: Dr Katharine Kemp, 19; Legal Aid Queensland, 12; Privacy108, 12.
[856] ACCC, DPI report (n 2) 426–8. See also Norwegian Consumer Council, 'Out of Control: How Consumers are Exploited by the Online Advertising Industry' (Report, 14 January 2020) 69, 179.
[857] Submissions to the Issues Paper: Dr Katharine Kemp, 18; Association for Data-Driven Marketing and Advertising, 19; Salinger Privacy, 29–31.
[858] Submission to the Issues Paper: OAIC, 46.
[859] Submissions to the Issues Paper: Financial Services Council, 7; Salinger Privacy, 4; Obesity Policy Coalition, 4; Dr Katharine Kemp, 7.
[860] Submission to the Issues Paper: OAIC, 29; Dr Katharine Kemp, 8.
[861] ACCC, DPI report (n 2) 49.

Benefits of direct marketing

A number of submissions noted that profiling and targeted advertising can have a positive impact on the digital economy, drive the success of online businesses and enable the personalisation of services. Facebook submitted that users prefer personalised advertising to non-targeted advertising - citing research finding that individuals would rather receive behavioural targeted advertisements that are relevant than randomised irrelevant advertisements.[862] Submissions also considered that targeted advertising enables the provision of free digital services, has reduced the cost of advertising for small to medium sized businesses and provides economic benefits to the Australian economy.[863] DIGI submitted that profiling and advertising helps to maintain a free and open advertisement-supported internet.[864]

Proponents of more explicit regulation of profiling and advertising indicated the importance of distinguishing between desirable and undesirable forms of profiling and behavioural advertising.[865] Salinger Privacy's submission referred to a need to distinguish between intrusive, covert tracking and an entity sending marketing materials to an existing customer base.[866] ADMA's submission indicated that any reform should not diminish an entity's ability to engage in responsible targeted marketing which is reasonably expected and understood by the individual,[867] and that 'the desire to protect individuals from bad actors must not have the end result of closing off the responsible use of technological innovation and data from the APP entities that do value trust in their relationship with their customer'.[868]

OP Bill and direct marketing

The OP Bill, through the OP code, will address some of the privacy issues which have been identified in relation to direct marketing and particularly targeted advertising. The OP code will strengthen existing notice and consent requirements and introduce new requirements on organisations subject to the OP code. The OP code will require organisations subject to the code to notify individuals, or to otherwise ensure they are aware, of the purposes for which information is collected, used and disclosed in a clear and understandable, current and timely manner. It will also require consent to be voluntary, informed, unambiguous, specific and current. Organisations subject to the code will also be required to take reasonable steps not to use or disclose personal information if requested by an individual.

Interaction between APP 7 and other Commonwealth legislation

Submitters raised concerns that the regulatory framework for direct marketing which spans APP 7, the *Spam Act* and the *DNCR Act*, establishes different obligations for different marketing channels, which creates regulatory fragmentation and confusion for consumers and industry.[869] ACMA highlighted that this confusion has been compounded by the convergence of communications channels, which has led to the blurring of traditional business marketing models across platforms.[870] ACMA noted 'strong drivers' for the existing rules in the *DNCR Act*, *Spam Act* and related powers and functions in the Telecommunications Act 1979 (Tel Act) to be consolidated and harmonised to align with the consent arrangements in the Act.[871]

---

[862] Submission to the Issues Paper: Facebook, 19.
[863] Submissions to the Issues Paper: DIGI, 9.
[864] Submission to the Issues Paper: DIGI, 9.
[865] Submissions to the Issues Paper: Salinger Privacy, 30–1; Privacy108, 12; Guardian Australia, 16.
[866] Submission to the Issues Paper: Salinger Privacy, 30–1.
[867] Submission to the Issues Paper: Association for Data-Driven Marketing and Advertising, 18.
[868] Ibid 19.
[869] Submissions to the Issues Paper: OAIC, 45; Australian Communications and Media Authority, 5; Gadens, 8.
[870] Submission to the Issues Paper: Australian Communications and Media Authority, 5.
[871] Ibid.

International approaches to direct marketing, targeted advertising and profiling

In contrast to Australia, overseas jurisdictions have introduced more explicit regulation of profiling and behavioural advertising.

The GDPR expressly defines 'profiling' and subjects it to additional protections including notification requirements, a right of access, a right to object and rights not to be subject to decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects.[872] The EU's ePrivacy Directive (ePD) further regulates the use of online tracking devices, such as cookies, by requiring that entities obtain consent prior to their use and provides capacity to withdraw consent at all times.[873]

Canada's proposed Bill C-11 would have required entities to obtain consent where personal information would be used for 'the purpose of influencing the individual's behaviour or decisions'.[874] California's CPRA also defines profiling and mandates that individuals be able to opt-out of the sharing and sale of their personal information.[875] The CRPA also indicates that subsequent regulation will be considered to further address automated decision-making, including profiling.[876]

Proposals

APP 7 was introduced in 2012 'because of the significant community interest about the use and disclosure of personal information for the purposes of direct marketing',[877] with the intent of 'more tightly regulat[ing] the use of personal information for direct marketing'.[878] The 2021 Deloitte Australian Privacy Index indicates that 74 per cent of consumers have concerns about the use of internet cookies to track their activity online to market to them and 85 per cent are concerned that brands sell information gathered by internet cookies to other companies.[879] 65 per cent of respondents were unhappy about receiving targeted advertising based on their online activity.[880]

In light of the privacy risks associated with tracking and profiling for the purpose of targeted advertising and the issues identified with the current effectiveness of the Act in regulating direct marketing, reforms are necessary to empower consumers and enhance individuals' trust that their privacy is being respected and protected. Importantly, the proposals being considered seek to distinguish between fair and reasonable direct marketing by organisations to existing clients as compared with intrusive direct marketing practices which lack transparency and to which more stringent obligations should apply.

Increase transparency and control over collection, use and disclosure for direct marketing

Submissions that called for greater transparency around personal information handling for direct marketing purposes proposed that entities should be required to provide notice when seeking to use personal information for profiling and targeted advertising.[881]

---

[872] See, GDPR (n 26) arts 4, 13, 14, 15, 21, 22.
[873] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)* [2002] OJ L 201/37 ('*ePrivacy Directive*').
[874] Bill C-11 (n 394) sub-cl 18(1).
[875] CPRA (n 120) 1798.140(1)(K). The CPRA will come into effect in 2023.
[876] Ibid 1798.185(a)(16).
[877] Submission to the Issues Paper: OAIC, 45. See also Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012 (n 139) 81.
[878] Commonwealth of Australia, *Parliamentary Debates*, House of Representatives, 23 May 2012, 5210 (Nicola Roxon MP).
[879] Deloitte, Australian Privacy Index 2021 (Report, 2021) 7, 17.
[880] Ibid 17.
[881] Submissions to the Issues Paper: Oracle, 12–13; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 18–19; Privacy108, 8; Consumer Policy Research Centre, 5–6; Dr Katharine Kemp, 12–15, 19–20; Obesity Policy Coalition, 5.

Under APP 5, an APP entity must take such steps (if any) as are reasonable in the circumstances to notify a person about the purpose(s) for which the entity is collecting and may use or disclose the information. Where personal information is collected by an entity for direct marketing as a primary purpose, the proposals in Chapter 8 to strengthen the Act's notice mechanisms would apply. That proposal would require APP entities to provide clear, current and understandable notice when collecting personal information, including for direct marketing purposes.

Where an organisation wishes to use information it already holds about an individual for direct marketing purposes, APP 7 requires that it obtain the individual's consent where the individual would not reasonably expect their personal information to be used for direct marketing or where it has been collected from a third party. However, APP 7 does not expressly require an individual to be notified of the matters set out in APP 5. Therefore it is not clear that an individual whose personal information is to be used or disclosed for marketing purposes will have received an APP 5 collection notice. While the process of obtaining consent may result in the individual becoming aware of the use or disclosure of their personal information for the purpose of direct marketing, in light of the concerns about informed consent set out in Chapter 9 and in Dr Kemp's submission specifically in the marketing context, this will not always be the case. Additionally, as APP 7 contains an exception for obtaining consent if it is impracticable to do so, consent may not be obtained in any case.[882]

Some submissions proposed that profiling and targeted advertising should require express consent in line with recommendation 16(c) in the DPI report.[883] ACMA's submission called for a universal consent-based framework, with consistent consent protections across all relevant marketing channels under which marketing contact could only occur where either consumer consent has first been obtained, or where a public interest exception is applicable.[884]

As detailed in Chapter 9, there are risks of consent fatigue and reduced effectiveness of consent if individuals are required to positively opt in to their information being collected through tracking technology, that is then used and disclosed to show them targeted advertising, on each website they visit. Europe's ePD requires websites to obtain explicit consent to the use of tracking devices, such as cookies.[885] Public consultations and reviews into the effectiveness of the ePD have found that users are overwhelmed by consent requests and in practice are not being protected against unsolicited marketing.[886] Consequently, the European Data Protection Board has called for reforms under the ePrivacy Regulation to explicitly address the issue of consent fatigue.[887]

Proposal – unqualified right to object to collection, use and disclosure for direct marketing

In light of the concerns regarding a lack of transparency and limits to the effectiveness of express consent, the current limited right to opt out of receiving direct marketing communications could be replaced with an unqualified right to object to the collection, use and disclosure of personal information for the purposes of direct marketing. This right would differ from the general right to object proposed in Chapter 14 as entities would need to stop, not just 'reasonable steps' to stop, the collection, use or disclosure of personal information for direct marketing purposes.

---

[882] *Privacy Act* (n 2) sch 1 APP 7.3(b)(ii).

[883] Submissions to the Issues Paper: Dr Katharine Kemp, 19–20; Shaun Chung and Rohan Shukla, 15; CAIDE and MLS, 7–8; Oracle, 11–14.

[884] Submission to the Issues Paper: Australian Communications and Media Authority, 6. The submission noted that the 'framing of consent under the European Union's General Data Protection Regulation (GDPR) may provide insights for a new Australian framework for consent'.

[885] *ePrivacy Directive* (n 873).

[886] European Commission, *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation* (Final Report, 31 January 2015) 12; European Commission, *Synopsis Report of the Public Consultation on the Evaluation and Review of the ePrivacy Directive* (Synopsis Report, 19 December 2016) 2.

[887] European Data Protection Board, *Statement 03/2021 on the ePrivacy Regulation* (adopted on 9 March 2021) 3.

As discussed in Chapter 14, if as a result of exercising this right, an entity determines that they are unable to offer or provide the individual with a product or service, the entity will need to demonstrate that the collection, use or disclosure is fair and reasonable. Importantly, this attracts consideration of whether the collection, use or disclosure was reasonably necessary to achieve the entity's functions.

The DPI report recommended that a digital platforms code should provide individuals with the ability to select global opt-outs or opt-ins, for the collection of personal information for online profiling purposes or sharing of personal information with third parties for targeted advertising purposes.[888] The ACCC noted that the 'ability of consumers to globally opt-in, stay opted-out, or make an intermediate decision could provide a useful way to minimise consent fatigue, by allowing consumers to select their preferred level of data collection as quickly as possible.'[889]

ACMA also proposed that all entities be required to provide a 'direct and one-step "unsubscribe" or "opt-out" functionality – regardless of the size of the entity, marketing channel used or whether the entity is otherwise exempt'.[890] It considered that 'this would preserve the public interest in the case of first marketing contacts from all entities but would give consumers additional agency to prevent further contact'.[891] Salinger Privacy submitted that similar to the 'unsubscribe' link on an email newsletter, online behavioural advertising (as opposed to contextual advertising) should be clearly identified to the user as an ad or message shown to the user, along with a mechanism allowing the easy opt out of all future direct marketing, messaging, profiling, targeting or tracking.[892]

The Review is seeking feedback on the practicalities of requiring a global opt-out mechanism, which could enable individuals to opt-out of tracking for the purposes of direct marketing. For tracking that occurs online this could be at a device or web browser level. These more prescriptive requirements could be considered through the development of the OP code or a future APP code. While the ACCC considered that such a mechanism could reduce consent fatigue, a standardised or global opt-out process could also make opting-out more accessible for individuals.

Proposal – influencing an individual's behaviour or decisions must be a primary purpose

Additional reforms could also increase the transparency of the collection, use and disclosure of information for direct marketing purposes. The Review is seeking feedback on whether the Act should require that the collection, use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to an individual at the point of collection. This purpose would encompass not only the collection, use and disclosure of personal information for targeted advertising to consumers of goods and services, but also the use of profiling to target individuals with ideological or political messaging, as outlined in greater detail in Chapter 6.[893]

An entity would therefore only be permitted to undertake direct marketing where it was the purpose for the original collection, as notified to the individual (see Proposal 10.4). This would address concerns about the prevalence of third parties collecting, using and disclosing personal information in the process of delivering targeted advertising to individuals without their knowledge. It is also intended to support the effectiveness of the proposed unqualified right to object to direct

[888] ACCC, DPI report (n 2) Recommendation 18. See also, recommendation 16(c) that any settings for data practices relying on consent should be pre-selected to 'off'.
[889] Ibid 490.
[890] Submission to the Issues Paper: Australian Communications and Media Authority, 6.
[891] Ibid.
[892] Submission to the Issues Paper: Salinger Privacy, 32.
[893] This wording borrows from s 18 of Canada's Bill C-11 (n 394) which would have required an entity to obtain consent for personal information collected or used for the purpose of influencing an individual's behaviour or decisions.

marketing, as individuals' awareness of the use or disclosure of their information for direct marketing is necessary to be able to exercise the right to object.

This proposal would not likely impose an additional compliance burden on organisations that wish to market to existing clients, because this purpose can be included in the notice which is provided when customers' information is collected for the purpose of completing the transaction. For organisations that collect personal information from third parties, this proposal would require collection notices to be issued in line with the strengthened notice requirements as set out in Chapter 8. While this proposal is intended to increase individuals' awareness of information handling which is occurring for the purpose of influencing their behaviour or decisions, the Review is conscious of the possibility of notice fatigue, and so is seeking feedback on its feasibility and potential impacts.

Proposal – enhance information on direct marketing in APP privacy policy

To further enhance awareness and understanding about the use of personal information for direct marketing, the Act could be amended so that an APP Privacy Policy must include the following information:

- whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing the individual's behaviour or decisions and if so, the types of personal information that will be used, generated or inferred (and any other type of information used) to influence the individual's behaviour or decisions, and
- whether the entity uses third parties to provide online marketing materials and if so, the details of those parties and information regarding the appropriate method of opting-out of those materials.

This recognises that the ecosystem of advertising has transformed into a multi-party system where it is often unclear to the individual who is responsible for the provision of marketing materials. Providing individuals with this information in the privacy policy will ensure that individuals have tangible information on how to exercise rights to object to direct marketing.

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.

Remove APP 7 in light of other proposals for reform

Two submissions considered that APP 7 is no longer fit for purpose and should be repealed.[894] Instead, it was proposed that direct marketing could be regulated under the remaining APPs with general application in light of other proposals for reform. Other submitters considered that APP 7 remains largely fit for purpose,[895] and argued that the brand and reputational damage that entities may incur when engaging in inappropriate direct marketing acts as a check on APP entity conduct.[896]

Removing APP 7 would recognise that its requirements would be largely replicated or strengthened through other proposals of this Review. In particular:

- Proposal 16.1 to introduce an unqualified right to object to the collection, use or disclosure of personal information for the purpose of direct marketing would apply in place of the current requirement in APP 7 to provide a simple means by which individuals may easily request not to receive direct marketing communications.
- Proposals 16.2 and 16.3 suggest that the use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose. This would require APP entities to notify individuals of that purpose on collection of their information (see Proposal 10.4), along with providing additional information in the privacy policy.

  This would apply in place of the current requirement in APP 7 which requires organisations to obtain consent to the use or disclosure of personal information for marketing purposes unless:

  - the organisation collected it from the individual and the individual would reasonably expect the organisation to use or disclose their information for that purpose, or
  - it is impracticable to obtain consent where the individual would not reasonably expect their information to be used for that purpose or the organisation collected the personal information from someone than the individual.
- Proposal 18.1 to require APP entities that have collected personal information about an individual indirectly to identify the source from which it was collected on request from the individual. This would apply in place of the current requirement in APP 7 that organisations must respond to an individuals' request to provide its source of personal information unless impracticable or unreasonable to do so.

In addition, the following proposals would address other issues which submitters have identified with the regulation of direct marketing.

- Proposal 2.1 to amend the definition of personal information to include a greater range of information and Proposal 2.2 to provide a non-exhaustive list of the types of information capable of constituting personal information – would address concerns that some targeted advertising may fall outside the scope of the Act due to the use of technical identifiers and data to explicitly target an unidentified individual's personal preferences with a high degree of accuracy.
- Proposal 2.4 to amend the definition of 'collection' to provide clarity that inferred personal information is covered by the Act – would address concerns that profiling which infers personal information may not be covered by the Act. It would ensure that where profiling

[894] Submissions to the Issues Paper: OAIC, 45; Salinger Privacy, 31.
[895] Submissions to the Issues Paper: Gadens, 7; Nine, 7. KPMG, 17.
[896] Submission to the Issues Paper: KPMG, 17.

results in inferred sensitive information, consent to that collection of sensitive information is required.

- Proposal 9.1 to require that consent must be voluntary, informed, current, specific, and an unambiguous indication through clear action – would address concerns that entities do not obtain meaningful consent for intrusive or unnecessary profiling and ensure that there is greater transparency around the individual practices to which individuals are consenting.
- Proposal 10.3 to require entities to take reasonable steps to ensure that indirect collections were originally collected from the individual in accordance with APP 3 – would address concerns about the prevalence of personal information that is sold or shared by third parties and aggregated to create digital profiles of individuals without an individual's knowledge or, when required, consent.
- Proposals 8.1, 8.2 and 8.3 to strengthen notice requirements – would, as indicated above, address concerns that individuals are unable to make informed decisions about their personal information as broad descriptions are used to describe the purpose of collecting personal information which does not explicitly disclose the extent of use for marketing, re-sale and profiling purposes.
- Proposals 10.1 and 10.2 that all collections, uses and disclosure must be fair and reasonable and for personal information that relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child – would address concerns about unfair and unreasonably intrusive collections, uses and disclosures of personal information for direct marketing purposes and the specific harmful nature of targeted advertising that is directed at children[897].
- Proposal 11.1 to introduce requirements in relation to restricted acts and practices and to potentially prohibit certain acts and practices – would address concerns about the most harmful forms of targeted advertising by heightening accountability obligations for entities who seek to undertake potentially risky activities with individuals personal information, and

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

Case study
A social network allows users to sign up by providing their email address, name, age, gender and address. Users of the network are able to connect with others, as well as join groups and forums based on their personal interests.

The network collects information about users based on their activity on the network as well as their browsing activity on third party websites which have implemented the network's advertising tracking technologies. The network also infers predicted interests and attributes of users through their activities on the network and browsing activity on third party websites. The network uses this information to create profiles attached to pseudonymised numerical identifiers. As a result, the network does not consider the profiles to be about reasonably identifiable individuals.

The social network uses the profiles to match advertising supplied by third parties to users who are likely to be interested in the subject matter of the advertising. For example, a political advertiser wishes to target its advertising to users based on their socioeconomic status, inferred religious beliefs and stances on certain social causes.

[897] See also the OP code requirements in relation to social media services in the OP Bill (n 1).

Impact of the proposals
As the profiles attached to pseudonymised identifiers contain a large amount of information allowing the network to target users with a high degree of accuracy, it is information that relates to a reasonably identifiable individual and would be covered by the Act. Where the network infers personal information about a user, this would be defined as a 'collection' under the Act, and any inferred sensitive information would require consent. Consent would need to be voluntary, informed, current, specific, and an unambiguous indication through clear action. Overall the network's collection, use and disclosure of personal information would need to be fair and reasonable in the circumstances.

The social network would be required to provide users with notice that is clear, current and understandable. As the network uses personal information for the purpose of influencing users' behaviour or decision through targeted advertising it would be required to specifically state that this is a primary purpose for collection in its notices. Notices would also need to provide information on a user's right to object to the collection, use or disclosure of their personal information. In particular, the network must provide users with an unqualified right to object to the collection, use or disclosure of their personal information for the purpose of direct marketing.

As the network is engaging in the large scale collection, use and disclosure of personal information for the purpose of direct marketing it would be required to take adequate steps to identify risks to privacy and implement measures to address the risks, which would likely require the network to undertake a privacy impact assessment. The network would also be required to include detail in its privacy policy about the types of personal information it uses to influence individuals' behaviour or decisions and any third parties that it engages with in the course of direct marketing.

Questions

- Should express consent be required for any collection, use or disclosure of personal information for the purpose of direct marketing?
- What are some of the practical challenges of implementing a global opt-out process, to enable individuals to opt out of all online tracking in one click?
- What are the potential impacts of requiring that a use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions be a primary purpose to be notified to the individual when their personal information is collected?
- Is there any benefit in regulating direct marketing through a separate privacy principle or should APP 7 be removed in light of other proposals for reform?
- Should the unqualified right to object to marketing extend to the collection and use of personal information where it is aggregated with the personal information of other users for marketing targeted at cohorts rather than individuals?
- Do customer loyalty schemes offer more tangible benefits to consumers, and should they be regulated differently to other forms of direct marketing?

17. Automated decision-making

The Act does not expressly regulate the use of personal information by automated decision-making (ADM) systems or otherwise regulate ADM. While not specifically raised in the Issues Paper, several submissions commented on the use of personal information in ADM systems and the privacy implications of ADM for individuals.[898]

What is automated decision-making?

ADM is the process of making a decision without human involvement.[899] Automated decisions can be based on factual data, as well as digitally created profiles or inferred data. ADM systems can rely on artificial intelligence (AI) to assist or replace the judgement of human decision-makers.[900] ADM systems range from systems that apply simple business rules to those that use sophisticated algorithms to make discretionary decisions.[901] Replacing human decision-makers with ADM systems offers the potential to increase the efficiency, accuracy and consistency of decisions, but these systems also raise complex ethical and legal issues.[902]f

The AHRC recently released its *Human Rights and Technology* Final Report (AHRC report) which explores these issues and 'provides a roadmap for how Australia should protect and promote human rights in a time of unprecedented change in how we develop and use new technologies'.[903] The AHRC report makes a number of recommendations on how Australia should regulate AI and other emerging technologies which can be used to make automated decisions.[904]

Impact on privacy

The use of AI is becoming increasingly common across government agencies and the private sector,[905] with levels of automation being provided for in a variety of Commonwealth legislation.[906] The OAIC's submission to the AHRC *Human Rights and Technology* Issues Paper stated that the increase in the use of AI is 'supported by a fundamental shift in analytical processes, together with the availability of large data sets, increased computational power and storage capacity'. The submission noted that although AI has 'the potential to yield great benefits, including in predictive capabilities' it can also have 'significant impacts on privacy'.[907] These impacts include the collation of data, including from third parties, generating inferred personal information and inferential decision-making based on data which may not be accurate.[908]

A small number of submissions to the Review raised concerns about the lack of transparency associated with automated decisions[909] and the risk that individuals will be subject to unfair treatment or unlawful discrimination as a result of ADM systems.[910] For example, Shaun Chung and

---

[898] Submissions to the Issues Paper: The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 2–3, 7–8; Australian Information Security Association, 6–9, 16, 23; CAIDE and MLS, 2–3; Centre for Cyber Security Research and Innovation, 4–5, 10; Dr John Zerilli, 1; Dr Kate Mathews Hunt, 5, 12; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 39–40; OAIC, 46, 4; Office of the Information Commissioner Queensland, 3; Reset Australia, 7; Salinger Privacy, 34-35.

[899] UK ICO, *What is automated individual decision-making and profiling?* (n 814).

[900] Information and Privacy Commission New South Wales, *Automated decision-making, digital government and preserving information access rights – for agencies* (September 2020) 1.

[901] Justice Melissa Perry and Alexander Smith, 'iDecide: the Legal Implications of Automated Decision-making' (2014) *Federal Judicial Scholarship* 17.

[902] AHRC Report (n 128).

[903] Ibid 9.

[904] Ibid 193–9.

[905] OAIC, *Submission to AHRC Human Rights and Technology Inquiry Issues Paper* (Web page, 19 October 2018).

[906] See *Migration Act 1958* (Cth); *Australian Citizenship Act 2007* (Cth); *Social Security Administration Act 1999* (Cth).

[907] OAIC, *Submission to AHRC Human Rights and Technology Inquiry Issues Paper* (n 905).

[908] Ibid.

[909] Submissions to the Issues Paper: CAIDE and MLS, 3.

[910] Submissions to the Issues Paper: Shaun Chung and Rohan Shukla, 7; Consumer Policy Research Centre, 13; Dr John Zerilli, 2.

Rohan Shukla referred to the potential for predictive policing to 'reinforce historical racial bias and enable targeted policing of a specific demographic'.[911]

International approaches to regulating ADM

The GDPR regulates the use of personal data in ADM systems 'which produce legal or similarly significantly effects'.[912] It requires that individuals be given prior notice of the use of personal data in ADM including profiling,[913] and a right to access information about the existence of ADM and 'meaningful information about the logic involved, as well as the significance and the envisaged consequences' of such processing to the individual.[914] It also provides that individuals have the 'right not to be subject' to certain forms of ADM and requires controllers to implement measures to enable individuals to obtain human intervention on the part of the controller, to express their point of view and to contest the decision.[915]

In California, the CPRA will allow regulations to be developed to grant access and opt-out rights with respect to ADM technology, and will require businesses' responses to access requests to include meaningful information about the logic involved in such decision-making processes.[916] Canada's Bill C-11 would have provided individuals with a right to access an explanation of an ADM system's prediction, recommendation or decision, and information about how personal information that was used to make the prediction, recommendation or decision.[917]

Lack of transparency – use of ADM and explanation of decision

Some submitters proposed that individuals should receive prior notice that an APP entity uses ADM systems.[918] The AHRC report recommended that government and private sector entities be required to notify of the use of AI in decision making where it is materially used in making an administrative decision,[919] or where it has a legal, or similarly significant effect on people's rights, respectively.[920]

Proposal – prior notification of use of personal information in ADM systems

Automated decisions may have implications for individuals where they are used for significant matters such as determining eligibility for employment, entitlements or opportunities.[921] In light of the potential harm to individuals from decisions made by ADM systems that rely on their personal information, APP entities could be required to state in privacy policies whether an entity will use personal information for ADM that has a legal or similarly significant effect. This would increase transparency about when their personal information is used in ADM that affects them.

The equivalent GDPR obligation is limited to 'decisions based solely on automated processing' that produce legal or similarly significant effects.[922] However, this requirement has been criticised as being overly restrictive, with commentators noting that few decisions are made without any level of human intervention and organisations can potentially bypass the article by including a negligible level of human involvement.[923] On this basis, and to capture the use of AI throughout the

---

[911] Submission to the Issues Paper: Shaun Chung and Rohan Shukla, 7.
[912] GDPR (n 26) art 22.
[913] Ibid arts 13(2)(f), 14(2)(g).
[914] Ibid art 15(1)(h).
[915] Ibid art 22. See also, European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts*, COM/2021/206.
[916] *CPRA* (n 120) 1798.185(16).
[917] Bill C-11 (n 394) sub-cl 63(3).
[918] Submissions to the Issues Paper: Office of the Information Commissioner Queensland, 3; Reset Australia, 7.
[919] AHRC Report (n 128) 60–1.
[920] Ibid 77–8.
[921] Ibid 45.
[922] See GDPR (n 26) art 13(2)(f).
[923] Michael Veale and Lilian Edwards, 'Clarity, surprises and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling' (2018) *Computer Law & Security Review* 34(2) 398, 400. See also Submission

decision-making process, the AHRC report preferred the terminology 'AI informed decision-making.'[924]

There have also been difficulties interpreting what is meant by 'similarly significant'.[925] In recognition of this issue, state-based draft privacy legislation in the United States has sought to provide additional clarification through the inclusion of a non-exhaustive list of significant effects.[926]

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

Question

- Should the concept of a decision with 'legal or similarly significant effect' be supplemented with a list of non-exhaustive examples that may meet this threshold?

to the Issues Paper: OAIC, 94 – who submitted that the OPC of Canada explicitly recommended against the use of 'solely' in Bill C-11 (n 394).

[924] AHRC Report (n 128) 38.

[925] Veale and Edwards (n 923) 401.

[926] Submission to the Issues Paper: OAIC. See also Consumer Rights to Personal Data Processing Bill SF 2912 (Minnesota); New York Privacy Bill SB 5642 (New York); Protecting Consumer Data Bill SB 5376 – 2019-20 (Washington State). These provide a non-exhaustive list of significant effects including denial of consequential services or support, such as financial and lending services, housing, insurance, education, criminal justice, employment opportunities and health care services.

18. Accessing and correcting personal information

The Issues Paper sought feedback on whether amendments to the Act are required to enhance individuals' ability to access personal information or to ensure that personal information is up-to-date and correct. Submissions were received from stakeholders from industry, academia, government, not-for-profits and the medical sector.

Access to personal information

APP entities must provide individuals with access to their personal information upon request.[927] There are a number of grounds on which an entity may refuse access to personal information, which differ depending on whether the entity is an organisation or agency.[928] An entity must 'give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so',[929] within 30 days after the request is made (for agencies) or within a reasonable timeframe after the request is made (for organisations).[930]

Personal information that may be requested

Inferred personal information

A number of submitters considered that individuals should have a greater ability to access personal information that is inferred about them by APP entities.[931] Dr Kate Mathews Hunt submitted that greater transparency about inferred personal information is required as personal information may appear unremarkable to an individual but an algorithm which interprets it may generate unfair or inaccurate inferences.[932] The Consumer Policy Research Centre noted that service usage data can be used to infer personal information such as socioeconomic status, sexual orientation, political views, mood, stress levels, health status, personal interests, customer worth or relationship status.[933]

As discussed in Chapter 2, the current definition of personal information likely captures inferred personal information.[934] However, the Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law noted that inferred personal information may not be recorded and held by entities in the traditional sense, by virtue of the use of particular machine learning techniques.[935]

Some submitters raised concerns that access to inferred personal information is not necessarily guaranteed under the Act,[936] and that the existing exception under APP 12.3(j) should be reviewed.[937] APP 12.3(j) provides grounds to refuse access where it would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

---

[927] *Privacy Act* (n 2) sch 1 APP 12.1.
[928] Ibid sch 1 APP 12.2–12.3.
[929] Ibid sch 1 APP 12.4(b).
[930] Ibid sch 1 APP 12.4(a).
[931] Submissions to the Issues Paper: Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 8; Dr Kate Mathews Hunt, 12; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 39–40; Queensland Law Society, 7; William Delaforce, 1.
[932] Submission to the Issues Paper: Dr Kate Mathews Hunt, 12.
[933] The Consumer Policy Research Centre noted that this information may be derived from device IDs, location, usage behaviour, search history, messaging content, relationships and contacts, biometrics, transactions and purchase interests: Submission to the Issues Paper: Consumer Policy Research Centre, 4.
[934] OAIC guidance states that a 'common example' of personal information is information or opinion inferred about an individual from their activities, such as their tastes and preferences from online purchases they have made using a credit card, or from their web browsing history: 'What is personal information?', OAIC (Web Page, May 2017).
[935] Submission to the Issues Paper: Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 8.
[936] Submission to the Issues Paper: Dr Kate Mathews Hunt, 12.
[937] Submission to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 40.

The proposals in Chapter 2 to clarify that the definition of personal information includes personal information that is inferred or generated by an entity would assist with the concerns that have been raised.

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?

Information about an organisation's source of personal information

Some submitters considered that APP 12 should permit individuals to request that an organisation identify the source from which their personal information was obtained.[938] In light of concerns about third party collections of personal information taking place without an individual's knowledge, it has been proposed that the obligation to provide notice should be strengthened.[939] Other submitters suggested that individuals should be provided with records to show who their personal information has been disclosed to.[940]

Under APP 7.6, an organisation must notify an individual about the source of personal information that it uses or discloses for the purpose of direct marketing on request by the individual, unless it is impracticable or unreasonable to do so.[941]

Proposal

Requiring an organisation to provide information about the source of personal information it has collected indirectly would enhance transparency in relation to third party collections of personal information, and the sharing of personal information between organisations. In light of Proposal 16.4 to remove APP 7, the existing requirement in APP 7.6 to provide the source of personal information being used or disclosed for direct marketing could instead be included in APP 12.

It is also anticipated that Proposal 10.3 would place organisations in a position to respond to such requests, insofar as documenting the source and manner of the original collection would likely satisfy the requirement to take reasonable steps to ensure that personal information was originally collected in accordance with APP 3.

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.

Exceptions to access

APP 12 sets out a number of grounds on which APP entities may refuse a request for access to personal information.[942] Submissions suggested that additional exceptions could be introduced for situations where access to personal information may be inappropriate. A number of submitters expressed concern about the application of APP 12 to certain employee records, in the event of changes to the employee records exemption.[943]

---

[938] Submissions to the Issues Paper: Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 8; OAIC, 46.

[939] For a further discussion of this proposal, see Proposal 8.4 in Chapter 8.

[940] Submissions to the Issues Paper: Dr Chris Culnane and Ben Rubinstein, 18; Rights in Records by Design (Monash University), 3.

[941] *Privacy Act* (n 2) sch 1 APPs 7.6(e), 7.7(b).

[942] Ibid sch 1 APPs 12.2–12.3.

[943] Submissions to the Issues Paper: OAIC, 63; Ramsay Australia, 4; Castan Centre for Human Rights Law – Monash University, 21; Australian Chamber of Commerce and Industry, 12.

Submitters were also concerned that the exception in APP 12.3(e) is not broad enough to cover the internal deliberative documents of an EDR scheme for the duration of the dispute resolution process, potentially undermining the integrity of an EDR scheme.

Proposal

An additional exception could be introduced in APP 12 to allow an organisation to refuse an individual's request for access to personal information relating to EDR services where giving access would prejudice the dispute resolution process. The proposed EDR exception would prevent individuals who are engaged in an EDR process from accessing internal working documents of an EDR provider while the dispute resolution process is in progress. The exception would recognise that allowing access to such documents could provide an unfair benefit to the requesting individual. Similar access exceptions are recognised in overseas privacy laws, such as Singapore's *Personal Data Protection Act 2012*.[944]

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.

Dealing with requests for access

Some submitters expressed concern that an expansion of the definition of personal information may result in APP entities being required to provide extensive amounts of technical information in response to access requests, resulting in regulatory burden and individuals potentially receiving voluminous amounts of technical information that would be meaningless to an ordinary person.[945] Submitters proposed a number of options to address this concern. Rights in Records by Design submitted that copies of requested records should be required to be provided in a human-interpretable form.[946] The Communications Alliance suggested that an additional APP 12 exception should apply where personal information is not 'readily retrievable'.[947]

APP 12 currently establishes a process for dealing with access requests. It requires APP entities to 'give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so',[948] which might include access by email, phone, hard copy, or electronic record.[949] Where an APP entity relies on an exception to access and refuses a request entirely, or in the manner requested, the entity is required to 'take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual'.[950] The APP Guidelines clarify that entities are 'expected to consult the individual to try to satisfy their request' and that an alternative means of access that may meet the needs of the entity and the individual might include 'giving a summary of the requested personal information to the individual'.[951]

Proposal

Providing clarification that an APP entity may consult with an individual in relation to a request for access could assist entities with providing access in a way that meets the needs of both parties. This

[944] See, eg, *Personal Data Protection Act 2012* (Singapore) sch 5, sub-s 1(d).
[945] Submissions to the Issues Paper: Federal Chamber of Automotive Industries, 20; Interactive Games and Entertainment Association, 16–17; Telstra and Telstra Health, 10; Communications Alliance, 11.
[946] Submission to the Issues Paper: Rights in Records by Design, 3. See generally Bill C-11 (n 394) cl 66, which would have required entities to provide information in response to an access request in 'plain language'.
[947] Submission to the Issues Paper: Communications Alliance, 11.
[948] *Privacy Act* (n 2) sch 1 APP 12.4(b).
[949] OAIC, APP Guidelines (n 21) [12.68].
[950] *Privacy Act* (n 2) sch 1 APP 12.5.
[951] OAIC, APP Guidelines (n 21) [12.71].

may be particularly useful where the requested information would result in the provision of technical information that is not readily understood by an ordinary person or would constitute a voluminous amount of information. Additionally, where the requested personal information is not in a readily understandable format, the right of access may be enhanced by enabling individuals to request a general summary of the personal information held. Commissioner-issued guidance could further clarify this process, indicating the types of matters that may be provided in a general summary of personal information, including a description of the types of personal information held and inferences that may be derived from it.

A small number of submitters suggested that the requirement for organisations to respond to access requests within a 'reasonable period' is too subjective.[952] The APP Guidelines indicate that 'as a general guide, a reasonable period should not exceed 30 calendar days'.[953] This requirement is sufficiently flexible to accommodate complex access requests, or access requests that must be responded to by smaller entities where longer than 30 days is required.

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.

Question

- Is there evidence to suggest that organisations are taking longer than a reasonable period after a request is made to grant individuals access to their personal information?

Correction and quality

APP 10 requires APP entities to take reasonable steps to ensure that the personal information they collect, use or disclose is accurate, up-to-date and complete.[954] APP 13 requires entities to take reasonable steps to correct information that is inaccurate, out-of-date, incomplete, irrelevant or misleading and enables individuals to request to have their personal information corrected. [955]

Several submissions provided feedback on these APPs. Two submitters suggested that APPs 10 and 13 should be merged.[956] Salinger Privacy said the existing obligation in APP 10 should be extended to require personal information to be relevant, not misleading, fair and fit for its intended purpose.[957] The OAIC recommended extending APP 13 to allow for the correction of personal information that is no longer 'held' by the entity, on the basis that the existing principle does not extend to the correction of publicly available information that has been posted online.[958]

Question

- Should an APP entity be required to keep personal information it has published online accurate, up-to-date and complete, and to correct it upon request – to the extent that the entity retains control of the personal information?

[952] Submission to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 40.
[953] OAIC, APP Guidelines (n 21) [12.67].
[954] *Privacy Act* (n 2) sch 1, APP 10.
[955] Ibid sch 1, APP 13.
[956] Submissions to the Issues Paper: Financial Services Council, 3; Minderoo Tech and Policy Lab, 21.
[957] Submission to the Issues Paper: Salinger Privacy, 28.
[958] Submission to the Issues Paper: OAIC, 51.

19. Security and destruction of personal information

The Issues Paper asked whether the security requirements under the Act are reasonable and appropriate to protect the personal information of individuals. It also sought feedback on whether there should be greater requirements placed on entities to destroy or de-identify personal information that they hold.

Current security and destruction requirements

APP 11.1 requires APP entities who hold personal information to take such steps as are reasonable in the circumstances to protect that personal information from misuse, interference and loss and from unauthorised access, modification or disclosure. APP 11.1 is expressed in a technology neutral way that is not prescriptive. This gives APP entities flexibility in their interpretation of what steps are reasonable in the circumstances to protect the personal information they hold.

APP 11.2 requires APP entities to destroy or de-identify all personal information which the entity no longer needs for any purpose for which the information may lawfully be used or disclosed under the Act. There are exceptions to this requirement for Commonwealth records and information the APP entity is required to retain under Australian law.

Is there a need for clearer security requirements?

Many submitters were supportive of the current security requirements under APP 11.1.[959] The flexibility and principles-based framing of this provision allows APP entities to scale security measures in accordance with the privacy and risk of information held,[960] as well as according to 'an entity's size, resources, complexity of operations and business model.'[961] Retaining a principles-based and technology neutral requirement will also help to future-proof the Act, particularly given rapid developments in information processing technology and data practices.

However, several submitters were of the view that the 'reasonable steps' test requires some clarification as entities can find it difficult to determine what security controls are reasonable in their circumstances, or what security measures are expected of them.[962] Further clarification would help increase certainty for both entities and the individuals entrusting their personal information to them about what technical and organisational measures should be deployed.

Suggestions in submissions to clarify the 'reasonable steps' test included amending APP 11.1 to:

- include some of the requirements of Article 32 of the GDPR around security measures that APP entities are expected to implement[963]
- specify assurance mechanisms and whether it is acceptable for APP entities to rely on audit reports and security certifications supplied by standard-setting organisations[964]

[959] Submissions to the Issues Paper supportive of the current security requirements under APP 11.1 included: OAIC, 47; Facebook, 41; McAfee, 1; Dr Kate Mathews-Hunt, 12; Australian Association of National Advertisers, 4; Griffith University, 16; Experian, 20; Federal Chamber of Automotive Industries, 19; Office of the Victorian Information Commissioner, 10; ANZ, 14; BSA | The Software Alliance, 8.

[960] Submissions to the Issues Paper supportive of APP 11.1's risk-based approach included: OAIC, 47; Office of the Victorian Information Commissioner, 10; ANZ, 14; BSA | The Software Alliance, 8–9.

[961] Submission to the Issues Paper: Optus, 11.

[962] Submissions to the Issues Paper: KPMG, 17; Avant Mutual, 13; Office of the Information Commissioner Queensland, 4; Australian Information Security Association, 22.

[963] Submission to the Issues Paper: Office of the Information Commissioner Queensland, 4. See also Submissions to the Issues Paper: KPMG, 17; Australian Information Security Association, 22.

[964] Submissions to the Issues Paper: Australian Information Security Association, 22; Australian Financial Markets Association, 12.

- introduce prescriptive security requirements for specific sectors or classes of information (such as sensitive information)[965]
- introduce some of the requirements from the Australian Signals Directorate's (ASD's) 'Essential Eight',[966] and
- introduce a security risk assessment obligation based on APRA CPS234 Prudential Standard.[967]

Other submissions suggested the OAIC could provide more proactive assistance to APP entities with good practice examples or measures that may be easily implemented by organisations and small businesses to increase protections.[968]

The OAIC commented that the principles-based approach of APP 11 is important to provide a flexible baseline requirement, but that it 'does not foreclose the possibility of technology specific regulation or legislative instruments in certain circumstances'.[969] The APP Guidelines already provide guidance about the 'reasonable steps' an APP entity should take, however these guidelines are non-binding.[970]

Data breach notifications may indicate a need for greater clarity for APP entities about what measures are required to protect information. The NDB Scheme, introduced in 2018, requires APP entities to report to the OAIC and individuals about loss or unauthorised access or disclosure of personal information likely to result in serious harm to any of the individuals affected. This scheme is discussed further in Chapter 27. The data reported to the OAIC provides some insight into the extent of APP entities losing or having personal information accessed or disclosed without authorisation. In the three years the scheme has been operating, notifications were made to the OAIC and affected individuals in respect of 3312 data breaches. The leading source of data breaches is malicious or criminal attacks (including cyber incidents).[971] This suggests that the steps APP entities are taking to protect personal information could be improved.

Proposals – clarify what 'reasonable steps' may require

APP 11.1 could be amended to clarify that reasonable steps include 'both technical and organisational measures'. The OAIC has previously explained that APP entities must protect personal information using both technical security measures and also by implementing strategies in relation to governance, internal practices, processes and systems, and dealing with third party providers.[972] APP 11 could also include a list of factors (drawn from the current APP Guidelines) that influence what reasonable steps may be required including:

- the nature of the APP entity
- the amount and sensitivity of personal information held
- the possible adverse consequences for an individual in the case of a breach, and
- the relative complexity involved in implementing a security measure against the net benefits the security measure may provide.

---

[965] Submissions to the Issues Paper: Australian Information Security Association, 22; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 37; SuperChoice, 4.
[966] While not necessarily in favour of a prescriptive approach, Queensland Law Society suggested any prescriptive requirements be tailored around recognised approaches such as the 'Essential Eight'. See submission to the Issues Paper: Queensland Law Society, 6.
[967] Submission to the Issues Paper: Queensland Law Society, 6. See also Submission to the Issues Paper: KPMG, 17.
[968] Submissions to the Issues Paper: Facebook, 41–2; Griffith University, 16; McAfee, 4–5; Ramsay Australia, 8; Royal Australian College of General Practitioners, 4.
[969] Submission to the Issues Paper: OAIC, 48.
[970] OAIC, APP Guidelines (n 21) [11.7]–[11.10].
[971] OAIC, *Notifiable Data Breaches Report: January–June 2021* (Report, August 2021) ('*NDB Report: January–June 2021*').
[972] OAIC, *Australia's 2020 Cyber Security Strategy: A call for views – submission to the Department of Home Affairs* (11 November 2019)('OAIC submission to Australia's 2020 Cyber Security Strategy').

For example, a pharmacy or medical practice that holds sensitive personal information, such as health information and uses outsourced providers to provide cloud and other IT services. These types of APP entities would be reasonably expected to have contractual measures in place to protect sensitive personal information and more sophisticated ICT security policies and software security as opposed to a smaller entity that only holds a small amount of personal information. However, even entities which only hold some personal information, such as a large retail store which holds customers' names and addresses, would still be reasonably expected to have a baseline level of ICT security and software security.

Detailed security principles currently exist in overseas data protection laws, including in the EU, the UK, and Canada.[973] The security principles in each of these jurisdictions make explicit what factors are relevant to determining 'reasonable' or 'appropriate' security measures. Adding a list of factors an APP entity could consider would add some complexity to the legislation. However, the list could be high level and inclusive in nature and would merely incorporate information that would otherwise be in the APP Guidelines into the Act.

As the OAIC explained in its submission regarding Australia's 2020 Cyber Security Strategy,[974] APP 11 codifies the relationship between information security (including cyber security) and privacy. There is a fundamental link between strong cyber protection and the protection of personal information. APP entities need to monitor their cyber risk environment for emerging threats and take reasonable steps to protect personal information by mitigating those risks in order to comply with APP 11.

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.

Separate to this Review, the Government is considering legislative changes and other incentives to make Australian businesses more resilient to cyber security threats.[975] This includes a proposal that industry develop an enforceable cyber security code under the Privacy Act that would outline minimum cyber security standards for certain entities. The intent of a potential code is to encourage industry to consistently adopt cost-effective cyber security controls that can address a large percentage of common threats. A code could be a combination of specific and principles-based requirements, to retain the advantage of flexibility.

If it is considered desirable for entities to have further detail about what are reasonable steps to protect information from a cybersecurity perspective, beyond what is proposed at 19.1 and 19.2, then this could be addressed through the proposed code. The Review is not seeking submissions on this proposal but submitters are encouraged to refer to www.homeaffairs.gov.au/cyber to make submissions regarding the proposed cyber security code.

Note: As part of Australia's Cyber Security Strategy 2020,[976] the Government committed to clarify cyber security obligations for Australian businesses, including in the areas of privacy laws, consumer protection laws and corporate governance. The government is proposing to develop an APP code to specify minimum cybersecurity standards required by APP 11.1. Refer to the discussion paper 'Strengthening Australia's cyber security regulations and incentives', available at www.homeaffairs.gov.au/cyber.

[973] See, eg, GDPR (n 26) art 32(1); *PIPEDA* (n 28) c 5 sch. 1 4.7.
[974] OAIC submission to *Australia's 2020 Cyber Security Strategy* (n 972).
[975] Further information is available from the discussion paper *Strengthening Australia's cyber security regulations and incentives,* available at www.homeaffairs.gov.au/cyber.
[976] Department of Home Affairs, Australia's Cyber Security Strategy 2020 (Web Page, 2020) ('*Australia's 2020 Cyber Security Strategy*').

Question

- What is the best approach to providing greater clarity about security requirements for APP entities?

Enforcement and regulatory cooperation in cyber regulation

Submitters also highlighted the OAIC's capacity to provided technical guidance to APP entities and investigate alleged breaches of APP 11.1 in relation to cybersecurity. Some submitters suggested the OAIC should provide more proactive assistance to APP entities,[977] or share regulatory responsibility with another body.[978]

The OAIC's regulatory strategy could include increased regulatory cooperation with Australian Government bodies that have cyber security expertise, such as the Australian Cyber Security Centre, or research bodies such as CSIRO's Data61, or the Cyber Security Co-Operative Research Centre. The OP Bill will also enhance the OAIC's ability to share information with other regulators. The government is also considering challenges and opportunities in enhancing regulator roles in cyber security, including terms of collaboration with policy agencies and the Australian Cyber Security Centre.

Is there a need to strengthen the destruction requirement?

Deloitte noted in its submission that 'despite legislative requirements and recommended best-practice to the contrary, many Australian organisations currently retain personal information for longer than is reasonably necessary for a particular function or activity'.[979] The Deloitte Australian Privacy Index 2018 identified that many Australian organisations have poor retention and destruction practices, with 67 per cent of privacy policies reviewed providing little or no details on how long personal information is retained and used for.[980]

Some submitters recommended that the deletion obligations in APP 11.2 be strengthened,[981] particularly for sensitive information.[982] Others suggested the deletion obligation should be hardened by requiring mandatory deletion when data is obsolete.[983] Several submissions advocated for specific maximum retention periods for personal information.[984] Some submitters argued that APP entities should be compelled to articulate their precise data retention periods in their privacy policies and whether they delete or de-identify data, as is required under the GDPR.[985]

Submitters also called for clearer definitions or guidance about what constitutes reasonable steps for destruction and de-identification, as well as when personal information could no longer be considered as being necessary for any purpose.[986] The OAIC recommended the introduction of enhanced code-making powers and new powers to make legally-binding rules under the Act to enable the IC to set requirements or standards for destruction and de-identification by legislative instrument where appropriate. Several submissions considered that the current requirements are

[977] Submission to the Issues Paper: Griffith University, 16.
[978] Submission to the Issues Paper: Privacy108, 14.
[979] Submission to the Issues Paper: Deloitte, 28.
[980] Deloitte, *Australian Privacy Index* (Report, 2018) 11.
[981] Submission to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 38.
[982] Submission to the Issues Paper: Consumer Policy Research Centre, 10.
[983] Submissions to the Issues Paper: Cyber Security Cooperative Research Centre, 10; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 38–9.
[984] Submissions to the Issues Paper: CAIDE and MLS, 8; Blancco, 54–5; SuperChoice, 8; Electronic Frontiers Australia, 11.
[985] Submission to the Issues Paper: Calabash Solutions, 9.
[986] Submissions to the Issues Paper: Law Council of Australia, 19–20; Blancco, 55; Australian Information Security Association, 22.

sufficient,[987] or that mandating set retention timelines would have an unreasonable impact on business practice or user experience (for example a customer returning to an online account to find it deleted).[988]

Proposal – strengthen destruction requirements

APP 11.2 could be amended so that APP entities must take *all* reasonable steps to destroy or anonymise personal information when it is no longer needed or required. This would acknowledge the need to retain flexibility for when information should be destroyed according to different entities' circumstances. However, the change in wording from 'such steps as are reasonable in the circumstances' to 'all reasonable steps' would strengthen the obligation on entities to take all possible steps to destroy or anonymise information that is no longer required. The word 'de-identified' would also be replaced with 'anonymised' to reflect Proposal 2.5 in Chapter 2.

The test in APP 11.2 would also be strengthened by Proposal 10.4 in Chapter 10 which would define a secondary purpose as one that is 'directly related to and reasonably necessary to support the primary purpose'. For example, currently even where an individual ceases to engage with an APP entity, it may continue holding their personal information for secondary purposes unrelated to providing the individual the service.

The acknowledgement in APP 11.2(c) and (d) that APP entities may be required by or under an Australian law to retain information will ensure that information which may be required for taxation purposes or to fulfil obligations under consumer law, and other laws would not be required to be destroyed. As discussed in Chapter 14, if the Proposal to introduce a right to object to the use or disclosure of an individual's personal information is accepted and an individual objects to all uses of their personal information, this would trigger the requirement to delete that information under APP 11.2.

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.

[987] Submissions to the Issues Paper: KPMG, 17; Department of Health of Western Australia, 8; Griffith University, 16; Australian Medical Association, 10; Experian, 20.
[988] Submissions to the Issues Paper: Optus, 11; Telstra, 17; Facebook, 42; Interactive Games and Entertainment Association, 16–17.

20. Organisational accountability

While not raised as a distinct issue in the Issues Paper, organisational accountability was discussed in some way by a number of submitters. Organisational accountability can be described as 'the different actions and controls that an entity must implement to comply, and demonstrate compliance, with the privacy regulatory framework'.[989]

Submissions that raised organisational accountability supported introducing further accountability measures in the Act.[990] Others supported this view by highlighting that the responsibility for privacy protection currently fall too heavily on individuals, raising concerns around fairness.[991] However, other submissions were supportive of current arrangements for organisational accountability, praising the principles-based approach of the Act or warning against over-prescription of accountability obligations on APP entities.[992]

What is organisational accountability?

The OAIC discussed organisational accountability in some detail in their submission, stating:

> *The concept of accountability focusses on whether a regulated entity has translated its privacy obligations into internal privacy management processes that are commensurate with, and scalable to, the risks and threats associated with its personal information handling activities.*[993]

Organisational accountability was raised by a number of submitters in the context of a concern that responsibilities for privacy protection are out of balance and too often rest with individuals. In their submission, Salinger Privacy stated:

> *Placing the burden of privacy protection onto the individual is unfair and absurd. It is the organisations which hold personal information – governments and corporations – which must bear responsibility for doing no harm.*[994]

Submissions identified a number of key measures of organisational accountability, including privacy by design and privacy by default, record keeping requirements, privacy impact assessments (PIAs), and privacy officers.[995] These are discussed in more detail below.

Current organisational accountability requirements under the Act

APP 1 seeks to ensure 'that entities manage personal information in an open and transparent way'.[996]

---

[989] Submission to the Issues Paper: OAIC, 97.
[990] Submissions to the Issues Paper: OAIC, 97; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 11; Salinger Privacy, 22;
[991] Submissions to the Issues Paper: CAIDE and MLS, 6; Legal Aid Queensland, 3; ; The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law, 7.
[992] Submissions to the Issues Paper: Ai Group, 8; Facebook, 27; Snap Inc., 4–5; Google, 4; Free TV, 3; Telstra and Telstra Health, 5.
[993] Submission to the Issues Paper: OAIC, 97.
[994] Submission to the Issues Paper: Salinger Privacy, 22.
[995] Submissions to the Issues Paper: OAIC, 98; Salinger Privacy, 27; ElevenM, 2; Privcore, 4; Privacy108, 11; Consumer Policy Research Centre, 7; ID Exchange, 11–12; Castan Centre for Human Rights Law – Monash University, 26; Australian Privacy Foundation, 25–6; Humanising Machine Intelligence Project - Australian National University, 2–3; Law Institute of Victoria, 3–4; Data Synergies, 4; CAIDE and MLS, 6; Centre for Media Transition – University of Technology Sydney, 15–16. See also GDPR (n 26) arts 25, 30, 35, 37.
[996] *Privacy Act* (n 2) sch 1 APP 1.1.

It requires that APP entities:

- take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the APP entity's functions or activities that will ensure compliance with the Australian Privacy Principles,[997] and
- have a clearly expressed and up-to-date policy (the APP privacy policy) about the management of personal information by the APP entity.[998]

The inclusion of APP 1 in the Act in 2012 was intended 'to keep the Privacy Act up-to-date with international trends that promote a 'privacy by design' approach, that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception'.[999]

Privacy by design involves 'data protection through technology design'.[1000] It is grounded in the idea that privacy protection is best addressed when it is integrated in technology when it is created,[1001] 'rather than being bolted on afterwards.'[1002] This principle may include measures such as the use of pseudonymisation and encryption.[1003]

The explanatory memorandum to the 2012 Bill clarified that policies and practices under APP 1.2 could potentially include:

- training staff and communicating to staff information about the agency or organisation's policies and practices
- establishing procedures to receive and respond to complaints and inquiries
- developing information to explain the agency or organisation's policies and procedures, and
- establishing procedures to identify and manage privacy risks and compliance issues, including in designing and implementing systems or infrastructure for the collection and handling of personal information by the agency or organisation.[1004]

Additionally, the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Australian Government Agencies Privacy Code) sets out further requirements that government agencies must implement as part of privacy management and governance. These include the following requirements:

- **Privacy Officer** – an agency must at all times have a designated Privacy Officer and ensure that certain functions are carried out, including handing of internal and external privacy enquiries, complaints and requests for access to and correction of personal information made under the Act, maintaining a record of the agency's personal information holdings and assisting with the preparation of PIAs.
- **PIAs** – an agency must conduct a PIA for all high privacy risk projects. A project may be a high privacy risk project if the agency reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals. An agency may publish a PIA, and they must maintain a register of the PIAs it conducts.

[997] *Privacy Act* (n 2) sch 1 APP 1.2.
[998] Ibid sch 1 APP 1.3.
[999] Explanatory Memorandum, Enhancing Privacy Protection Bill (n 139) 73.
[1000] Intersoft Consulting, 'GDPR: Key Issues - Privacy by Design' (Web Page).
[1001] Ibid.
[1002] Submission to the Issues Paper: OAIC, 99.
[1003] European Commission, *What does data protection 'by design' and 'by default' mean?* (Web page).
[1004] Explanatory Memorandum, Enhancing Privacy Protection Bill (n 139) 73.

International approaches to organisational accountability

The GDPR framework includes a number of organisational accountability measures, including privacy by design and privacy by default. Privacy by default requires entities to ensure that, by default, personal information is handled with the highest privacy protections. It is a complementary principle to privacy by design. It includes only collecting the minimum amount of personal information that is necessary for the specific purpose for which it will be used.[1005] These principles are prescribed in the UK. [1006]

The GDPR also requires entities that handle personal data to maintain certain records of processing activities, including records of the purposes of processing, a description of the categories of personal data being processed, and where possible, a general description of the security measures implemented to ensure a level of security of the data appropriate to the risk.[1007] The UK has similar record keeping requirements under the *Data Protection Act 2018*.[1008]

Canada proposed similar requirements in the now lapsed Bill C-11.[1009] That Bill included an 'appropriate purposes' clause, which required an organisation to determine at or before the time of the collection of any personal information, each of the purposes for which the information is to be collected, used or disclosed, *and to record those purposes*.[1010] If an organisation sought to use or disclose personal information for a new purpose, they would need to record that new purpose before undertaking the use or disclosure.[1011]

Canada requires federal government institutions to undertake PIAs for new or substantially modified programs or activities involving the creation, collection and handling of personal information.[1012] Data protection impact assessments are also required in the EU and in the UK.[1013] These assessments are required where a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons.[1014]

Privacy or data protection officer requirements are in place under the GDPR, as well as in the UK, New Zealand and Canada. A privacy officer is a designated person within an organisation who is responsible for ensuring compliance with the relevant privacy or data protection laws, and typically also assist with PIAs and act as the contact point for the relevant authority.[1015]

Another relevant measure in the GDPR is the controller-processor distinction. This measure distinguishes between those organisations that determine the purposes of data processing (controllers), and those organisations (processors) which process data on behalf of the first-mentioned organisation. This distinction supports accountability as the controller must only use processors that provide sufficient guarantees to implement appropriate measures that meet the requirements of the GDPR, and ensure the protection of the rights of the data subject.[1016] Processors must process data in accordance with instructions from the controller.[1017] Controllers are also

---

[1005] Submission to the Issues Paper: OAIC, 99–100.
[1006] UK ICO, *Guide to the General Data Protection Regulation* (Web Page, 1 January 2021), 174–5 ('Guide to the GDPR').
[1007] GDPR (n 26) art 30.
[1008] *Data Protection Act 2018* (UK) (n 37) sch 6 para 25.
[1009] Bill C-11 (n 394) cl 12(3).
[1010] Ibid; Submission to the Issues Paper: OAIC, 102.
[1011] Bill C-11 (n 394) cl 12(4).
[1012] Treasury Board of Canada Secretariat, *Directive on Privacy Impact Assessment* (Web Page, 18 June 2020) 5.1.
[1013] GDPR (n 26) art 35.
[1014] Ibid.
[1015] Ibid art 39; *Data Protection Act 2018* (UK) (n 37) sch 6 paras 29–30; *Privacy Act 2020* (NZ) (n 29) s 201; *PIPEDA* (n 28) sch 1 4.1.1.
[1016] GDPR (n 26) art 28.
[1017] GDPR (n 26) art 29.

responsible for the compliance of their processor(s) with any conditions of processing.[1018] The controller-processor distinction is discussed in more detail in Chapter 21.

Are further organisational accountability measures required?

Some of the submissions that discussed organisational accountability expressed support for the flexibility currently provided by the principles-based approach of the Act, which allows APP entities to implement their obligations in a way that best suits their circumstances.[1019]

Some submissions expressed concern about the potential regulatory burden that could be imposed on APP entities from overly prescriptive regulation.[1020] Others noted that responsibility for privacy protection should be shared between individuals and APP entities.[1021] Telstra expressed the need for balance between business and privacy interests, stating that a principles-based regime that recognises both of these interests will best serve the needs of consumers.[1022]

Other submissions that supported the current approach to accountability under the Act expressed concern that overly prescriptive requirements carry a risk of deterring innovation.[1023] In their submission, Facebook stated that:

> *Given the rapidly developing nature of the global digital economy, there is also a possibility that Australian consumers and businesses will be left behind if our regulatory framework is too rigid and not sufficiently adaptable. Data protection laws should be outcome-oriented and leave room for different ways in which to achieve relevant overall compliance goals.*[1024]

However, other submitters highlighted the importance of organisational accountability measures as the regulatory counterbalance to privacy self-management, particularly in light of the limitations of notice and consent to adequately protect individuals' privacy.[1025]

More than half of the submissions that discussed organisational accountability supported introducing further measures into the Act – including expressly requiring privacy by design, requirements to keep records in certain circumstances and expanding the circumstances in which APP entities must conduct a PIA.

The OAIC made several recommendations for changes to the Privacy Act to incorporate greater accountability requirements:

- APP 1 should be amended to require that APP entities:
    - *be able to demonstrate* reasonable steps taken to implement practices, procedures and system that will ensure compliance with the APPs (and any relevant registered APP Code)
    - implement, and be able to demonstrate implementation of, a privacy by design and privacy by default approach, and
    - appoint a privacy officer and ensure their functions are undertaken.
- The explanatory memorandum to the Bill implementing these amendments should include a note that 'an ongoing and demonstrable, comprehensive privacy management program,

[1018] UK ICO, Guide to the GDPR (n 1006) 15.
[1019] Submissions to the Issues Paper: Ai Group, 8; Facebook, 27; Google, 4; Free TV, 3.
[1020] Submissions to the Issues Paper: Ai Group, 8–9; Telstra and Telstra Health, 5.
[1021] Submissions to the Issues Paper: Association of Data-driven Marketing and Advertising, 16; Ai Group, 8.
[1022] Submission to the Issues Paper: Telstra and Telstra Health, 5.
[1023] Submissions to the Issues Paper: Facebook, 27; Ai Group, 8.
[1024] Submission to the Issues Paper: Facebook, 27.
[1025] Submissions to the Issues Paper: Data Synergies, 12; Centre for Media Transition – University of Technology Sydney, 15–16; Humanising Machine Intelligence Project - Australian National University, 2–3; Castan Centre for Human Rights Law – Monash University, 26; Professor Kimberlee Weatherall, 7–8.

which includes conducting privacy impact assessments where appropriate, is central to facilitating privacy by design and privacy by default approach'.
- APP 3 should be amended to expressly require APP entities to determine, at or before the time of collection, each of the purposes for which the information is to be collected, used or disclosed and to record those purposes.[1026]

In making these recommendations, the OAIC acknowledged that while individuals should retain some responsibility for privacy self-management, this should be complemented by organisational accountability measures 'to ensure that the burden of understanding and consenting to complicated practices does not fall solely on individuals'.[1027]

Other submissions also supported introducing a more explicit privacy by design approach in the Act.[1028] This included the Australian Privacy Foundation (APF), which endorsed the OAIC's recommendations for demonstrable accountability, and noted that 'PIAs lie at the very heart of privacy protection'.[1029] Many of these submissions also supported a privacy by default approach being required by the Act.[1030] Several submitters expressed support for mandating PIAs in certain circumstances, including for high risk or new projects, or any initiative that may adversely impact people.[1031] Some submissions also noted that prescribing further organisational accountability measures would bring the Act into line with other international frameworks, such as the GDPR.[1032]

Proposal

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. In light of the emergence of particularly high privacy risk acts and practices by virtue of technological advances since APP 1 was introduced, it is considered that there is scope to introduce some further organisational accountability measures to increase transparency and accountability in respect of these high privacy risk acts or practices.

Other proposals in this paper would support the accountability and transparency of APP entities' information handling practices by requiring additional information to be included in their privacy policies, such as:

- whether the APP entity's collection of personal information is required or authorised by or under an Australian law, or a court or tribunal order – including the name of the Australian law, or details of the court or tribunal order that requires or authorises the collection
- the main consequences, if any, for the individual if all or some of the personal information is not collected by the APP entity

[1026] Submission to the Issues Paper: OAIC, 101–2. The OAIC's submission also included a recommendation regarding a domestic privacy certification scheme as part of its discussion of organisational accountability (recommendation 45). Chapter 23 of this paper discusses the concept of such a scheme in further detail.
[1027] Submission to the Issues Paper: OAIC, 97.
[1028] Submissions to the Issues Paper: Privacy108, 11; Centre for Media Transition – University of Technology Sydney, 15; CAIDE and MLS, 6; Law Institute of Victoria, 3–4; Humanising Machine Intelligence Project - Australian National University, 2-3; Salinger Privacy, 3.
[1029] Submission to the Issues Paper: Australian Privacy Foundation, 41–2.
[1030] Submissions to the Issues Paper: ID Exchange, 11–12; Castan Centre for Human Rights Law – Monash University, 26.
[1031] Submissions to the Issues Paper: Privcore, 4; ElevenM, 2; Institute for Cyber Investigations and Forensics, University of the Sunshine Coast, 8; Salinger Privacy, 27.
[1032] Submissions to the Issues Paper: Australian Privacy Foundation, 25–6; Salinger Privacy, 27; Humanising Machine Intelligence Project - Australian National University, 2–3; Professor Kimberlee Weatherall, 7–8.

- whether the APP entity is likely to disclose the personal information to overseas recipients – and if so, the countries in which such recipients are likely to be located and the specific personal information that may be disclosed [1033]
- whether the APP 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
- whether the APP 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,[1034] and
- whether the APP entity uses personal information in ADM which has a legal, or similarly significant effect on people's rights.[1035]

As outlined in Chapter 11, Option 1 in Proposal 11.1 would require APP entities that engage in restricted practices to undertake additional organisational accountability measures to adequately identify and mitigate privacy risks in a flexible and scalable way. This could require a formal PIA depending on the circumstances. Specific record keeping requirements could also apply to enable the APP entity to demonstrate compliance with the principle of privacy by design for assessment by the Information Commissioner, if required.

These enhanced scrutiny requirements would extend a similar obligation already in place for government agencies under the Australian Government Agencies Privacy Code to the private sector, in a flexible and scalable way when those organisations engage in restricted practices.

Further, in light of the increasing use of personal information by third parties, including through the increasing prevalence of data analytics, additional measures to increase accountability in respect of secondary purposes for use or disclosure of personal which are not notified to the individual when their information is collected are warranted.

At this time, it is not considered that there is a need for APP 3 to be amended to expressly require APP entities to determine, at or before the time of collection, each of the purposes for which the information is to be collected, used or disclosed, and to record those purposes. This should be already done through the process of issuing a collection notice. However, some submissions raised that APP entities may be able to use personal information that has already been collected for a secondary purpose without individuals knowing about that use, as no notice was required to be given for that secondary purpose.[1036] These submissions echo the conclusions in the ACCC's DPI report about the ability of APP entities to use personal information that has already been collected for secondary purposes without the awareness of individuals, as notice is not required.[1037]

In light of this, the Act would be amended to expressly require APP entities to determine each of the secondary purposes for which personal information is to be used or disclosed, at or before using or disclosing that personal information for a secondary purpose. Those secondary purposes must be recorded. This proposal is in addition to the proposed reforms to APP 6 set out in Chapter 10. This would enable APP entities to understand the uses to which they are putting their data as well as facilitate the effectiveness of additional self-management mechanisms, including an ability for

[1033] These are matters which would no longer be included in a collection notice but would instead be set out in the APP entity's privacy policy. For a further discussion of this proposal, see Chapter 8 of this paper. For a further discussion regarding increased transparency requirements in relation to potential overseas disclosures, see Chapter 22.
[1034] For a further discussion of these proposals, see Chapter 16 of this paper.
[1035] For a further discussion of this proposal, see Chapter 17 of this paper.
[1036] Submissions to the Issues Paper: OAIC, 102; Salinger Privacy, 28; Office of the Victorian Information Commissioner, 6; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 26.
[1037] ACCC, DPI report (n 2) 438.

individuals to object to collections, uses and disclosures of their personal information. This is discussed further in Chapter 14.

This approach to organisational accountability seeks to introduce measures to enhance the accountability of entities in a way which is flexible, scalable and proportionate to the level of privacy risks associated with their handling of personal information.

20.1 Introduce further organisational accountability requirements into the Privacy Act, targeting measures to where there is the greatest privacy risk:

- Amend APP 6 to expressly require APP entities to determine, at or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.

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?

21. Controllers and processors of personal information

While the Issues Paper did not seek views on whether to amend the Act to introduce the concepts of data controllers and data processors, a number of submissions commented on the distinction, with the majority being private sector organisations.

What are controllers and processors?

These concepts are found in many overseas data protection frameworks. Generally, a *data controller* is an entity which, alone or jointly with others, determines the purposes and means of the processing of personal information and a *data processor* is an entity which processes personal information on behalf of the controller.[1038] While a data processor can exercise some control over the manner of processing such as the technical aspects of how a service is delivered (within the scope of the direction provided by the controller), legal responsibility for compliance with privacy laws falls directly on the data controller and not the data processor.[1039]

For example, a business engages a printing company to produce invites for an event. The business provides the printing company with the names and addresses of their clients from their database. The printing company uses this information to send out invitations. The business is considered the controller of the personal information that is used to send the invitations since it has determined the purpose of processing the personal information (to send invitations for an event) and the means of the processing. The printing company is only processing the personal information as per the business' instructions and is therefore a processor and not a controller.

Joint controllers

If two or more entities jointly determine the purposes and means of the processing of the same personal information, they will be joint controllers.[1040] Entities will not be joint controllers if they are processing the same information for different purposes. Joint controllers must make arrangements as to which entity will take primary responsibility for complying with legal obligations such as access and correction requests and make this information available to individuals.[1041]

Benefits of adopting the controller processor distinction

Clarify entities' accountability

A number of submitters recommended introducing the concepts of controllers and processors in the Act.[1042] It was considered that the distinction would increase the efficiency of the Act by allocating responsibilities relating to notification, consent and security. These submitters were of the view that a clear allocation of accountability between data controllers and processors is key to a successful data protection regime.[1043]

Imposing obligations to ensure data controllers, rather than data processors are accountable for the protection of personal information is analogous to the requirement in APP 8 and section 16C (discussed further in Chapter 22) which states APP entities are responsible for taking reasonable steps to ensure personal information is protected once it is disclosed overseas.

[1038] GDPR (n 26) art 4(7), 4(8).
[1039] UK ICO, *Data controllers and data processors: what the difference is and what the governance implications are* (2018) 16.
[1040] UK ICO, *What does it mean if you are joint controllers?* (Web Page, accessed 26 May 2021).
[1041] UK ICO, *Controllers, joint controllers and processors* (Web Page, accessed 26 May 2021).
[1042] Submissions to the Issues Paper: Microsoft Australia, 1–2; Communications Alliance, 9; Records and Information Management Professionals of Australasia, 5–6; Salesforce, 2; Google, 11–12; Business Council of Australia, 4; Privacy108, 13; elevenM, 3; Snap Inc., 2; BSA, 2.
[1043] Submissions to the Issues Paper: Records and Information Management Professionals of Australasia, 6; Information Technology Industry Council, 1; elevenM, 3; Snap Inc., 2; BSA, 3.

Submitters considered that since data processors only act on the documented instructions of the data controllers that engage them, processors should not be subject to the same compliance obligations as they lack the authority to make independent decisions about how to use personal information.[1044] Some submitters were of the view that processors should be responsible for following the controller's instructions, data security and notifying the controller of a data breach and that controllers should maintain responsibility for meeting privacy obligations under the Act and providing redress to individuals.[1045]

Submissions noted that the distinction would provide clarity to individuals about the roles of different entities and which entity to contact in the event they want to exercise their rights under the Act.[1046] Submissions also noted that a controller/processor distinction could assist in clarifying obligations under APP 8 in the context of overseas cloud service providers.[1047] Telstra submitted that entities often engage specialist contractors and that it was 'hard to see any benefit to consumers of requiring collection notices each time personal information was shared in these types of circumstances' and noted that requiring processors to also give notice could lead to an increased sharing of contact information to facilitate the provision of notice.[1048]

Notifiable Data Breaches scheme

Submitters noted that the lack of distinction between controllers and processors in the Act can lead to complications when responding to data breaches.[1049] Under the current provisions, the obligation to report an eligible data breach applies in relation to personal information 'held' by an entity,[1050] which can lead to multiple entities having reporting obligations in relation to the same breach.[1051] Some submitters were of the view that while a processor may be in possession of personal information, it may generally not be best-placed to assess whether an 'eligible data breach' had occurred or to notify affected individuals.[1052] Submitters were of the view that notification and assessment of harm issues have been resolved overseas by assigning clear roles and liabilities through a distinction between controllers and processors.[1053] However, it is not clear that limiting reporting obligations to controllers would be beneficial as it could reduce protection for individuals affected by a breach by removing the obligation for an entity acting as a processor to notify the OAIC of a breach where the controller fails to do so.

International approaches

Submissions noted that the distinction between controllers and processors is present in many international data protection regimes including GDPR, CBPR and the domestic privacy laws of New Zealand, Brazil, Japan, Hong Kong, the Republic of Korea and Singapore.[1054] The distinction is also present in the draft privacy laws of India and Indonesia and in Canada's now lapsed Bill C-11.[1055] Submitters were of the view that introducing a distinction in the Act would align Australia with

---

[1044] Submissions to the Issues Paper: Microsoft Australia, 1–2; Google, 11; Information Technology Industry Council, 1.
[1045] Submissions to the Issues Paper: Microsoft Australia, 1–2; Communications Alliance, 9; Google, 11.
[1046] Submissions to the Issues Paper: Salesforce, 2; Information Technology Industry Council, 1; Snap Inc., 2; BSA, 3; OAIC, 98.
[1047] Submissions to the Issues Paper: Australian Financial Markets Association, 13; Law Institute of Victoria, 11.
[1048] Submission to the Issues Paper: Telstra, 8.
[1049] Submissions to the Issues Paper: BSA, 3; Workday, 1–2.
[1050] *Privacy Act* (n 2) sub-s 26WE(1)(a).
[1051] Submission to the Issues Paper: Workday, 1–2.
[1052] Ibid.
[1053] Submissions to the Issues Paper: Australian Retail Credit Association, 11; Australian Banking Association, 8.
[1054] Submissions to the Issues Paper: Salesforce, 2; Information Technology Industry Council, 1; Snap Inc., 2.
[1055] Linklaters, *Data Protected – India* (Web Page, March 2020); PWC, *Digital Trust NewsFlash* (Web Page, May 2020); Bill C-11 (n 394).

global best practice and streamline obligations for Australian businesses required to comply with the privacy laws of other jurisdictions.[1056]

Challenges of introducing these concepts in the Act

The Act in its current form does not generally apply to small businesses with an annual turnover of less than $3 million, subject to certain exceptions (see Chapter 4). This would be likely to pose some difficulties with adopting the concepts of controllers and processors in the same way they have been adopted overseas. For example, if a small business controller not covered by the Act engaged an APP entity as a processor, neither entity would be required to provide notice, seek consent, ensure security or notify the OAIC of a data breach.

This could potentially be addressed by limiting the adoption of the concepts to instances where both the controller and processor are APP entities covered by the Act. However this may increase complexity and cause confusion for entities and individuals as to entities' obligations where it is not clear whether or not an entity is covered by the Act.

Questions

- Are there any other advantages or disadvantages of introducing these concepts in the Act?
- If limitations in the Act's coverage makes full adoption of these concepts impractical, would partial adoption be beneficial? If yes, how could this occur without being overly complex?
- If adopted, what obligations under the Act should processors have (record keeping, security, NDB etc.)?

[1056] Submissions to the Issues Paper: Microsoft Australia, 1–2; Information Technology Industry Council, 1; Snap Inc., 2.

22. Overseas data flows

The Issues Paper sought feedback on topics related to overseas data flows including the Act's extraterritorial application, the Act's approach to cross-border disclosures of personal information, Australia's implementation of the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system, the possible benefits of a domestic privacy certification scheme and the benefits and disadvantages of Australia seeking adequacy under the GDPR. The Review received a high level of interest in these issues and received submissions from a wide variety of stakeholders including government agencies, academics, research centres, private sector organisations, industry peak bodies, individuals and consumer advocates.

Extraterritorial application

The Issues Paper asked whether the exception to the Act's extraterritorial application for acts or practices required by an applicable foreign law is still appropriate. Submissions on this topic expressed support for the exception and noted that it is required to minimise conflict of laws where companies are faced with the choice of breaching the laws of one country or another.[1057] A small number of submissions also suggested amendments to clarify the extraterritorial application of the Act.[1058]

Clarifying the scope of the Act's extraterritorial application

The extraterritorial provisions of the Act are intended to capture multinational corporations based overseas with offices in Australia, as well as entities with an online presence (but no physical presence in Australia) that 'carry on business in Australia' and collect or hold personal information in Australia.[1059] The OAIC's submission noted that an increasing number of matters being considered by the IC present situations that enliven these provisions.[1060] The submission outlined the practical difficulties in establishing that a foreign business has collected information directly from Australia, and noted that it can be resource intensive to establish jurisdiction over motivated and well-resourced international companies.[1061]

The OAIC recommended amendments to list particular indicators of 'carrying on business in Australia' and that the requirement for information to have been collected or held in Australia be removed and instead be listed as one of the indicators of 'carrying on business in Australia'.[1062] Amendments to clarify the extraterritorial application of the Act are being progressed as part of the OP Bill. The OP Bill includes an amendment to remove the requirement that personal information be collected or held in Australia.[1063] Removing the condition that an organisation has collected or held information within Australia will mean that organisations that collect the personal information of Australians from digital platforms that do not have servers in Australia will more clearly be subject to the Act.[1064]

The accountability approach

As noted in the Issues Paper, the aim of APP 8 and section 16C of the Act is to facilitate the free flow of information across national borders, while ensuring the privacy of individuals is respected.[1065]

[1057] Submissions to the Issues Paper: Information Technology Industry Council, 3; Optus, 12; Gadens, 10.7; Interactive Games and Entertainment Association,19; Facebook, 44; Palo Alto Networks, 4; Griffith University, 18. Karen Meohas, 12; Communications Alliance, 12.

[1058] Submissions to the Issues Paper: Australian Privacy Foundation, OAIC.

[1059] Privacy Act (n 2) s 5B; *Australian Information Commissioner v Facebook Inc (No 2)* [2020] FCA 1307.

[1060] Submission to the Issues Paper: OAIC, 113.

[1061] Ibid, 114.

[1062] Ibid, 114.

[1063] Exposure Draft, OP Bill (n 1) sch 1, cl 2.

[1064] Explanatory Paper, OP Bill (n 1), 21.

[1065] *Privacy Act* (n 2) s 2A(f).

APP 8.1 provides that before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure the overseas recipient does not breach the APPs in relation to the information.[1066] Section 16C provides that an APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs. That is, the act or practice engaged in by the overseas recipient that would be a breach of the APPs is taken to have been done by the APP entity and to be a breach of the APPs by the APP entity.[1067] Under the accountability approach, an APP entity will be liable for the acts and practices of an overseas recipient, and an individual will have a means of redress, even if the entity took reasonable steps to ensure the overseas recipient complied with the APPs, although any reasonable steps may be taken into account as mitigation for the breach.[1068] APP 8.2 provides a number of exceptions to this framework.

The Issues Paper sought feedback on the benefits and disadvantages of the accountability approach and whether APP 8 and section 16C are still appropriately framed. Submissions generally expressed support for the current approach and noted that the accountability approach creates awareness for data protection during cross-border disclosures.[1069] However, submitters suggested a number of amendments to APP 8 to better protect consumers and support entities disclosing information to overseas jurisdictions.

Exception – overseas recipient is subject to substantially similar law or binding scheme

Under APP 8.2(a) an APP entity is not required to take 'reasonable steps' (and would not be liable under section 16C) if the entity reasonably believes the recipient of the information is subject to a law or binding scheme that, overall, is at least substantially similar to the APPs and there are mechanisms that an individual can access to take action to enforce those protections.[1070] Consistent with feedback provided to previous reviews,[1071] submissions expressed concern that the current approach places the burden on an APP entity to determine whether overseas laws are 'substantially similar' to the APPs,[1072] and noted that entities have difficulty undertaking this assessment.[1073]

Proposal

Introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a)

As noted in the Issues Paper, the ALRC previously recommended that the government develop and publish a list of laws and binding schemes in force outside Australia that provide privacy protections that are substantially similar to the APPs.[1074] A large number of submissions supported the publication by government of a list of laws and binding schemes that provide substantially similar protections to the APPs.[1075] The view of submitters was that this would provide APP entities greater

---

[1066] Ibid, sch 1, APP 8.1. Note APP 8.1 refers to a breach of the APPs with the exception of APP 1.
[1067] Ibid, s 16C.
[1068] OAIC, APP Guidelines (n 21) [8.58].
[1069] Submissions to Issues Paper: Information Technology Industry Council, 3; Microsoft, 5–6; Palo Alto Networks, 4; Federal Chamber of Automotive Industries, 21; Association for Data-driven Marketing and Advertising, 20; Atlassian, 5; Australian Banking Association, 7; Data Synergies, 47; Experian, 22; Facebook, 44; Gadens, 11; Optus, 12; Royal Australian College of General Practitioners, 4.
[1070] *Privacy Act* (n 2) sch 1, APP 8.2(a).
[1071] ALRC Report 108 (n 53) 1092–95; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, 2005, 77.
[1072] Submissions to the Issues Paper: Calabash Solutions, 10; CSIRO, 9; KPMG, 18; Experian, 22.
[1073] Submissions to the Issues Paper: Calabash Solutions, 10; Cyber Security Cooperative Research Centre, 10–1; Dr Kate Mathews Hunt, 13; Griffith University, 18; Experian, 22; Gadens, 11.
[1074] ALRC Report 108 (n 53) 1122.
[1075] Submissions to the Issues Paper: AGL Energy Limited, 4; ANZ, 15–6; Atlassian, 5; Australian Banking Association, 7; Australian Financial Markets Association, 13; Australian Privacy Foundation, 28; DIGI, 12; Calabash Solutions, 10; CSIRO, 9; Cyber Security Cooperative Research Centre, 11; Department of Health of Western Australia, 9; Experian, 22; Federal Chamber of Automotive Industries, 21; Gadens, 11; Griffith University, 18; illion, 6; Interactive Games and Entertainment Association, 18; National Health and Medical Research Council, 2; OAIC, 112; Roche, 8; United States Chamber of Commerce, 3; Federal Chamber of Automotive Industries, 21.

certainty when disclosing personal information overseas and would allow consumers to make informed choices about where their data is disclosed.[1076]

A process of prescribing countries and overseas binding schemes with privacy laws that provide substantially similar protections to the APPs could achieve this objective. Disclosures of personal information to prescribed countries would not attract the current obligations under APP 8.1 and section 16C. These transfers would be similar to those facilitated through adequacy agreements under the GDPR.[1077] Recent reforms to the NZ Privacy Act have introduced a similar mechanism to enable countries with privacy laws that provide comparable safeguards to be prescribed.[1078] The NZ Act also provides that a country may be prescribed subject to specific qualifications relating to the type of entity that personal information may be disclosed to, and the type of personal information that may be disclosed.[1079] The OAIC's submission noted that a list of prescribed countries would need to give due consideration to the available mechanisms for individuals to enforce protections as required under APP 8.2(a).[1080] This could take the form of reciprocal arrangements between the OAIC and equivalent overseas regulators, or clear dispute resolution processes for schemes such as the CBPR system.

The OAIC's submission also acknowledged that certification schemes are likely to be considered binding schemes for the purpose of APP 8.2, provided the certification has a binding effect and enables individuals to seek redress.[1081] Similar to prescribing countries, certification schemes could also be prescribed. A number of submitters proposed that international certification schemes be recognised as a basis for transferring personal information outside Australia under APP 8.2(a).[1082] For example, the APEC CBPR system, discussed further below, is an international certification scheme with well-established enforcement mechanisms that could be considered for inclusion on the prescribed list as a binding scheme subject to an assessment of the CBPR Program Requirements.

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

Introduce standard contractual clauses

A number of submitters also supported the introduction of standard contractual clauses (SCCs) for transferring personal information overseas, which contain safeguards stipulating how an overseas recipient of personal information is expected to handle that information. These clauses could be used by APP entities when contracting with entities overseas to facilitate transfers to countries that are not prescribed.[1083] SCCs would reduce the regulatory burden on APP entities to negotiate appropriate clauses for the handling of personal information when contracting with overseas entities,[1084] which could be particularly beneficial for smaller businesses that are required to comply with the Act and entities that do not disclose personal information overseas as a regular part of their business. The OAIC's submission noted that SCCs should support accountability under APP 8.1, as

[1076] Submissions to the Issues Paper: AGL Energy Limited, 4; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 42–3; ANZ, 15; Atlassian, 5.
[1077] GDPR (n 26) art 45.
[1078] NZ Privacy Act (n 29) s 214.
[1079] Ibid sub-s 214(3).
[1080] Submission to the Issues Paper: OAIC, 112.
[1081] Submissions to the Issues Paper: illion, 6; OAIC, 111.
[1082] Submissions to the Issues Paper: Ramsay Health Care, 9; Calabash Solutions, 10; Australian Information Security Association, 24; illion, 6–7.
[1083] Submissions to the Issues Paper: AGL Energy Limited, 4; CSIRO, 9; Federal Chamber of Automotive Industries, 21; Western Union, 3; Global Data Alliance, 2; Queensland Law Society, 7; OAIC, 110; United States Chamber of Commerce, 3; Google, 11.
[1084] Submissions to the Issues Paper: AGL Energy Limited, 4; CSIRO, 9; Federal Chamber of Automotive Industries, 21; Western Union, 3; Global Data Alliance, 2; Queensland Law Society, 7; OAIC, 110; United States Chamber of Commerce, 3.

opposed to being an exception to accountability under APP 8.2.[1085] AGL's submission noted that APP 8 currently results in heavy reliance being placed on contractual obligations which may not adequately assist affected consumers or place sufficient emphasis on proactive management and monitoring of cross-border disclosures by holders of personal information.[1086] SCCs could mitigate this risk by providing templates that appropriately address these issues.

The NZ Office of the Privacy Commissioner has recently published model contract clauses to assist NZ entities meet their privacy obligations.[1087] Clauses are tailored to the requirements of the NZ Privacy Act and are designed to make it easier for regulated entities to comply with the NZ equivalent of APP 8. SCCs are also used under the GDPR to ensure adequate privacy protections continue to apply to personal data transferred outside of the EU.[1088]

22.2 SCCs for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information

International Money Transfers

The Australian Banking Association and ANZ submitted that APP 8 should be amended to provide permanent relief to remitting International Money Transfers (IMTs).[1089] This could be achieved by incorporating an additional exemption for IMTs in APP 8.2. The IC has provided temporary relief through Public Interest Determinations (PIDs) from contraventions of APP 8, section 15, and subsection 16C(2) for cross-border disclosures of a beneficiary's personal information for the process of an IMT.[1090] In February 2020, the IC issued the most recent PID to provide ANZ, the Reserve Bank of Australia and other financial institutions with relief so that remitting banks will not be in breach of APP 8 when processing IMTs. The current PID is due to expire in 2025, at which time the IC would be required to undertake a period of public consultation before issuing a further PID.[1091]

A proposal to amend the Act to include a permanent exception for IMTs was raised by the Australian Banking Association in the consultation process undertaken prior to the current PID being issued. The Explanatory Statement to the current PID references this proposal and states the Commissioner's view that PIDs are the most appropriate mechanism for providing an exception for IMTs from the Act as the process for issuing a PID ensures that relevant risks are regularly assessed. On this basis, there does not seem to be sufficient merit in departing from the current process for exempting personal information transferred overseas through IMTs from relevant requirements of the Act.

Proposal

Remove the exception to accountability where consent is obtained

APP 8.2(b) provides an exception to accountability if an entity expressly informs an individual that if they consent to the disclosure of their personal information, APP 8.1 will not apply to the disclosure, and after being informed, the individual consents to the disclosure.[1092] When an entity seeks express consent under APP 8.2, the entity is not required to take reasonable steps to ensure that the overseas recipient does not breach the APPs.

[1085] Submission to the Issues Paper: OAIC, 111.
[1086] Submission to the Issues Paper: AGL Energy Limited, 4.
[1087] New Zealand Privacy Commissioner, *IPP 12 – Model clauses – template* (Web Page, accessed 27 May 2021).
[1088] GDPR (n 26) art 46.
[1089] Submissions to the Issues Paper: ANZ, 14; Australian Banking Association, 8.
[1090] *Privacy (International Money Transfers) Generalising Determination 2020* (Cth).
[1091] *Privacy Act* (n 2) ss 76–9.
[1092] Ibid, sch 1, APP 8.2(b).

Some submitters were of the view that the consent exception places an unfair expectation on consumers to understand the implications of disclosure and that if they consent to an overseas disclosure their personal information may not be subject to any privacy protections.[1093] The APP Guidelines note that consent is not required before every proposed cross-border disclosure, and an entity can obtain an individual's consent to disclose a particular kind of personal information for the same purpose on multiple occasions.[1094]

Removing the express consent exception could increase the regulatory burden on entities seeking to disclose personal information overseas. However the extent of reliance by business on this exception is unclear. Furthermore, the various proposals in this Chapter would make it easier for entities to fulfil their accountability obligations. In light of the concerns about the effectiveness of consent outlined in Chapter 9, retaining the consent exception would result in a disproportionate burden being placed on individuals to consider the risks to their privacy if their personal information were to be disclosed to an overseas recipient.

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

Question

- Would the other exceptions to APP 8.2, together with proposals such as creating a list of prescribed countries and binding schemes and introducing standard contractual clauses facilitate overseas disclosures of personal information in the absence of the informed consent exception?

Strengthen notice requirements

APP entities are currently required to give notice that they are likely to disclose an individual's personal information to an overseas recipient.[1095] Some submitters suggested that overseas disclosures should be supported by enhanced transparency requirements.[1096] The OAIC's guidance states that privacy notices could be used by entities to explain any practical effects or risks associated with the disclosure that the APP entity would reasonably be expected to aware of.[1097] In light of Proposal 8.2 to limit the amount of information in collection notices to improve individuals' comprehension of information relevant to a particular collection of personal information, the current requirement to state whether an APP entity is likely to disclose personal information to overseas recipients in APP 5.2(i) could be replaced with a requirement to provide more specific information about potential overseas disclosures in the APP privacy policy required under APP 1.

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.

Obligations apply only to 'disclosures'

APP 8 explicitly applies to 'disclosure' of personal information to overseas recipients rather than to 'transfers' or 'uses'. This means that APP 8 does not apply to the overseas movement of personal information if that movement is an internal use by the entity, rather than a disclosure.[1098] APP 8 is not intended to apply where personal information is routed through servers outside Australia.[1099]

[1093] Submissions to the Issues Paper: Australian Privacy Foundation, 42–3; Dr Kate Mathews Hunt, 13.
[1094] OAIC, APP Guidelines (n 21) 8.32.
[1095] *Privacy Act* (n 2) sch 1, APP 5.2(i)
[1096] Submissions to the Issues Paper: Electronic Frontiers Australia, 12; Shogun Cybersecurity, 5.
[1097] OAIC, APP Guidelines (n 21) 5.33.
[1098] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 83.
[1099] Ibid.

However, submissions raised concerns that the application of APP 8 to Cloud Service Providers is unclear.[1100] Submitters considered that it can be difficult to distinguish between a 'use' and a 'disclosure' as the terms are undefined, and recommended amending APP 8 to provide clarity.[1101]

OAIC guidance distinguishes between the concept of 'use' encompassing information handling and management activities occurring within an entity's effective control, and disclosure which occurs when an entity makes information accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.[1102] The focus is on the act done by the disclosing party, and not on the actions or knowledge of the recipient. An entity can 'disclose' personal information even where it is already known to the recipient. The release of personal information may be a proactive release, a release in response to a specific request, an accidental release or an unauthorised release by an employee.[1103]

The ALRC's report 108 noted that concerns about personal information being sent or held overseas appeared to be a 'visceral reaction and an existential anxiety' among the general public.[1104] Some submissions expressed concern that the application of APP 8 to 'disclosures' and not 'uses' does not cover the movement of personal information to an overseas cloud server, where data could be processed, stored or disposed of outside Australia.[1105] Some submitters were of the view that APP 8 and section 16C should apply to any movement of personal information outside Australia.[1106] This would be consistent with the approach adopted in the GDPR, which imposes obligations on all forms of data processing including storage.[1107] The Act's focus on overseas 'disclosures' is consistent with the approach adopted in the NZ Privacy Act.[1108]

A small number of submissions also expressed concern that the use of 'disclosure' rather than 'transfer' means there are no limits on international intra-company transfers of personal information, which allows transfers to countries with no data protection laws, without imposing any additional requirements to ensure compliance by the foreign office.[1109] The suggestion to extend APP 8 to overseas 'uses' or 'transfers' of personal information was supported by a view among some submitters that sending personal information overseas presents an inherent safety and security risk.[1110] These submissions noted that personal information transferred overseas could potentially be accessed by overseas governments, and that it could be more difficult for individuals to enforce privacy risks and access justice for overseas privacy infringements.[1111] Other submissions suggested that personal information is not inherently safer or more secure simply because it is stored in Australia.[1112] Submitters that took this view recommended amending the Act to clarify that data localisation is not required for APP entities to meet their obligations under APP 8.[1113]

[1100] Submissions to the Issues Paper: Australian Medical Association, 10–1; Commonwealth Department of Health, 10; Avant Mutual, 14; Communications Alliance, 12; Optus, 12; Palo Alto Networks, 4.
[1101] Submissions to the Issues Paper: CSIRO, 9; Roche, 8; Interactive Games and Entertainment Association, 18; Avant Mutual, 14.
[1102] OAIC, APP Guidelines (n 21) B.64, B.68.
[1103] Ibid B.64, B.65.
[1104] ALRC Report 108 (n 53) 125.
[1105] Submissions to the Issues Paper: Blancco, 64; CSIRO, 9; Australian Medical Association, 11.
[1106] Submission to the Issues Paper: Calabash Solutions, 10.
[1107] GDPR (n 26) art 4.
[1108] *Privacy Act 2020* (NZ) (n 29) Information Privacy Principle 12.
[1109] Submissions to the Issues Paper: Australian Privacy Foundation, 27; Blancco, 64.
[1110] Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 43; Dr Kate Mathews Hunt, 13.
[1111] Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 43; Dr Kate Mathews Hunt, 13.
[1112] Submissions to the Issues Paper: Global Data Alliance, 2; BSA – The Software Alliance, 9; ANZ, 15; Facebook, 44.
[1113] Submissions to the Issues Paper: Global Data Alliance, 2; BSA – The Software Alliance, 9; ANZ, 15; Facebook, 4; Information Technology Industry Council, 3; Palo Alto Networks, 4.

Proposal

Introduce a definition of 'disclosure'

Defining the concepts of 'use' and 'disclosure' in the Act, would assist with determining the application of APP 8 to overseas transfers of personal information and clarify that it does not apply to entities that provide personal information to secure Cloud Service Providers located overseas. Including a definition of disclosure in the Act would also assist with interpreting the Act's application in other contexts which reference 'disclosures' but not 'uses'.[1114]

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

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

A number of submitters were of the view that the current wording of APP 8 is overly subjective and expressed particular concern about the use of the phrase 'such steps as are reasonable in the circumstances'.[1115] Submissions noted that this language often leads to disputes about what measures entities must put in place to protect personal information.[1116] Submitters suggested the government should provide guidance on how to assess whether a potential overseas recipient of personal information will breach the APPs.[1117] A number of submissions suggested APP entities should be required to 'ensure' rather than 'take such steps as are reasonable in the circumstances to ensure' that an overseas recipient did not breach the APPs.[1118]

The APP Guidelines state that whether 'reasonable steps' requires a contract to be entered into, the terms of the contract, and the steps the APP entity takes to monitor compliance with any contract (such as auditing), will depend upon the circumstances including:

- the sensitivity of the personal information
- the entity's relationship with the overseas recipient
- the possible adverse consequences for an individual if the information is mishandled by the overseas recipient
- existing technical and operational safeguards implemented by the overseas recipient which will protect the privacy of the personal information, and
- the practicability, including time and cost involved. However, an entity is not excused from ensuring that an overseas recipient does not breach the APPs by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.

This proposal would elevate the factors in the APP Guidelines into the wording of APP 8 to assist entities in understanding what their obligations are before disclosing personal information overseas.

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

[1114] For example, the NDB scheme and APP 11.1(b).

[1115] Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 43; Minderoo Tech and Policy Lab – University of Western Australia School of Law, 20; Australian Privacy Foundation, 27; ANZ, 15.

[1116] Submissions to the Issues Paper: Information Technology Industry Council, 3; Palo Alto Networks, 4; Avant Mutual, 14; Association for Data-Driven Marketing and Advertising, 20; Experian, 22; Optus, 12; KPMG, 18.

[1117] Submission to the Issues Paper: AGL Energy Limited, 4–5.

[1118] Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 43; Minderoo Tech and Policy Lab – University of Western Australia School of Law, 21.

General Data Protection Regulation

The DPI report recommended that reforms to the Act have regard to whether the Act should be revised such that it could be considered by the European Commission to offer 'an adequate level of data protection' to facilitate the flow of information to and from overseas jurisdictions such as the EU.[1119] The Issues Paper sought feedback on the potential benefits and challenges of Australia seeking adequacy under the GDPR. Submissions that addressed GDPR generally expressed support for the framework and recommended that Australia should seek an adequacy decision from the European Commission.[1120]

Current transfers between Australia and the EU

Under the GDPR, personal information can only be transferred outside the EU to countries or organisations that provide an adequate level of privacy protection.[1121] In the absence of an adequacy decision from the European Commission, overseas transfers of personal information are permitted on the condition that individual rights under the GDPR are enforceable, and effective remedies are available to individuals.[1122] In addition, the transferring entity is required to comply with Article 46 of the GDPR, which outlines the safeguards that must be in place when transferring personal information to a country without an adequacy decision, such as Australia. Australian businesses may also be required to comply with the GDPR indirectly when entering into agreements with overseas entities that are subject to the GDPR.

The GDPR recognises contracts as a method of ensuring personal information transferred outside the EU is adequately protected.[1123] As Australia's privacy laws are not recognised as adequate by the EU, Australian businesses that wish to trade with organisations in the EU bear the costs of additional contractual arrangements, including the costs of periodic audits of compliance with these arrangements.[1124] Businesses bound by both the Act and the GDPR may be required to navigate inconsistent privacy protections that apply to the same collection, use or disclosure of personal information.

Benefits of seeking adequacy

Submissions noted that an adequacy decision would benefit Australian businesses as it would result in a reduction of regulatory costs associated with contractual provisions,[1125] and allow businesses to compete more effectively in international markets.[1126] As well as streamlining interactions with businesses trading in the EU,[1127] submitters were of the view that the GDPR is becoming the global standard for cross-border disclosures and that an adequacy decision could facilitate cross-border data flows more broadly.[1128] Submissions noted that an adequacy decision could serve as a

---

[1119] ACCC, DPI report (n 2) 36

[1120] Submissions to the Issues Paper: Griffith University, 18–9; Ramsay Health, 9; Centre for Cyber Security Research and Innovation, 11; Roche, 7; Karen Meohas, 13; Privacy 108, 15; Salesforce, 3; Association for Data-Driven Marketing and Advertising, 20; Law Council of Australia, 21; Fintech Australia, 12; Fastmail, 1; Business Council of Australia, 4; Data Republic, 64; Australian Information Security Association, 25; Gadens, 10.13; Interactive Games and Entertainment Association, 20; Australian Privacy Foundation, 31; Blancco, 65.

[1121] GDPR (n 26) art 45.

[1122] Ibid, art 46.

[1123] Ibid.

[1124] ALRC Report 108 (n 53) 1329.

[1125] Submissions to the Issues Paper: Griffith University, 19; Privacy 108, 15; Business Council of Australia, 4; AusPayNet, 12; Gadens, 10–3; Australian Privacy Foundation, 31–2; Association for Data-driven Marketing and Advertising, 20.

[1126] Submissions to the Issues Paper: Fintech Australia, 12–3; Interactive Games and Entertainment Association, 20; Australian Information Security Association, 24.

[1127] Submissions to the Issues Paper: Snap Inc, 5; Ramsay Health, 9; Centre for Cyber Security Research and Innovation, 11; ElevenM, 1; Salesforce, 3; Australian Financial Markets Association, 14; Business Council of Australia, 4; Western Union, 3; Experian, 23; Gadens, 11; Interactive Games and Entertainment Association, 19–20.

[1128] Submissions to the Issues Paper: Blancco, 65; Queensland University of Technology Faculty of Law, 23–4; Data Republic; 16; Gadens, 10.13; Interactive Games and Entertainment Association, 20; Australian Privacy Foundation, 31; illion, 6.

certificate of trust in Australia's privacy practices both national and internationally, and would increase the confidence of Australia's trading partners.[1129] The Issues Paper noted that of Australia's top 15 two-way trading partners in goods and services, only two were from the EU. However, some submitters suggested that when assessing the importance of data transfers, the value of goods traded may be an ineffective proxy.[1130] In addition, it is likely that one third of Australia's top 15 trading partners will soon be either a GDPR country or a country with GDPR adequacy.[1131] Some submitters suggested that without an adequacy decision, Australia is competitively disadvantaged when participating in global markets, potentially preventing technical innovation from entering Australia.[1132]

Challenges in seeking adequacy

Submissions noted that an adequacy assessment could require major legislative development across a range of laws,[1133] and that organisations would bear a regulatory cost in stepping up to GDPR standards.[1134] Openly Australia noted the regulatory landscape could become complex if Australia were to pursue GDPR adequacy alongside implementing CBPR, introducing a domestic certification scheme and requiring compliance with the Act.[1135] Telstra's submission suggested that consumers would be better served by amendments to the Act designed with Australia's unique regulatory, legal and cultural context in mind – rather than amendments made solely to achieve GDPR adequacy.[1136]

Barriers to adequacy

The decision to seek an adequacy assessment would depend on broader reforms to the Act. Proposals put forward in other chapters would more closely align the Act with some of the standards contained in the GDPR, however, barriers to GDPR adequacy could remain. While a formal EU adequacy decision would not require Australia's framework to mirror that of the GDPR,[1137] following the introduction of reforms which extended the Act to the private sector, the EU released an opinion expressing concern about the sectors and activities excluded from the protection of the Act and mentioned, in particular, the small business and employee records exemptions.[1138] Evidence given to the Senate Legal and Constitutional References Committee noted that the small business exemption was of particular concern to the EU and that it was likely the key outstanding issue between the EU and Australia.[1139]

[1129] Submissions to the Issues Paper: Snap Inc, 5; Griffith University, 19; Ramsay Health, 9; Salesforce, 3–4; Association for Data-Driven Marketing and Advertising, 20; Queensland University of Technology Faculty of Law, 24; Experian, 23; Australian Information Security Association, 25; Openly Australia, 5; OAIC, 116; Facebook, 45; Australian Privacy Foundation, 31–2.

[1130] Submissions to the Issues Paper: AusPayNet, 12; Interactive Games and Entertainment Association, 20.

[1131] Germany is bound by the GDPR, the United Kingdom, Japan and New Zealand have current adequacy determinations and the Republic of Korea is expected to have an adequacy decision formalised shortly.

[1132] Submissions to the Issues Paper: Fintech Australia, 12; Interactive Games and Entertainment Association, 19; OAIC, 116.

[1133] Submissions to the Issues Paper: Queensland University of Technology Faculty of Law, 24; Optus, 13; Facebook, 45.

[1134] Submissions to the Issues Paper: Gadens, 11; Optus, 13.

[1135] Submission to the Issues Paper: Openly Australia, 5.

[1136] Submission to the Issues Paper: Telstra and Telstra Health, 12.

[1137] GDPR (n 26) art 45(1).

[1138] Article 29 Data Protection Working Party, Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000 (Opinion, 26 January 2001).

[1139] Evidence provided by the Australian Government Attorney-General's Department; Commonwealth of Australia, Parliamentary Debates, Senate Legal and Constitutional References Committee, 19 May 2005, 63 (C Minihan).

23. Cross-Border Privacy Rules and domestic certification

The Issues Paper sought feedback on the challenges of implementing the CBPR system in Australia. Submitters were generally supportive of the continued implementation of the CBPR system,[1140] and were of the view that the system could provide a mechanism to facilitate further cross-border data flows and deliver trade benefits across APEC economies.[1141]

Overview of the CBPR system

The APEC CBPR system is a regional certification scheme that operates as a mechanism for businesses to safeguard the free flow of data while protecting the privacy rights of individuals.[1142] The CBPR system is a voluntary certification scheme which assesses business' personal information handling practices in relation to notice, collection, use, choice, integrity and security of personal information, access, correction and accountability against a set of CBPR privacy standards (known as CBPR program requirements).[1143] Entities seeking certification must submit to an audit of their privacy practices and procedures by an APEC-certified Accountability Agent. The scope of the certification is flexible and may cover the operations of an entire organisation, or a particular data type or business process. Accountability Agents also provide privacy dispute resolution services to certified businesses and consumers if a privacy complaint is made against a business that has been certified in Australia. Any unresolved privacy complaints would ultimately be regulated by the IC.

APEC endorsed Australia's application to participate in the CBPR system in November 2018. The other participating economies are the United States of America, Mexico, Canada, Japan, Republic of Korea, Singapore, Chinese Taipei and the Philippines. The US, Japan and Singapore are the only economies that have fully implemented the system domestically.

Benefits of the CBPR system

The CBPR system is intended to enhance consumer trust that certified businesses will handle data responsibly, and to provide dispute resolution services through a nominated Accountability Agent if an issue arises. Of Australia's top 15 two-way trading partners in goods and services (2019), 12 were from the APEC region. During that period, APEC economies accounted for approximately 73 per cent of trade.[1144] As a majority of Australian trade is undertaken within the APEC region, it makes sense to offer Australian businesses the opportunity to participate in a system which assures the reciprocal protection of privacy within and between businesses operating in APEC region economies.
In so doing, consumer trust may be enhanced and participating businesses can build on this trust to enhance their economic and reputational position in the ever increasing regional digital economy. It would also enable Australian businesses to enter more streamlined contractual arrangements when sharing data with another CBPR-certified businesses.

What is needed to implement the CBPR system in Australia?

The CBPR system would be implemented through the development of an APP code as the mechanism for ensuring the CBPR program requirements are enforceable. The code would apply to businesses with CBPR certification. Small businesses not covered by the Act that wish to participate in the CBPR system would need to opt-in to the Act before applying for certification. The code would incorporate the CBPR system program requirements, while ensuring interoperability with the APPs.

[1140] Submissions to the Issues Paper: Information Technology Industry Council, 3; Calabash Solutions, 10; United States Chamber of Commerce, 4; Salesforce, 3; Openly Australia, 3; Workday, 4; Business Council of Australia, 4; DIGI, 12, Interactive Games and Entertainment Association, 18–9.
[1141] Submissions to the Issues Paper: Calabash Solutions, 10; Openly Australia, 3; Workday, 4; Business Council of Australia, 4; Interactive Games and Entertainment Association, 18–9.
[1142] APEC, APEC Privacy Framework (Report, 2015) 30.
[1143] APEC, Cross-Border Privacy Rules System Program Requirements (Report, November 2019).
[1144] Australian Government – Department of Foreign Affairs and Trade, Composition of Trade – Australia – 2018-19 (Report, January 2020).

The code developer would be responsible for consulting with businesses and industry and working with the OAIC to finalise the code for registration.

There are currently no Accountability Agents operating in the Australian market. To be accredited by APEC, an Accountability Agent must have either a location in the APEC member economy or be subject to the jurisdiction of the relevant privacy regulator. It is anticipated that prospective Accountability Agents could be third party assessment organisations (such as accountancy or consulting firms) or an International Organisation for Standardisation certification body. The Joint Oversight Panel (JOP) administers the CBPR system. Decisions about an organisation's eligibility to be an Accountability Agent are informed by the JOP but ultimately made by APEC economies.

Challenges in implementing the CBPR system

Submissions recognised a number of challenges to implementation, including a limited understanding of the CBPR system within industry,[1145] the costs and resources required for businesses to participate,[1146] the limited adoption of the CBPR system internationally (at both the jurisdictional and organisational level)[1147] and difficulty associated with encouraging organisations to become Accountability Agents.[1148]

The OAIC's submission noted that under the current provisions, the development of a code would require the IC to identify a code developer, who would then be responsible for developing the code and ensuring that it adequately gives effect to the requirements of the CBPR system. The code developer would also be required to ensure appropriate consultation took place with relevant stakeholders, including the public and the OAIC.

The OAIC's submission expressed concern about the potential difficulty in identifying an appropriate entity to develop a CBPR code since it would need to be able to apply to a broad range of entities. Code developers are required to be generally representative of the entities to which the code will apply,[1149] and it may be challenging to identify a code developer that is sufficiently representative. The OAIC's submission recommended that the IC be authorised to draft a CBPR code in the first instance.[1150] Proposal 3.1 (discussed in Chapter 3) to amend the code-making power to allow the IC to draft an APP code on the direction of the Attorney-General, if implemented, could be utilised in the event that a suitable industry representative cannot be identified to develop the code.

Proposed model

Australia's implementation of the CBPR system would involve one or more entities becoming accredited Accountability Agents that would certify businesses as being compliant with the CBPR program requirements on a fee for service basis. The fees charged by Accountability Agents would be market driven and not regulated by government. Accountability Agents would also provide privacy dispute resolution services to certified businesses and consumers if a privacy complaint has been made against a business that has been certified under the CBPR system in Australia. Any unresolved privacy complaints would ultimately be regulated by the OAIC.

23.1 Continue to progress implementation of the CBPR system.

[1145] Submissions to the Issues Paper: Salesforce, 3; Experian, 23; Privacy108, 15.
[1146] Submissions to the Issues Paper: Experian, 23; Roche, 9; Australian Information Security Association, 24; Gadens, 2.
[1147] Submissions to the Issues Paper: Roche, 9; Privacy108, 15; Western Union, 3; Australian Financial Markets Association, 13.
[1148] Submissions to the Issues Paper: OAIC, 117; Openly Australia, 2.
[1149] OAIC, Guidelines for developing codes – issued under Part IIIB of the Privacy Act 1988, (Web page, September 2013) 12.
[1150] Submission to the Issues Paper: OAIC, 104.

Questions

- What benefits would CBPR certification have for Australian businesses?
- Would there be a benefit in the CBPR system being expanded beyond APEC to include countries beyond the APEC region?
- Would Australian businesses (both APP entities and businesses not covered by the Act) be interested in obtaining CBPR certification on a fee for service basis? That is, paying annual certification fees to an Accountability Agent?
- What organisations may be suitable to be accredited as an Accountability Agent?
- What organisations may be suitable to develop or assist with developing a CBPR code?

Domestic privacy certification

The DPI report recommended the government consider introducing an independent certification mechanism to monitor and demonstrate the compliance of particular APP entities collecting, using and disclosing a large volume of personal information.[1151] The Issues Paper sought feedback on whether it would be beneficial to develop a domestic privacy certification scheme in addition to implementing the CBPR system. There were mixed views among submitters as to the potential value of a domestic certification scheme. This is consistent with feedback received by the ACCC when the proposal was considered in the DPI report.[1152]

Benefits of introducing a domestic privacy certification scheme

Some participating economies in the CBPR system maintain domestic certification schemes alongside the CBPR, including Singapore's Data Protection Trustmark Certification and Japan's PrivacyMark. NZ also has a domestic privacy certification scheme. These schemes differ in their nature, scope and requirements but ultimately enable entities that meet certification criteria to display a 'seal' or 'trustmark' as evidence of certification. GDPR also makes provision for the introduction of data protection certification mechanisms, including data protection seals and marks, at both the member-state level and at the EU level for the purposes of demonstrating compliance with the requirements of the GDPR.[1153] However, there are no EU approved certification criteria or accredited bodies for GDPR certification.

The OAIC's submission noted that internationally recognised privacy certification schemes can play a role in facilitating overseas transfers of personal information, but that an independent domestic certification scheme could also significantly increase the transparency of organisations' data practices by enabling Australians to quickly assess the level of data protection offered by an APP entity.[1154] The OAIC also considered that an independent third-party certification scheme could assist in ensuring that regulated entities are meeting their obligations under the Act without the need to substantially increase regulatory action.[1155] The DPI report also noted that an independent domestic certification mechanism could address issues arising from consumers not reading or being able to understand digital platforms' privacy policies by outsourcing the potentially complex and time-consuming assessment to a qualified and independent third-party.[1156]

A number of submissions supported the introduction of a voluntary domestic certification scheme, suggesting that a domestic certification scheme would provide companies with a mechanism for demonstrating their compliance with Australian privacy laws.[1157] Submissions also suggested that having an independent assessment of an entity's privacy controls could increase consumer

[1151] ACCC, DPI report, (n 2) 480.
[1152] Ibid 480-481.
[1153] GDPR (n 26) arts 42, 43; rec 100.
[1154] Submission to the Issues Paper: OAIC, 103–4.
[1155] Ibid.
[1156] ACCC, DPI Report (n 2) 480.
[1157] Submissions to the Issues Paper: Avant Mutual, 14; Calabash Solutions, 10; Gadens, 2; illion, 6–7; Information Technology Industry Council, 3; OAIC, 107; Openly Australia, 3-4.

confidence and that certified businesses could gain a competitive advantage by differentiating themselves from uncertified businesses.[1158] This could potentially be beneficial for small businesses that choose to opt-in to the Act, as it could provide them with a mechanism to advertise this to consumers. Illion's submission noted that certification could provide businesses with certainty that potential suppliers were compliant with the Act which would reduce the time and cost expended to validate capabilities of suppliers while also providing a mechanism to demonstrate compliance to customers.[1159]

Challenges in introducing a domestic privacy certification scheme

A small number of submitters were of the view that there is limited merit to developing a domestic certification, stating that mechanisms such as privacy seals, badges and certification have had limited success overseas.[1160] The Australian Privacy Foundation submitted that overseas certification schemes had resulted in circumstances where individuals were misled that their personal information was safe.[1161] Submissions also noted that having multiple certification and enforcement regimes could create further complexity, mistrust and enforcement 'red tape' that could function contrary to the intended benefits of a certification scheme, and that a certification scheme would need to provide demonstrable benefits and avoid duplication with CBPR.[1162]

Proposal – introduce a domestic certification model

Submissions suggested that any domestic certification scheme should be voluntary,[1163] and should be flexible and scalable by allowing entities to seek enterprise-wide certification for all of its operations, or certification for specific products, data types or business processes.[1164] Submitters also recommended that the scheme should be interoperable with CBPR and other domestic schemes to minimise fragmentation and burden on entities.[1165]

Certification guidelines issued by the European Data Protection Board state that certification criteria should be:

- uniform and verifiable
- auditable in order to facilitate the evaluation of processing operations under the GDPR
- relevant to the business model of different entities (for example business to business and business to customer)
- interoperable with other certifications where appropriate, and
- flexible and scalable for application to different types and sizes of organisations.[1166]

The OAIC's submission stated it would be preferable for an independent third party to administer the scheme to ensure the functional independence of the OAIC in light of its enforcement role. This view was supported by other submitters.[1167] The OAIC suggested considering whether there is a current government body that could undertake the certification function and that the OAIC should be identified as the scheme's regulator for privacy breaches.[1168]

[1158] Submissions to the Issues Paper: Calabash Solutions, 10; OAIC, 103.
[1159] Submission to the Issues Paper: illion, 6–7.
[1160] Submissions to the Issues Paper: Privacy108, 14–5.
[1161] Submission to the Issues Paper: Australian Privacy Foundation, 30–1.
[1162] Submission to the Issues Paper: IGEA, 19.
[1163] Submissions to the Issues Paper: Calabash Solutions, 10; Facebook, 44–5; IGEA, 19; Information Technology Industry Council, 3; OAIC, 104, 107; Global Data Alliance, 3.
[1164] Submissions to the Issues Paper: Information Technology Industry Council, 3; Calabash Solutions, 10; illion, 6–7.
[1165] Submissions to the Issues Paper: Information Technology Industry Council, 3; OAIC, 105.
[1166] European Data Protection Board, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation (Web page, June 2019).
[1167] Submissions to the Issues Paper: Australian Privacy Foundation, 31; Law Institute of Victoria, 21; Openly Australia, 3–4.
[1168] Submission to the Issues Paper: OAIC, 105–7.

The OAIC's submission supported a model adopted by the UK ICO which could be implemented for a domestic privacy certification scheme. The UK certification framework involves:

- the ICO publishing accreditation requirements for certification bodies to meet
- the UK's national accreditation body, UKAS, accrediting bodies and maintaining a public register of accredited certification bodies
- the ICO approving and publishing certification criteria for use by certification bodies
- accredited certification bodies issuing certification against those criteria, and
- data controllers and data processors applying for certification and using it to demonstrate compliance with UK data protections laws.

The proposed Australian domestic certification scheme would draw from both the UK and the CBPR certification models. The OAIC would develop assessment criteria for use in accrediting certification agents. Private sector organisations would apply to the OAIC to be accredited as certification agents. Businesses wishing to be certified as compliant with the Act would apply for certification from an accredited certification agent. It is anticipated that an accredited certification agent for the domestic scheme would also be an Accountability Agent for CBPR certification. However, under the domestic certification scheme, a certification agent would not be required to handle complaints about businesses with domestic certification. These complaints would be made directly to the OAIC.

A domestic certification scheme would operate on a 'cost recovery' basis so that businesses would pay certification agents a certification fee and certification agents would pay the OAIC an accreditation fee. The DPI report noted that a privacy certification would need to be carefully designed to avoid the conflict of interest that could arise where third-party certification bodies receive payment for certification by the entities they are assessing for certification.[1169] To address this concern, the proposed model would require certification agents to be re-accredited by the OAIC at regular intervals (12 to 24 months). Businesses would also be required to be re-certified at similar intervals.

The OAIC would have oversight over the domestic certification scheme as the accrediting body and the enforcing regulator. It would also have the ability to audit certification agents to ensure they were undertaking appropriate assessments of businesses seeking to be certified. A privacy certification would not preclude the OAIC from investigating or taking action against a business that was certified under the scheme, however, as suggested by the OAIC, certification would be an element that could be used to help demonstrate compliance.[1170]

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

Questions

- Would Australian businesses (both APP entities and businesses not covered by the Act) be interested in obtaining domestic certification scheme based on the requirements of the Act, alongside CBPR certification?
- Would Australian businesses be more interested in pursuing domestic certification, CBPR certification or both?
- How could the certification process be streamlined for businesses interested in pursuing both forms of certification?

[1169] Submissions to the ACCC DPI: Australian Privacy Foundation, 5; UN Special Rapporteur on the Right to Privacy, 7–8.
[1170] Submission to the Issues Paper: OAIC, 103–7.

Part 3: Regulation and enforcement

24. Enforcement

The current framework of the Act places a strong emphasis on the IC attempting to resolve complaints by conciliation and, failing that, making binding determinations against APP entities including determinations for compensation and costs.

Accordingly, the OAIC has historically focused on resolving complaints. However, the scale and sophistication of the use of personal information by APP entities raises the question about whether there is a need for the OAIC's regulatory capacity to be enhanced so that it can take more proactive enforcement of privacy standards and provide greater education and guidance for regulated entities and the public on how the Act applies.

The Issues Paper asked whether the current enforcement framework for interferences with privacy is working effectively. It asked whether the right balance is being struck between conciliating complaints, investigating systemic issues, and addressing serious non-compliance. It also asked whether the IC requires additional enforcement mechanisms and if so, what those mechanism should look like.

Civil penalty provisions

A tiered approach to civil penalties and infringement notices

Currently, the Act does not contain any penalty provisions for interferences with privacy that are not serious or repeated. The IC may only make a determination requiring an APP entity to take certain actions or pay compensation or accept an enforceable undertaking from an entity such as where the respondent has cooperated with the IC's investigation. Submissions suggested the OAIC requires a broader range of enforcement powers and remedies to appropriately respond to breaches.[1171] Some submitters noted the current lack of penalties for organisations that have a history of ongoing, but relatively minor, non-compliance with the Act.[1172]

The OAIC recommended introducing civil penalties for interferences with privacy (rather than only for serious or repeated interferences).[1173] Maurice Blackburn suggested the IC should have a suite of measures to address varying but serious interferences with privacy. It recommended introducing civil penalties for interferences with privacy or a 'course of conduct' that gives rise to an interference with privacy (similar to the penalty regime under the Fair Work Act).[1174]

Under section 155 of the DP Act, the UK ICO can issue a penalty notice to a person who has failed to comply with many provisions of the DP Act and the GDPR including the principles of processing, rights of the data subject, and obligations of controllers and processors.[1175] There is no seriousness threshold but, when deciding whether to give a penalty notice, the UK ICO must have regard to certain matters including the nature, gravity and duration of the failure.[1176] Persons can appeal a

[1171] Submission to the Issues Paper: Adobe, 12.
[1172] Submission to the Issues Paper: Energy and Water Ombudsman NSW, 2.
[1173] Submission to the Issues Paper: OAIC, 126–9.
[1174] Submission to the Issues Paper: Maurice Blackburn, 8.
[1175] *Data Protection Act* (UK) (n 37) ss 155, 149. The IC can issue a penalty notice under s 155 where he or she is satisfied a person has failed or is failing as described under section 149(2), (3), (4) or (5) or where the person has failed to comply with an information notice, an assessment notice, or an enforcement notice. Some of the provisions for which a penalty notice can be issued under s 149(2) include: a provision of Chapter II of the GDPR (n 26) or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing); a provision of Articles 12 to 22 of the GDPR or Part 3 or 4 of this Act conferring rights on a data subject and a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors).
[1176] Ibid, sub-s 155(3).

penalty notice at the Tribunal.[1177] As an example of the use of these powers, in October 2020 the UK ICO issued a penalty notice to British Airways, fining the company £20 million.[1178]

Proposal

There is merit in increasing the spectrum of enforcement mechanisms available to the IC. This could be achieved through introducing two additional categories of civil penalty provisions that cover less serious conduct than that under existing section 13G. The first would be to create a new mid-tier civil penalty for any interference with privacy with a lesser maximum penalty amount than for section 13G.

The benefit of a mid-tier civil penalty provision is that it would be a stronger deterrent than a determination because the court would be able to order an APP entity pay a pecuniary penalty. Whilst the OAIC would exercise discretion in determining when to use this civil penalty provision, it would give the OAIC a greater range of enforcement tools to ensure the range of interferences may be responded to appropriately. This provision would bridge the current gap between an IC-issued determination and the higher civil penalty for a serious or repeated interference.

For example, the OAIC might use the mid-tier civil penalty provision where an APP entity has collected more personal information than reasonably necessary for the entity's functions and also did not take reasonable steps to protect this personal information from unauthorised access. The APP entity has then been targeted in a cyber-attack in which personal information about many individuals was accessed without authorisation. The APP entity notified the OAIC of the data breach as soon as they became aware of it.

The OAIC may be limited in its ability to initiate court proceedings where the conduct is likely to fall short of the 'serious' or 'repeated' threshold for the s 13G civil penalty provision. However, a determination may not provide adequate deterrence because the OAIC is unable to impose a pecuniary penalty. It may also be impossible to identify which individuals' personal information was accessed and misused in which case the determination also could not include a requirement for the entity to pay compensation to affected individuals. The determination could only require the entity to take steps to ensure it no longer collected unnecessary amounts of personal information and improved its information security practices, but the entity would not be exposed to any cost by way of paying compensation or a fine.

The second new category of civil penalty provisions would be to create a series of low-level civil penalty provisions under certain APPs for administrative breaches of the APPs with attached infringement notice powers for the IC. These would have a lower maximum penalty than the other two civil penalty provisions. For example, an infringement notice could attach to a civil penalty provision under APP 1.3 for failing to have a privacy policy.

An infringement notice gives the person to whom the notice is issued the option to pay a fine in full as an alternative to prosecution for an offence or litigation of a civil matter in court. Infringement notice powers are appropriate where enforcement officers can make assessments based on straightforward and objective criteria. They are typically used for administrative failing by entities which do not require an evaluative judgment on the part of the enforcer.[1179]

There is precedent for regulators to have infringement notice powers. ASIC, the ACCC, the eSafety Commissioner and the Work Health and Safety Commissioner all have infringement notice powers.

[1177] Ibid, s 162.

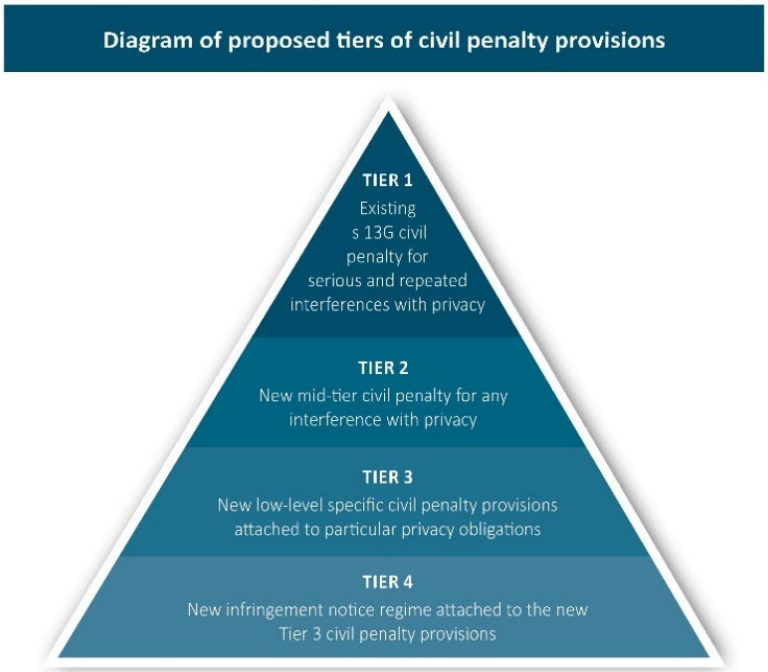
[1178] UK ICO, *ICO fines British Airways £20m for data breach affecting more than 400,000 customers*, (Web Page, 2021).

[1179] AGD, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, (Web Page, 2013) 57; ALRC, 'Principled Regulation – Federal Civil & Administrative Penalties in Australia' (Report No 95, March 2003), 439; Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, (Final Report, February 2019), 439.

Under the OP Bill,[1180] the IC will be empowered to issue an infringement notice when an APP entity fails to give information to the IC when required to do so under the Act, which the entity could elect to pay, instead of the matter being heard by a court.

The OAIC's submission recommended introducing infringement notices for interferences with privacy as a faster and more cost-efficient means of deterrence for less serious misconduct. It would encourage compliance with the Act by ensuring that minor and straightforward breaches of the Act could be addressed without placing too great a cost and time burden on the OAIC, APP entities or the courts. Submissions supported giving the IC the proposed infringement notice powers, particularly for companies that do not respond promptly in an investigation.[1181] The Cyber Security Cooperative Research Centre noted that 'providing the option to pay a fine as an alternative to prosecution for an offence or litigation of a civil matter in court would help mitigate against a backlog of cases and assist the IC to use the resources of the OAIC more effectively'.[1182]

Figure 24.1 Proposed tiers of civil penalty provisions



It is not considered appropriate to attach an infringement notice regime to the proposed broader mid-tier civil penalty for any interference with privacy. It is also important to note the OAIC would continue to use discretion in the exercise of its powers and entities would not necessarily be exposed to a penalty for any breach without regard to the circumstances. The OAIC should only issue an infringement notice where they are prepared to pursue the matter in court should the respondent choose not to pay.

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.

The 'serious' or 'repeated' civil penalty

Currently, section 13G of the Act is a civil penalty provision which applies if an APP entity engages in an act or practice that is a 'serious' or 'repeated' interference with privacy. An APP entity will only contravene this provision if it engages in a serious interference with an individual's privacy, or if it

[1180] Exposure Draft, OP Bill (n 1).
[1181] Submissions to the Issues Paper: Cyber Security Cooperative Research Centre, 12; Facebook, 45.
[1182] Submission to the Issues Paper: Cyber Security Cooperative Research Centre, 12.

repeatedly does an act or engages in a practice that is an interference with the privacy of one or more individuals. 'Serious' and 'repeated' are not defined in the Act and there have been no decided cases under this provision. The OAIC's litigation against Facebook which is currently before the Federal Court is the first time the OAIC has brought a proceeding under this provision.[1183]

Proposal

There could be benefit in clarifying some aspects of the threshold. For example, the threshold could more clearly express that breaches affecting a large number of individuals without affecting any one individual seriously can be subject to this civil penalty provision. Section 13G could more clearly capture breaches involving:

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

The benefit of more clearly identifying the type of conduct captured is that it would increase clarity for the OAIC, APP entities, and the courts.

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

OAIC powers: assessments, investigations and inquiries

Submitters indicated support for a more proactive regulatory model to better protect individuals' privacy, particularly in their capacity as consumers.[1184] This would require the OAIC to undertake more systematic audits and investigations.[1185]

Enhance assessment powers

The IC can currently conduct assessments of an entity's compliance with the Act, even in the absence of a breach of the Act or a complaint having been made. An assessment provides a professional, independent and systematic appraisal of how well an agency or organisation (or discrete part of an agency or organisation) complies with all or part of its privacy obligations.[1186] The Act states the IC may conduct the assessment in such manner as the IC considers fit but does not confer specific assessment related powers on the IC.[1187] Despite this power, entities can decline to cooperate with an assessment.

Submitters noted that assessments are a valuable regulatory and educative tool to identify emerging privacy issues and minimise breaches, and recommended the OAIC use its assessment powers more frequently.[1188] Dr Kate Mathews Hunt noted that the Act would be better enforced by the regulator conducting more frequent audits, particularly targeting organisations or industries with a history of ongoing minor breaches.[1189] The OAIC should audit several companies in a sweep to gain better understanding of industry practices and performance.[1190] The Association for Data-Driven Marketing and Advertising noted if the proposed increase in penalties is to have the desired deterrent effect, the OAIC would need to conduct more compliance audits.[1191] Giving the OAIC greater ability to

[1183] Submission to the Issues Paper: Cyber Security Cooperative Research Centre, 11.
[1184] Submission to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 44.
[1185] Submissions to the Issues Paper: Association for Data-driven Marketing and Advertising, 21; Dr Kate Mathews Hunt, 13.
[1186] OAIC, *Privacy Assessments*, (Web Page, 2021).
[1187] *Privacy Act* (n 2) sub-s 33C(2).
[1188] Submission to the Issues Paper: Association for Data-driven Marketing and Advertising, 21.
[1189] Submission to the Issues Paper: Dr Kate Mathews Hunt, 13.
[1190] Ibid.
[1191] Submission to the Issues Paper: Association for Data-driven Marketing and Advertising, 21.

initiate proactive audits would put more pressure on APP entities to better manage how they collect, use and disclose personal information which would minimise the number of actual breaches and reduce exposure to privacy harm.[1192] Blancco also recommended frequent audits to ensure the APPs are followed throughout the entire technology development process.[1193]

To assist the IC conduct assessments, the OP Bill[1194] will give the IC a new information-gathering power for the purposes of conducting an assessment, of any kind. The IC would be able to issue a notice to produce information or a document relevant to the assessment, subject to safeguards.[1195] Giving the OAIC these monitoring powers will enable it to better audit entities to ensure compliance with the requirements of the Act. The OP Bill also gives the Minister a new ability to request the IC conduct an assessment of whether a social media service is maintaining and handling personal information of children in accordance with a registered OP code.

Enhance investigation powers

The Association for Data-driven Marketing and Advertising suggested giving the OAIC more investigative powers to proactively audit and investigate entities such as those under the CPRA.[1196] Adobe agreed that the OAIC needs powers and resources to conduct investigations.[1197]

When conducting investigations, the IC's current powers include:

- to make such inquiries as she thinks fit, including by holding a hearing[1198]
- to be given information and documents by issuing a written notice on the entity[1199]
- to examine witnesses on oath or affirmation[1200]
- to direct a person to attend compulsory conference[1201]
- to conduct a compulsory conference[1202]
- to refer matters to other authorities, and[1203]
- to enter premises and inspect relevant documents by consent or with a warrant.[1204]

The OAIC's submission recommended that the power under section 68 to enter a premises with a warrant should expressly permit the IC to make copies of information and documents specified in the warrant. It also recommended that the OAIC be given explicit power to operate electronic materials to determine whether the kinds of information and documents specified in the warrant are accessible. The OAIC's submission also recommended the IC should have the power to seek a warrant to preserve or secure information and documents where there is a possibility that a person may destroy such materials or cause them to be unavailable for use in an investigation. The OAIC also recommended that it be an offence to destroy evidence that may be reasonably required by the IC.[1205]

[1192] Ibid.
[1193] Submission to the Issues Paper: Blancco, 69.
[1194] Exposure Draft, OP Bill (n 1).
[1195] See *Privacy Act* (n 2) s 33C which only states the IC may conduct an assessment.
[1196] Submission to the Issues Paper: Association for Data-driven Marketing and Advertising, 21; CPRA (n 120). Note, the CPRA will come into effect in 2023.
[1197] Submission to the Issues Paper: Adobe, 12.
[1198] *Privacy Act* (n 1) s 43.
[1199] Ibid s 44.
[1200] Ibid s 45.
[1201] Ibid s 46.
[1202] Ibid s 47.
[1203] Ibid s 50.
[1204] Ibid s 68. Note s 2B of the *Acts Interpretation Act* (n 104) defines 'document' broadly including anything on which there is writing or from which writings can be reproduced with or without the aid of anything else.
[1205] Submission to the Issues Paper: OAIC, 128 (Recommendation 50).

The ACCC currently has these investigation powers. Where an inspector or executing officer has entered premises with consent or under a search warrant, they have the power to make copies of evidential material and operate electronic equipment to see whether the evidential material is accessible.[1206]

Proposal

To enhance the OAIC's investigation powers the Act could be amended to give the IC the investigation powers listed in Part 3 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) (Regulatory Powers Act).[1207] The investigation powers under the Regulatory Powers Act create a framework for gathering material that relates to the contravention of civil penalty provisions where the civil penalty provision is made subject to investigation under Part 3 of the Regulatory Powers Act.

This includes powers for an authorised person to exercise general investigation powers which would give the IC additional powers including to:

- search premises for evidential material[1208]
- make copies of information and documents specified in a warrant[1209]
- operate electronic materials to determine whether the kinds of information and documents specified in a warrant are accessible, and[1210]
- seize evidential material and other things (which would prevent the destruction of evidence).[1211]

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.

Introduce inquiry powers

Data Synergies suggested the OAIC should be enabled to conduct 'wide ranging and open-ended policy and industry reviews' such as those undertaken by the ACCC.1212 While the IC may conduct assessments into the information handling practices of APP entities, the IC does not currently have the power to undertake a public inquiry into specified industries or acts or practices. This is inconsistent with comparable regulators such as the ACCC and the AHRC. The benefit of giving the OAIC this power would be to allow the OAIC to more proactively identify widespread industry practices which are not meeting the standards set by the Act and to consult widely on the issues. Such inquiries can be conducted publicly, giving the Australian community an opportunity to share a wide variety of views to give a comprehensive insight into the situation. This would enable the OAIC to provide a report to the Minister so that government may consider whether legislative or other reforms are needed.

Proposal

The Act could be amended to enable the OAIC to conduct public inquiries and reviews as directed by or subject to Ministerial approval. It would be modelled on the inquiry powers of the ACCC[1213] and

[1206] *CCA* (n 67) ss 154E, 154G.
[1207] *Regulatory Powers (Standard Provisions) Act 2014 (Cth)* (Regulatory Powers Act).
[1208] Ibid ss 49(a) and (b).
[1209] Ibid s 49(d).
[1210] Ibid s 50.
[1211] Ibid sub-ss 49(b)(ii) and s 52.
[1212] Submission to the Issues Paper: Data Synergies, 6.
[1213] *CCA* (n 67) s 95H.

the inquiry and review functions of the AHRC.[1214] This power would involve the ability to take evidence and require the production of documents but would not extend to a hearing power.

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

Question

- Would each of the enhanced regulatory powers described above assist the OAIC to be a more proactive regulator and encourage better levels of compliance with the Act?

Determinations

Proactive requirement to mitigate damage

Currently the IC lacks the power to require an APP entity to take action to identify and mitigate reasonably foreseeable risks or losses to individuals that may result from an interference with privacy. This includes the risk of information being published for sale on the dark web or of identity theft or fraud occurring because of the incident.

Proposal

The OAIC recommended the IC be given the power to require an APP entity to perform a reasonable act or course of practice to identify, mitigate and redress reasonably foreseeable loss or damage in addition to actual loss or damage suffered by individuals. For example, this could include requiring the entity to pay a reputable provider for credit monitoring services to monitor whether information that is the subject of the breach has been used for identity theft or fraud for a certain time period after the incident.[1215] This amendment would be consistent with the protective intent of existing paragraph 52(1)(b)(ii) and 52(1A)(c) but require the APP entity to be more proactive following a breach to identify reasonably foreseeable consequences of a breach and take reasonable steps to mitigate these.

Allowing the OAIC to require entities who have interfered with an individual's privacy to take reasonable steps to ensure the individual does not suffer loss or damage in the *future* could be a useful tool for proactive regulation. However, the Review is interested in views on what would or would not be reasonable action to take. The OP Bill also contains amendments that will further enhance the types of determinations the IC can make at the conclusion of an investigation.[1216]

24.5 Amend paragraph 52(1)(b)(ii) and 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined:

> a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals.

Question

- Is the proposal to allow the OAIC to require an entity to take reasonable steps to prevent future loss occurring reasonable?

[1214] The Australian Human Rights Commission (AHRC) has conducted inquiries, such as the Respect@Work: Sexual Harassment National Inquiry Report, pursuant to its statutory functions including s 11(1)(g) of the AHRC Act to promote an understanding and acceptance, and the public discussion, of human rights in Australia. The AHRC also conducts reviews under this same function such as its current independent review into Gymnastics in Australia. Sections 13 and 14 of the AHRC Act allow the Commission to hold inquiries in such manner as it thinks fit. In exercising the Commission's functions relating to human rights, the Commission has the power to obtain information and documents (s 21) and to examine witnesses (s 22).

[1215] Submission to the Issues Paper: OAIC, 127.

[1216] Exposure Draft, OP Bill (n 1).

Range of available Federal Court orders in a civil penalty proceeding

Where the IC has been successful in a civil penalty proceeding under section 13G of the Act, the Federal Court has the power to make an order for the respondent to pay a pecuniary penalty.[1217] The Act does not allow the Federal Court to make any order it sees fit after determining there has been a serious or repeated interference with privacy in a section 13G civil penalty proceeding.

In contrast, under a section 52 determination, the IC can require a respondent to:

- take steps to ensure such conduct is not repeated or continued
- take action to redress the complainant's loss or damage,
- pay the complainant compensation.

If the respondent refuses to comply with a section 52 determination, the IC or complainant may apply to the Federal Court to enforce the determination under section 55A. If the Court is satisfied there has been an interference with the complainant's privacy, it can make any order it sees fit.[1218]

Sections 25 and 25A of the Act allow a person who has suffered loss or damage because of a contravention of the Act to apply to the Federal Court or Federal Circuit Court for a compensation order after a civil penalty order has been made or the entity has been found guilty of an offence. However these provisions specifically exclude such compensation orders to be made after a civil penalty order for a contravention of section 13G.

This means that even after the Court has determined that a respondent has engaged in a serious or repeated interference with a complainant's privacy under section 13G, unless the IC makes a section 52 determination requiring the respondent to pay compensation, the complainant will not be compensated, nor will the respondent be required to take action to redress the complainant's loss or damage or ensure the conduct is not repeated or continued.

Proposal

The OAIC recommended providing the Federal Court with express statutory power to make conduct orders after determining there has been an interference with privacy in the context of a civil penalty proceeding. This would allow the court to make the same types of conduct orders which are available to the IC through a section 52 determination.

This proposal would be more efficient than the current model in which the IC may potentially be required to make two separate applications to the Federal Court: one for a pecuniary penalty for the section 13G civil penalty provision, and the other under section 55A to enforce a determination requiring the respondent to engage in certain conduct or pay compensation.

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.

Question

- Is it necessary and appropriate to give the Federal Court the express power to make any orders it sees fit or should the amendment only enable the Federal Court to make compensation orders in addition to an order imposing a pecuniary penalty?

[1217] *Privacy Act* (n 2) s 80U provides that each civil penalty provision is enforceable under Part 4 of the Regulatory Powers Act (n 1207). Section 82 of the Regulatory Powers Act enables the Court to make an order for a person to pay a pecuniary penalty.
[1218] *Privacy Act* (n 2) sub-s 55A(2).

Fund the OAIC through an industry funding arrangement

The majority of submissions recognised the OAIC requires adequate funding, staffing, and support (along with a regular review of its resourcing) to enable it to fulfil its wide-ranging responsibilities to the necessary standard.[1219] Submissions also noted the importance of the OAIC providing community focused education[1220] and developing channels to directly disseminate information to the community about the data practices of entities.[1221] The importance of working collaboratively with entities to promote the development of industry best practice was also emphasised. Submitters wanted the OAIC to conduct deeper and more regular engagement with industry[1222] and publish better and more industry-specific guidelines. There were suggestions for the OAIC to identify and call out examples of good privacy practices and conduct sector benchmarking analyses.[1223]

The OAIC also noted it must be appropriately resourced to take on more substantive regulatory action and pursue enforcement through the courts. Although the OAIC is currently able to seek a costs order against an entity to reimburse it for the costs of litigation, this is only available to the OAIC after the court has found an entity has breached a civil penalty provision. The OAIC needs resourcing to be available before initiating such an action to enable it to prepare for and sustain litigation which may last for years, particularly against large multinational technology giants.

Proposal

An industry funding arrangement could be introduced to fund the OAIC's provision of guidance, assistance and advice for organisations as well as undertaking systemic reviews and enforcement action. A levy would recognise that entities should pay for services the OAIC provides to them in the form of tailored guidance, advice, and assessments (particularly any proactive risk assessments where the OAIC would work with the entity to help ensure its policies and practices are sufficient). A narrower group of entities which operate in a high privacy risk environment could also contribute a statutory levy to support the OAIC's management of public inquiries and investigation into their acts or practices (i.e. entities that collect, use or disclose significant amounts of personal information or engage in sophisticated information handling practices). This may include social media platforms and entities which trade in personal information such as digital marketing businesses.

Cost recovery levies and statutory levies have been successfully implemented by other regulators including ASIC and the UK ICO. The Government's industry funding arrangements for ASIC commenced in 2017. Around 90 per cent of ASIC's regulatory activities are now recovered in the form of industry funding levies with the remaining 10 per cent recovered via fees for service. ASIC publishes its regulatory costs as part of an annual Cost Recovery Implementation Statement (CRIS). The CRIS outlines ASIC's forecast regulatory costs and activities by subsector for each financial year and provides details on how ASIC allocated its costs in the previous year. The CRIS also provides industry with indicative levies for the following year to help them plan.

[1219] Submissions to the Issues Paper noting the OAIC needed adequate resourcing included: Law Institute of Victoria, 15; Dr Kate Mathews Hunt, 2; Shogun Cybersecurity, 2, 6; Legal Aid Queensland, 15; Information Technology Industry Council, 3; Electronic Frontiers Australia, 12; Communications Alliance, 12; Office of the Victorian Information Commissioner, 1; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 44; Association for Data-driven Marketing and Advertising, 22; Office of the Information Commissioner Queensland, 5; Centre for Cyber Security Research and Innovation, 12; Australian Information Security Association, 25; CAIDE and MLS, 11; Data Republic, 17; Telstra,11; Reset Australia, 9; ACCC, 7; Atlassian, 2.

[1220] Submission to the Issues Paper: Australian Association of National Advertisers, 4.

[1221] Submission to the Issues Paper: Australian Council on Children and the Media, 3.

[1222] Submission to the Issues Paper: Communications Alliance, 12.

[1223] Submission to the Issues Paper: Data Synergies, 6.

In the UK every organisation or sole trader who processes personal information needs to pay a data protection fee to the UK ICO, unless they are exempt.[1224] This levy has proved successful in generating significant revenue to support the UK ICO's operations.

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.

Questions

- Which of the OAIC's costs should be recovered from industry?
- What are the high privacy risk industries where it would be most appropriate for entities to bear the costs of the OAIC investigating complaints and undertaking enforcement action in the courts?

Annual reporting requirements

Submitters were concerned about a lack of transparency in the OAIC's complaint handling process and lack of ability for individuals to appeal from a decision of the IC to dismiss a complaint.[1225] Salinger Privacy said they had seen complaints which they believed had merit dismissed by the OAIC without making a section 52 determination.[1226] This included where the respondent and complainant disagreed about the interpretation of an APP where a ruling on the matter would have had much broader application than just the complainant's case. The Australian Privacy Foundation also noted the frequent number of dismissals and relatively small number of determinations made each year.[1227]

Under section 46 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), Commonwealth entities are required to provide the accountable authority (here the Attorney-General) with an annual report on the entity's activities for presentation to the Parliament. Section 30 of the AIC Act requires that the IC's annual report contain freedom of information matters, privacy matters, and consumer data right matters. The only 'privacy matters' the IC must report on are defined in section 32 of the AIC Act. These include a statement of the performance of the IC's privacy function of issuing rules relating to tax file number information, and a statement about the operation of registered APP codes including details about the number of complaints made under codes, their nature and outcome.[1228]

Proposal

Better publicising data about which provisions complaints are being dismissed under would assist potential claimants to assess the merits of their complaints and manage their expectations. Providing information around common reasons why complaints are dismissed may reveal common misunderstandings which could assist the OAIC in updating its guidance material. It would assist in providing greater clarity about how the Act is being interpreted and applied.

24.8 Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41.

[1224] *Data Protection (Charges and Information) Regulations 2018* (UK).
[1225] Submissions to the Issues Paper: Legal Aid Queensland, 14-15, Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 43; Australian Privacy Foundation, 33; Salinger Privacy, 36, Reset Australia, 9, MyCRA Lawyers, 8.
[1226] Submission to the Issues Paper: Salinger Privacy, 36.
[1227] Submission to the Issues Paper: Australian Privacy Foundation, 33.
[1228] *Australian Information Commissioner Act 2010* (Cth) s 32, ('*AIC Act*').

Question

- Would amending the OAIC's annual reporting requirements to require more specific figures assist with transparency for complainants?

Better visibility of OAIC investigations

Submissions noted the importance of the regulator providing community focused education[1229] and developing channels to directly disseminate information to the community about the data practices of entities.[1230] The OP Bill contains measures that will enhance the ability for the OAIC to publicise the work that it does, including information about ongoing investigations where it is in the public interest.[1231] In addition, the OP Bill will give the IC a new determination power which could require the APP entity to prepare and publish a statement about the conduct that led to the interference of privacy and steps they have taken or will take to remediate the contravention. This will give greater visibility to the community about OAIC investigations and privacy breaches that have occurred.[1232]

Regulatory model

Submissions raised concerns about the tension between the OAIC's current dual roles as conciliator and regulator which may hinder the OAIC in its ability to carry out both roles and adversely impact public confidence in the OAIC's effectiveness as both a complaints conciliator and a regulator.

The CAIDE and MLS joint submission noted concerns that the current design of the regime 'puts the regulator at the heart of the matter both as the initial finder of fact but also as the entity that can bring a representative action'.[1233]

MyCRA Lawyers expressed similar concerns, stating that:

> *…the OAIC currently has too many roles in the enforcement of Privacy breaches, including acting as an External Dispute Resolution body (EDR), an enforcement body and a final determinative body offering guidance on the interpretation of the Act. It contrasted this with 'other areas, for example financial law, [in which] these areas would normally be dealt with by 3 separate bodies . . . the OAIC is unable to perform all these functions adequately, as the need for targeted enforcement action is not always in congruence with providing fair and balanced outcomes for all complainants who are potentially wronged*.[1234]

MyCRA lawyers suggested splitting the dispute resolution, enforcement, and guidance roles of the regulator amongst three separate entities to allow for more specialised bodies and ensure appropriate emphasis is given to each role. The Law Institute of Victoria and the CAIDE and MLS joint submission recommended creating a privacy ombudsman separate to the OAIC.

The OAIC submission expressed a desire for more flexibility to shift to a risk-based regulatory approach which is more proactive, investigative and enforcement-focused. Currently, the IC is required to investigate and attempt to conciliate all complaints which may be an interference with privacy and which the IC considers reasonably possible to conciliate successfully.[1235] Given the OAIC receives over 2,600 privacy complaints each year,[1236] a significant portion of its efforts are dedicated to resolving individual complaints which do not have a broader deterrent effect. The OAIC proposed providing the IC with greater discretion in when to investigate individual complaints 'to allow the

[1229] Submission to the Issues Paper: Australian Association of National Advertisers, 4.
[1230] Submission to the Issues Paper: Australian Council on Children and the Media, 2.
[1231] Exposure Draft, OP Bill (n 1).
[1232] Submission to the Issues Paper: Cyber Security Cooperative Research Centre, 12.
[1233] Submission to the Issues Paper: CAIDE and MLS, 11.
[1234] Submission to the Issues Paper: MyCRA Lawyers, 6.
[1235] *Privacy Act* (n 2) ss 40, 40A.
[1236] The OAIC received 2,673 complaints in the last financial year: OAIC, *Annual Report 2019–20* (Report, 15 October 2020) 13.

OAIC to identify sectors and acts or practices of concern and prioritise matters accordingly'.[1237] It was suggested that the ability to take more substantive regulatory and enforcement action on the IC's initiative would shift the behaviour of regulated entities across sectors and provide broader deterrence.

Alternative regulatory models

Option 1 – encourage greater use of EDRs

The Act could be amended to require APP entities to participate in a recognised EDR where one is available and the OAIC could refer all privacy complaints in that sector to the EDR wherever possible. The IC already recognises EDR to handle particular privacy complaints under the Act.[1238] Recognised EDRs such as AFCA, the Telecommunications Industry Ombudsman, and the various state and territory energy and water ombudsman services specialise in providing fair, independent and accessible EDR services to resolve complaints. For example, many privacy complaints about telecommunications providers are already being referred to the Telecommunications Industry Ombudsman (who received 4,328 complaints involving privacy issues in the 2019 –20 financial year).

Currently there are only a small number of sectors where EDR schemes have applied to be recognised under the Act. At present, the only sectors in which the IC has recognised EDRs are the financial, energy and water, telecommunications and tolling sectors (and public transport in Victoria only). The top 10 sectors for which the OAIC received privacy complaints in the last financial year included the Australian Government, health service providers, retail, online services, real estate agencies, insurance, and personal services including employment and childcare.[1239] Under this option, APP entities that handle personal information could be required to participate in an EDR scheme, and those 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 provider if a complaint is made against them.

Option 2 – create a Federal Privacy Ombudsman

Alternatively, a separate Federal Privacy Ombudsman (FPO) could be created, which could be responsible for triaging and conciliating privacy complaints. A FPO could also utilise recognised EDRs however it would be responsible for maintaining a register of all privacy complaints dealt with by EDRs and would resolve any complaints where no suitable EDR exists. The OAIC would focus on IC-initiated investigations. Where the FPO or EDR considered that a complaint may be an interference with privacy and is unsuitable for conciliation or may require enforcement action, they would refer the matter to the OAIC for investigation. The OAIC could then investigate and invoke the appropriate regulatory response, which may include making a determination, issuing an infringement notice, or pursuing a civil penalty or injunction in the Federal Court. The implications for the FOI functions currently undertaken by the IC would need to be considered further if this proposal was to be adopted.

This option would give the OAIC a clearer, narrower mandate as a strategic privacy regulator. The OAIC would be able to concentrate on building the requisite institutional capacity to be a more proactive enforcement-focused regulator by directing its attention to taking regulatory action, including conducting systemic industry reviews and undertaking enforcement action in the courts This option would be consistent with the model used by ASIC and the ACCC, which has allowed them to establish themselves as strategic, proactive regulators. Instead of ASIC conciliating financial complaints, the AFCA provides consumers and small businesses with fair, free and independent dispute resolution for financial complaints.[1240] Similarly the ACCC does not receive consumer law

[1237] Submission to the Issues Paper: OAIC, 120.
[1238] *Privacy Act* (n 2) s 35A.
[1239] OAIC, *Annual Report 2019–20* (n 1236).
[1240] AFCA, *About AFCA* (Web Page, 2021).

complaints as these are handled by consumer protection agencies along with industry ombudsmen and dispute resolution offices in each state and territory.[1241]

A key limitation of this option it that it would require creating a new federal government entity which would require its own resourcing to establish and maintain. There may also need to be a transition period to ensure that individuals know where they should lodge complaints and for existing complaints being conciliated by the OAIC to be transferred to the FPO.

Option 3 – establish a Deputy Information Commissioner – Enforcement

A third option would be to establish a Deputy Information Commissioner – Enforcement within the OAIC. This would allow more of the OAIC's focus to be dedicated to enforcement while maintaining the OAIC's current complaint handling functions. Under this option, there would still be a need for information barriers within the OAIC where it must be careful to ensure that any information obtained through its impartial conciliation service is not used in its investigations[1242] and enforcement action against entities for breaches.[1243]

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.

Questions

- Which option would most improve the complaints handling process for complainants and allow the OAIC to focus on more strategic enforcement of the Act?
- Are there other options that could achieve this outcome that should be considered?

[1241] ACCC, *Where to go for consumer help* (Web Page, 2021).

[1242] *Privacy Act* (n 2) s 44.

[1243] The FPO's information sharing provisions would need to allow it to share data about the nature of complaints it receives with the OAIC to enable the OAIC to identify sectors and entities of concern and systemic issues which the OAIC would use in its strategic enforcement.

25. A direct right of action

The ability of individuals to litigate a claim for breach of their privacy under the Act is limited. The DPI report recommended that individuals be given a direct right to bring actions and class actions against APP entities in court to seek compensatory damages as well as aggravated and exemplary damages (in exceptional circumstances) for the financial and non-financial harm suffered as a result of an interference with their privacy under the Act.[1244]

The Issues Paper noted the government had supported the DPI's recommendation to introduce a direct right of action in principle and asked:

> *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?*

More than half of submissions supported introducing a direct right of action to empower individuals to exercise greater control over the enforcement of their privacy rights.[1245] They considered that the possibility of individual or class actions being brought against entities for interferences with privacy is likely to provide an additional incentive for entities to comply with their obligations and deter poor behaviour.[1246] It would also increase the amount of jurisprudence under the Act, providing guidance for individuals and entities on their rights and obligations.[1247] It would also be more efficient for cases for breaches of privacy to be dealt with in court alongside other actions (for example, discrimination) rather than the privacy aspect being dealt with by the OAIC separately.[1248]
If high profile actions for interferences with privacy are successful, this may increase public awareness of privacy.[1249] Several submissions raised concerns about whether a direct right of action would have the desired outcome of giving individuals greater control. We have outlined and attempted to mitigate these concerns under each element of the proposed model below.

Proposal

The Review has considered what the direct right of action could look like if it is enacted.

Who could exercise the right?

The proposed right would be available to both individuals and representative classes of individuals who have suffered an alleged interference with their privacy.[1250] Some submitters raised concerns about the potential for class actions under this right and reflected on the broader use of class actions

---

[1244] ACCC, DPI report (n 2) 473.
[1245] Submissions to the Issues Paper supportive of some form of direct right included: Public Interest Advocacy Centre, 8–9; Office of the Information Commissioner Queensland, 5; Reset Australia, 9–10; OAIC, 130; ACCC, 7; Salinger Privacy, 36; Legal Aid Queensland, 16; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia, 42; Law Institute of Victoria, 16; Dr Kate Mathews Hunt, 13; Shogun Cybersecurity, 5; Cyber Security Cooperative Research Centre, 12; Electronic Frontiers Australia, 12; Privcore, 4; MyCRA lawyers, 11; Centre for Cyber Security Research and Innovation, 12; Calabash Solutions, 11; Australian Information Security Association, 26; CAIDE and MLS, 11; Shaun Chung and Rohan Shukla, 18; Deloitte, 30; Illion, 7; elevenM, 3; Australian Society of Archivists, 3; Digital Rights Watch, 4; Reset Australia, 9; Castan Centre for Human Rights Law, 45; Maurice Blackburn, 10.
[1246] Submissions to the Issues Paper: Shogun Cybersecurity, 5; Cyber Security Cooperative Research Centre, 12–3; Office of the Information Commissioner Queensland, 5; ACCC, 7.
[1247] Submissions to the Issues Paper: Australian Privacy Foundation, 35–6; Public Interest Advocacy Centre, 10.
[1248] Submission to the Issues Paper: Public Interest Advocacy Centre, 8-11.
[1249] Submission to the Issues Paper: Deloitte, 30.
[1250] Note Class actions under the proposed direct right of action would only be able to be brought in the Federal Court, as the Federal Circuit Court does not have jurisdiction to hear representative proceedings.

in Australia and perceived inadequacies around the current regulation of class actions and litigation funders.[1251]

The government is currently considering the findings from the Parliamentary Joint Committee on Corporations and Financial Services' report (PJCCFS report) on litigation funding and the regulation of the class action industry, which was tabled in December 2020.[1252] The Committee found that, in many cases, litigation funders appear to be making windfall profits that are disproportionate to the costs incurred and the risk undertaken. Recommendation 20 of the PJCCFS report seeks to address this concern. The Government is actively considering the recommendation of the PJCCFS Report, and future reforms in this space will strike an effective balance between ensuring class members receive a fair and proportionate share of the proceeds of a class action, and ensuring the viability of litigation funding arrangements that can provide ordinary Australians with access to justice.

Submissions supportive of allowing class actions identified that proceedings are expensive for individuals to run and class actions would make this right of action more accessible, particularly for individuals involved in privacy breaches which have affected many people.[1253] The OAIC considered that a direct right of action in the Federal Court would be a more appropriate vehicle for representative complaints than going through the OAIC's conciliation process in certain circumstances.[1254]

Forum for the direct right of action

Many submitters, including the OAIC, supported the ACCC's recommendation in the DPI report that a forum for this right be the Federal Court or Federal Circuit Court (FCC).[1255] This would allow a greater body of jurisprudence to be developed by the court, which would assist the public and APP entities to better understand their rights and obligations.

Other submitters were concerned about access to justice, noting the prohibitively high cost and delays of court action.[1256] However, allowing class actions could increase access to justice for individuals who might not otherwise have the resources to initiate proceedings in court. In addition, a 'small claims procedure' could be created for privacy matters in the FCC to reduce the burden on individuals seeking to exercise the direct right of action – both in terms of costs, and the burden of complying with the procedural rules in the Federal Court. This could be modelled on existing 'small claims' regimes in the FCC, such as that for consumer credit matters under the *National Consumer Credit Protection Act 2009* (Cth) and for industrial law claims, which both offer reduced filing fees for smaller matters. However, any suggestion of a 'small claims procedure' being established for privacy matters should be considered in light of the existing caseload and resourcing of the Federal Court and the FCC.

Gateway to enliven the right

Some submitters were concerned that if the model was not carefully designed, it could significantly impact on court resources.[1257] Several submissions suggested a gatekeeper model similar to that

---

[1251] Submissions to the Issues Paper: Ai Group, 21–3; Australian Finance Industry Association, 8; Free TV, 17; Information Technology Industry Council, 3–4.
[1252] Parliamentary Joint Committee on Corporations and Financial Services, 'Litigation funding and the regulation of the class action industry' (Report, 21 December 2020).
[1253] Submissions to the Issues Paper: OAIC, 130; Legal Aid Queensland, 15–6 ; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 45; Public Interest Advocacy Centre, 10; Shogun Cybersecurity, 5; Cyber Security Cooperative Research Centre, 12–3; Centre for Cyber Security Research and Innovation, 12; Calabash Solutions, 11; CAIDE and MLS, 11; Deloitte, 30; Castan Centre for Human Rights Law, 45.
[1254] Submission to the Issues Paper: OAIC, 132.
[1255] ACCC, DPI report (n 2) 473.
[1256] Submissions to the Issues Paper: Free TV, 17; Adobe, 11; Legal Aid Queensland, 15.
[1257] Submissions to the Issues Paper: Ai Group, 20; Telstra and Telstra Health, 19; Avant Mutual, 15; Facebook, 46; OAIC, 132.

under the *Australian Human Rights Commission Act 1986* (Cth) in which complainants first file with the OAIC and are subject to conciliation before the direct right is enlivened.[1258] Avant Mutual suggested conciliation should be a compulsory step before bringing an action.[1259]

Some submitters warned a gatekeeper model could increase complexity (particularly where there is more than one cause of action), add procedural steps and create a 'bottleneck' and delays, impacting access to justice.[1260] The Public Interest Advocacy Centre advised against requiring all individuals to go through a conciliation process before applying to the courts, noting that the court generally orders mediation as an early step anyway where individuals choose to apply directly to the courts in human rights matters.[1261]

Under the proposed model, claimants would first make a complaint to the OAIC or other complaint handling body such as a recognised EDR Scheme, Industry Ombudsman or FPO[1262] and have their complaint assessed for conciliation.[1263] The complainant could then elect to initiate action in court either:

- instead of pursuing conciliation
- after conciliation has proven unsuccessful
- where the OAIC has determined the matter not suitable for conciliation, or
- where the OAIC has terminated the matter.

The complainant would also need to seek leave of the court to make the application.

This model would balance the need to give individuals a more direct pathway to redress in court while also protecting the court's resources from being overburdened by frivolous claims. Where matters are assessed as suitable for conciliation, the complainant may realise it would be in their best interests to undertake conciliation prior to initiating court action. However, it also recognises that some complaints are unsuitable for conciliation.[1264] The OAIC would have the option to initiate its own investigation into the alleged interference and bring civil penalty proceedings either prior to or after an individual has initiated a matter under the direct right of action.

Harm threshold: what the complainant would need to establish

Some submitters recommended the direct right of action should be limited to only serious interferences with privacy to protect the court's resources.[1265] However, if complainants are first assessed for conciliation, and if complainants must obtain leave of the court before bringing an action, this should prevent the court from being flooded by frivolous or vexatious claims. The Federal Court and Federal Circuit Court are also costs jurisdictions. Other submissions noted existing safeguards in the judicial process which reduce frivolous litigation: including lawyers only acting if there are reasonable prospects of success and the disincentive of a costs award.[1266]

The Public Interest Advocacy Centre was concerned that a seriousness threshold would add complexity.[1267] The OAIC considered a seriousness threshold would substantially curtail the

[1258] Submissions to the Issues Paper: Calabash Solutions, 11; Blancco, 73; Google, 12; Ramsay Health Care, 9; Federal Chamber of Automotive Industries, 23.
[1259] Submission to the Issues Paper: Avant Mutual, 15.
[1260] Submissions to the Issues Paper: Public Interest Advocacy Centre, 10–11; Salinger Privacy, 36.
[1261] Submission to the Issues Paper: Public Interest Advocacy Centre, 10–1.
[1262] For a further discussion of the proposed Federal Privacy Ombudsman, see Chapter 24.
[1263] See options for alternative complaint-handling processes in Chapter 24.
[1264] Submission to the Issues Paper: MyCRA Lawyers, 8.
[1265] Submissions to the Issues Paper: Adobe, 12; Avant Mutual, 15; Calabash Solutions, 11; Clubs Australia, 5-6; Cyber Security Cooperative Research Centre, 13.
[1266] Submission to the Issues Paper: Shaun Chung and Rohan Shukla, 18–9.
[1267] Submission to the Issues Paper: Public Interest Advocacy Centre, 10.

effectiveness of this right by precluding people from seeking recourse in the courts and limiting the opportunity for courts to interpret the APPs.[1268]

Role of the OAIC as amicus curiae

Some submitters believed the IC should be able to be heard in proceedings as amicus curiae using a similar model to that used by the Australian Human Rights Commissioner.[1269] The OAIC submitted that it should have the right to intervene in proceedings (or seek leave to intervene) as well as a right to seek leave to act as amicus curiae.[1270]

An amicus curiae is a person who assists the court while not being a party to the proceedings. For example, ASIC may appear as amicus curiae either after ASIC seeks leave of the court to appear or at the court's request.[1271] The value of regulators appearing as amicus curiae include to:

- alert the court to any aspect of proceedings which the parties may not otherwise raise
- assist the court interpret legislation the regulator administers or formulate a principle of law, and
- articulate broader issues that may affect other stakeholders.[1272]

ASIC also has the right to intervene in proceedings. However, it generally prefers to appear as amicus curiae.[1273]

Under the proposed model, the OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court or on their own motion where the orders sought would affect privacy rights of people generally, the administration of the Act, or where there were other special circumstances in the public interest. The OAIC would not have the right to intervene in proceedings because it is more appropriate for the Attorney-General to intervene in such matters. As noted above, the OAIC would have the option to initiate its own civil penalty proceedings either prior to or after an individual has initiated a matter under the direct right of action.

Remedies

The proposed model would adopt the DPI report's proposal that available remedies under this right should include compensatory damages as well as aggravated and exemplary damages (in exceptional circumstances) for the financial and non-financial harm suffered as a result of an infringement of the Act and the APPs.[1274] The Federal Court would also be able to order any other equitable relief the Court thinks necessary. An individual or class action under this direct right would also have the ability to apply directly to the Federal Court or Federal Circuit Court under section 80W of the Act to obtain a performance injunction or restraining injunction for contraventions of the Act.

Some submitters suggested a statutory cap should be imposed on damages to balance the tension between adequately compensating individuals and unduly burdening business.[1275] However, several other submissions were concerned any cap on damages may discourage people from bringing

---

[1268] Submission to Issues Paper: OAIC, 131.
[1269] Submissions to Issues Paper: Public Interest Advocacy Centre, 10; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 45.
[1270] Submission to Issues Paper: OAIC, 133–4.
[1271] This can be either under the Federal Court (Corporations) Rules 2000 or the court's inherent jurisdiction.
[1272] ASIC, ASIC's approach to involvement in private court proceedings (Web Page, 2013).
[1273] Ibid.
[1274] ACCC, DPI report (n 2), 473.
[1275] Submitters supportive of a statutory cap – Submissions to the Issues Paper: Salinger Privacy, 37; Law Institute of Victoria, 16; Cyber Security Cooperative Research Centre, 13; Avant Mutual, 15; elevenM, 3.
Submitters not supportive of a statutory cap – Submissions to the Issues Paper: OAIC, 133; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 45; Public Interest Advocacy Centre, 11; Castan Centre for Human Rights Law, Monash University, 46; Centre for Cyber Security Research and Innovation, 12; Calabash Solutions, 11.

serious matters and enable perpetrators to make settlement offers relative to the cap. Compensation should match the loss suffered and a cap may be a disincentive for class actions (unless the cap took into regard the number of individuals within a class).

The OAIC used the compensation regime for unlawful discrimination under the *Australia Human Rights Commission Act 1986* (Cth) as an example of damages awarded for non-economic loss which does not have a damages cap. The OAIC said this approach would allow compensation to reflect the changing landscape of privacy harms.[1276] Courts, through their judgments, would set standards for appropriate types and levels of damages for privacy breaches, taking into account the particular facts and circumstances of each case. Other submissions noted the EU, NZ and Canada do not have a cap on damages for their direct rights of action.

The Public Interest Advocacy Centre suggested that rather than introducing a cap to reduce the incentive for parties to litigate, it is preferable that the OAIC encourage use of its conciliation mechanisms to resolve complaints.[1277] Several submitters supported the availability of aggravated and exemplary damages in exceptional circumstances for financial and non-financial harm.[1278] The Law Institute of Victoria submitted that any other equitable relief the Court thinks necessary should be allowed.[1279]

25.1 Create a direct right of action with the following design elements:

- The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.
- The action would be heard by the Federal Court or the Federal Circuit Court.
- The claimant would first need to make a complaint to the OAIC (or FPO)[1] and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman.
- The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application.
- The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.

Question

- Is each element of the proposed model fit for purpose? In particular, does the proposed gateway to actions strike the right balance between protecting the court's resources and providing individuals a more direct avenue for seeking judicial consideration and compensation?

[1276] Submission to the Issues Paper: OAIC, 133.
[1277] Submission to Issues Paper: Public Interest Advocacy Centre, 11.
[1278] Submissions to the Issues Paper: OAIC, 133; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 45; Centre for Cyber Security Research and Innovation, 12; Calabash Solutions, 11.
[1279] Submission to the Issues Paper: Law Institute of Victoria, 16.

26. A statutory tort of privacy

The Issues Paper asked several questions about a statutory tort for invasions of privacy, including about the need for a tort as well as questions as to its design.

Submissions were divided between supporting the establishment of a statutory tort, supporting the development of a tort through the common law, and opposing the establishment of a statutory tort.

Submissions in favour of establishing a tort for invasions of privacy were largely from individual submitters, academics, privacy regulators and experts, and not-for-profit entities focused on cybersecurity, consumer advocacy and digital rights.[1280] These submissions identified that a statutory tort would fill gaps in the legal framework for privacy protection. That is, existing causes of action do not appropriately address breaches of privacy as a standalone interest,[1281] and individuals cannot seek compensation for emotional distress for invasions of privacy litigated through other causes of action.[1282]

Submissions in favour of a tort highlighted the increasing ease with which serious invasions of privacy occur in the digital age, facilitated by mobile technology and the internet.[1283] Submissions also noted the sorts of serious invasions of privacy where victims are currently prevented from obtaining compensatory damages as including:

- intimate image abuse[1284] and interference with bodily and territorial privacy[1285]
- individuals accessing personal information about another person available to them through their employment, but for which the employer is not liable because it was a misuse for a personal purpose, such as blackmail or in Family Court proceedings[1286]
- misuse of private information by entities not covered by the Act including small business operators, media organisations, registered political parties, or misuse of private information contained in an employee record[1287]
- unwarranted surveillance by insurance companies for insurance claim assessment purposes, which may extend to persons who are not a party to the insurance contract,[1288] and
- breaches of the Act, such as disclosure by police of a spent conviction to a man's partner and employer, where a tort would permit an applicant to seek a greater amount in damages than may become available under a direct right of action if statutory compensation limits apply.[1289]

[1280] See, eg, Submissions to the Issues Paper: Dr Jelena Gligorijevic, 2; Salinger Privacy, 38–9; Dr Kate Mathews Hunt, 13–4; Cyber Security Cooperative Research Centre, 13–4; Electronic Frontiers Australia, 13; Shogun Cybersecurity, 5; Legal Aid Queensland, 15–7; MyCRA Lawyers, 12–3; Michael Douglas, University of Western Australia, 2–3; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 46–9; New South Wales Information and Privacy Commission, 4; Law Institute of Victoria, 16–7; Public Interest Advocacy Centre, 11-13; Office of the Information Commissioner Queensland, 4–5; Bennett + Co, 2-3; Centre for Cyber Security Research and Innovation, 12; Australian Information Security Association, 27; OAIC, 135–7.

[1281] Submission to the Issues Paper: Dr Jelena Gligorijevic, 2.

[1282] Submissions to the Issues Paper: Public Interest Advocacy Centre, 13; Salinger Privacy, 38; Cyber Security Cooperative Research Centre, 14.

[1283] Submission to the Issues Paper: Michael Douglas, University of Western Australia, 2–3, citing Michael Douglas, 'Characterisation Of Breach Of Confidence As A Privacy Tort In Private International Law' (2018) 41(2) *UNSW Law Journal 490*, pt III, 'The Identity of Breach of Confidence'.

[1284] Submission to the Issues Paper: Salinger Privacy, 38.

[1285] AHRC Report (n 128), 123.

[1286] Submissions to the Issues Paper: Public Interest Advocacy Centre, 13; Salinger Privacy, 38.

[1287] Submission to the Issues Paper: Public Interest Advocacy Centre, 13.

[1288] Submission to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 48.

[1289] Submission to the Issues Paper: Salinger Privacy, 38–9.

Some submitters identified benefits to having a tort of privacy develop through the common law, rather than via statute. In her submission, Dr Gligorijevic noted that common law development should be preferred over statutory intervention, given the normative complexities around protecting individuals' privacy. She also notes that in jurisdictions where individual privacy is protected by law – such as England, Wales, Canada, and New Zealand – privacy protection has mostly developed through the common law.[1290] The ALRC has also identified benefits to a common law tort for invasions of privacy, noting that a statute can have unintended consequences, and it may capture, or fail to capture, conduct that was not considered when the statute was enacted. The common law also provides flexibility for the cause of action to adapt to changing circumstances and technology, whereas a statute may become outdated and legislative amendments may not keep up with such changes.[1291]

Those submissions opposed to a statutory tort, mostly from media and business stakeholders, argued that it is unnecessary given the existing legal avenues which cover similar ground. These include the online safety framework, criminal law offences of voyeurism, and civil law actions such as trespass to land, nuisance, action on the case for intentionally causing harm, defamation and the equitable breach of confidence.[1292] Submissions from media organisations also emphasised the potential for a statutory tort to adversely affect the free flow of information and freedom of expression by the media.[1293] Some submissions also noted that there would likely be increased costs if a statutory tort were established, including legal and court costs as a result of increased litigation arising from a new cause of action. [1294] Opponents of a tort also argued that it is a remedy that, in practice, is only likely to be used by those who can afford to risk bringing legal action. In the absence of other remedies, those who can afford it will have greater privacy protection than those who cannot.

Comparing approaches to a tort of privacy across jurisdictions

Case law involving breaches of privacy in overseas jurisdictions illustrate how such breaches can be litigated through different causes of action. For example, in some jurisdictions this has occurred through a common law tort for invasions of privacy, a statutory tort, or through other avenues including the equitable action for breach of confidence.

The High Court in *Australian Broadcasting Corporation v Lenah Game Meats* contemplated the possibility of a tort of privacy being developed in Australia,[1295] however such a tort has yet to evolve at common law. Arguably this may imply there is no significant lacuna in the law or, alternatively, the mischief to be addressed lacks precise elaboration. This is in contrast to comparable jurisdictions such as the UK and NZ, where causes of action at common law for breach of privacy have developed, including from an equitable action for breach of confidence.[1296]

[1290] Submission to the Issues Paper: Dr Jelena Gligorijevic, 10.
[1291] ALRC Report 123 (n 778), 23; Submission to the Issues Paper: Law Council of Australia, 24.
[1292] Submissions to the Issues Paper: Arts Law Centre of Australia, 8–9; Google, 12; Telstra and Telstra Health, 10–11; Medical Insurance Group Australia, 10; KPMG, 20; Free TV, 16; Australia's Right to Know Coalition, 1; Federal Chamber of Automotive Industries, 24; Nine, 6; Commercial Radio Australia, 1–2.
[1293] Submissions to the Issues Paper: Free TV, 17; Australia's Right to Know Coalition, 1; Commercial Radio Australia, 1; SBS, 9.
[1294] Submissions to the Issues Paper: Australian Financial Markets Association, 15; Avant Mutual, 15–16; Ramsay Health, 9.
[1295] [2001] HCA 63.
[1296] In New Zealand: *Hosking v Runting* [2005] 1 NZLR 1 (CA); *C v Holland* [2012] NZHC 2155, [2012] 3 NZLR 672, ('*C v Holland*'). In the United Kingdom: *Wainwright v Home Office* [2004] 2 AC 406; *Campbell v MGN Ltd* [2004] 2 AC 457, ('*Campbell*') – in this case, the equitable action for breach of confidence was expanded to address misuse of private information.

In Canada, a tort of privacy regarding intrusion upon seclusion has developed at common law in Ontario,[1297] while other provinces have introduced statutory torts of privacy.[1298]

Internationally, the tort of privacy has largely been used by high profile individuals against media outlets.[1299] However, there have also been cases involving intimate image abuse that have been litigated using the equitable duty of confidence in Australia and the tort of privacy in NZ.[1300] In recent years there has been increased recognition of the serious harm caused by this type of behaviour in Australia, including through the introduction of a removal notice scheme requiring internet providers and perpetrators to take down intimate images.[1301] Failure by a digital platform to comply with the notice is subject to a civil penalty scheme. The eSafety Commissioner may take action against perpetrators by issuing formal warnings, infringement notices and seeking an injunction or civil penalty order from a court.[1302] The image-based abuse complaints and reporting scheme does not include any mechanism to enable victims to claim compensation from a perpetrator.

In 2019–20, the eSafety Commissioner handled 2702 reports of image-based abuse, which was a 184 per cent increase on the previous reporting period. In 2019–20, seven removal notices were issued to websites and hosting service providers, five of which were complied with. Four formal warnings and one informal warning was issued to persons responsible for image-based abuse. [1303] Victims of image based abuse were predominantly female.[1304]

Recognition of this type of harm was the basis for recently extending the New Zealand *Privacy Act 2020* to apply certain Information Privacy Principles (IPPs) to individuals in connection with their personal or domestic affairs, where their collection, use or disclosure of personal information would be highly offensive to a reasonable person.[1305] The 'highly offensive' test is based on that used in the New Zealand tort of invasion of privacy, and is also used in the privacy principles of the New Zealand Broadcasting Standards Authority.[1306] The provision in the *Privacy Act 2020* (NZ) provides an alternative complaint mechanism, without having the expense or burden of launching a tort action through the courts. The damages available will also differ between the two options for pursuing a privacy claim. There is a cap of $350,000 if the matter is pursued through the Human Rights Review

---

[1297] The tort of intrusion upon seclusion was recognised in Ontario in *Jones v Tsige* [2012] O.J. No. 148, (*'Jones'*).

[1298] British Columbia: Privacy Act [RSBC 1996], c 373, s 1; Saskatchewan: Privacy Act [RSS 1978], c P-24, s 2; Newfoundland and Labrador: Privacy Act [RSNL 1990], c P-22, s 3; Manitoba: Privacy Act [CCSM 1987], c P125, s 2.

[1299] *HRH Duchess of Sussex v Associated Newspapers Ltd* [2021] EWHC 273 (Ch); *Campbell* (n 1296); *Douglas v Hello!* [2001] QB 967.

[1300] In Australia: *Giller v Procopets* [2008] VSCA 236; *Wilson v Ferguson* [2015] WASC 15 – Both of these cases involved women suing former partners in actions for breach of confidence for sharing videos of their intimate sexual relations. Damages for emotional distress were awarded in both cases. In New Zealand: *C v Holland* (n 1296) - C lived in a house with her partner and Mr Holland. Mr Holland took videos of C in the shower and stored them on a hard drive. Mr Holland was convicted of a criminal offence and ordered to pay $1000 to C. C sought civil compensation for breach of privacy. The Court held Mr Holland liable for intrusion into C's seclusion by videoing her in the shower, as he intruded her intimate personal space and activity without consent or legislative authority, infringed a reasonable expectation of privacy and was highly offensive to the reasonable person.

[1301] *Online Safety Act* (n 605), Pt 3, Div 3.

[1302] Ibid, Pt 10.

[1303] ACMA and Office of the eSafety Commissioner, *Annual Reports 2019–20,* (Report, 9 September 2020), 214. The *Online Safety Act* (n 605) establishes a civil penalties scheme that gives the eSafety Commissioner range of powers to take action against perpetrators, such as issuing a formal warning, issuing an infringement notice and seeking an injunction or civil penalty order in Court. eSafety Commissioner, 'Our legislative functions', (Web Page, 2021).

[1304] 68 per cent were female, 27 per cent were male, while 5 per cent not provided or preferred not to disclose - ACMA and Office of the eSafety Commissioner, Annual Reports 2019–20 (n 1303), Figure 2.8.

[1305] New Zealand Law Commission, *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4*, (Report 123, 2011) [4.68] (*'NZLC Report 123'*); *Privacy Act 2020* (NZ) (n 29), s 27. For clarity, section 27 only applies obligations under IPPs 1-3, 4(b) and 5-12 to individuals in these circumstances. It does not require individuals to comply with other obligations under New Zealand Privacy Act in connection with their personal or domestic affairs, for example requirements to designate privacy officers (*Privacy Act 2020* (NZ), section 201).

[1306] NZLC Report 123 (n 1305) [4.75].

Tribunal under the *Privacy Act 2020* (NZ), whereas an individual can seek damages above this amount if a tort action is brought in the High Court.[1307] In recommending the 'highly offensive' test, the New Zealand Law Reform Commission cited the privacy tort case of *Hosking v Runting,*[1308] stating that:

> *'highly offensive' publicity would involve 'very personal and private matters', and would be 'determined objectively, by reference to its extent and nature, to be offensive by causing real hurt or harm'.*[1309]

The recent New Zealand case of *Peters v Bennett & Ors*, further confirmed the 'highly offensive' requirement. This case confirmed that, for a plaintiff to make out the tort of breach of privacy, there must be both a reasonable expectation of privacy, and a disclosure of private facts that would be regarded as highly offensive to a reasonable person.[1310]

Other cases in overseas jurisdictions involving invasions of privacy have included individuals improperly accessing the personal information of others through their employment, and ex-partners publishing materials online relating to their former partner and children of the relationship.[1311] One matter involving a breach of privacy by a media organisation in the UK was the phone tapping of abducted and murdered schoolgirl Millie Dowler, by News of the World in 2002. However, this matter was not ultimately the subject of any judicial decision. The parents sued News International for a breach of privacy and received an out of court settlement.[1312]

Proposals

The need for a statutory tort for invasions of privacy will continue to be considered following responses to the Discussion Paper.

The model of a statutory tort for invasion of privacy

If the need for a statutory tort is accepted, questions remain as to whether its scope and application should be prescribed by the legislature, or whether these elements should be left to the courts to develop. If reform is considered desirable, there are two applicable approaches which are set out further below.

Statutory tort – ALRC model

The ALRC Report 123 recommended a statutory tort with two limbs:

- Intrusion upon seclusion, and
- Misuse of private information.[1313]

Under the formulation recommended by the ALRC, a plaintiff would need to prove that:

- the public interest in privacy outweighed any countervailing public interest
- the breach of privacy satisfied a seriousness threshold, and
- they had a reasonable expectation of privacy in all the circumstances.[1314]

[1307] New Zealand Ministry of Justice, *Human Rights Review Tribunal*, (Web Page, 2021); New Zealand Ministry of Justice, *Claims you can take to civil court*, (Web Page, August 2020).
[1308] [2005] 1 NZLR 1, [125]–[126].
[1309] NZLC Report 123 (n 1305) [4.75].
[1310] [2020] NZHC 761. This case involved leaking of private information to the media about former Deputy Prime Minister of New Zealand, Winston Peters, which related to an overpayment of superannuation from the New Zealand Ministry of Social Development. The High Court of New Zealand held that, while Mr Peters had made out these two requirements, he had not established that it was the defendants who had made the disclosure. Mr Peters is appealing this matter.
[1311] *Jones* (n 1297); *Nesbitt v Neufeld* (2010) BSC 1605; *VMY v SHG* [2019] O.J. No. 6702.
[1312] J Deans, 'Phone hacking: NI confirms £2m for Dowlers and £1m charity donation', *The Guardian* (online, 22 October 2011).
[1313] ALRC Report 123 (n 778), 9.
[1314] Ibid 9–10.

A number of submissions to the Issues Paper supported the recommendations of the ALRC to establish a statutory tort.[1315] Some expressed the view that this model for statutory tort would help fill the gap in existing laws and create a more effective framework for responding to breaches of privacy, particularly given the increased use of data and proliferation of data handling practices.[1316]

The recent AHRC Report recommended that the Australian Government introduce a statutory cause of action for serious invasion of privacy.[1317] The AHRC stated that extending the protection of Australian law beyond 'information privacy' as recommended by the ALRC 'could address some, though not all, of the concerns about how personal information can be misused in the context of facial recognition and other forms of biometric surveillance, and AI-informed decision making generally'.[1318]

However, the Castan Centre identified that there is a risk that the ALRC model is too narrow and overly prescriptive in that it is limited to serious and intentional or reckless invasions of privacy, and therefore, less serious or negligent invasions of privacy would not be covered.[1319] The Castan Centre also raised that its prescriptiveness may limit the ability of the tort to apply and adapt to new and emerging situations.[1320] For example, in Ontario, the common law has evolved to recognise a tort of intrusion into seclusion (2012), publication of embarrassing private facts (2016) and false light privacy tort (2019).[1321]

Dr Jelena Gligorijevic's submission noted that, contrary to the ALRC recommendations about balancing privacy with other interests in establishing a cause of action, 'competing interests can appropriately be accounted for in the 'reasonable expectation' threshold test, and in the set of distinct defences to the privacy action'.[1322]

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

Minimalist statutory tort

As an alternative to the prescriptive model proposed by the ALRC, some submitters favoured a minimalist approach the development of a statutory tort.

Dr Gligorijevic considered that any statutory intervention should still permit the courts to develop the tort – that is, the primary purpose of any legislative action should be to activate the courts to provide remedies in appropriate cases, rather than dictating to the courts in precise terms the substantive contours of the protected interest.[1323]

A more minimalist statutory tort could be an alternative to the ALRC model – one that recognises the existence of a tort, but leaves the development of its scope and application to the courts. This would be similar to the approach of several Canadian provinces, which have established a statutory tort through minimal prescription in their relevant Acts. For example, the British Columbian Act establishing a privacy tort provides that 'it is a tort, actionable without proof of damage, for a

[1315] Submissions to the Issues Paper: Salinger Privacy, 38; Dr Kate Mathews Hunt, 13; Cyber Security Cooperative Research Centre, 13–14; Electronic Frontiers Australia, 13; Office of the Information Commissioner Queensland, 5; Bennett + Co, 2; Australian Information Security Association, 27.
[1316] Submissions to Issues Paper: New South Wales Information and Privacy Commission, 4; Cyber Security Cooperative Research Centre, 13.
[1317] AHRC Report (n 128) 121.
[1318] Ibid 122.
[1319] Submission to the Issues Paper: Castan Centre for Human Rights Law - Monash University, 60.
[1320] Ibid 57.
[1321] Ibid 53.
[1322] Submission to the Issues Paper: Dr Jelena Gligorijevic, 22.
[1323] Ibid 10.

person, wilfully and without a claim of right, to violate the privacy of another'.[1324] However, similar to a tort developing at common law, this approach would rely on cases coming before the courts and may therefore involve long periods of uncertainty as the law develops.

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.

Extending the Privacy Act to individuals

A tort could be allowed to develop at common law as required, but the Act could be extended to individuals. This would explicitly recognise the particular harm caused by misuse of personal information by individuals, often facilitated by the internet, which enables that information to be shared widely. This would be a similar approach to that taken in New Zealand where individuals in a non-business capacity are covered in respect of the collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person. This would not affect the obligations of APP entities under the Act. Rather, this would be a stand-alone provision that applies obligations under the Act to individuals in a non-business capacity, where the relevant threshold is met.

It would provide an avenue of redress for collection, use or disclosure of personal information which meets the 'highly offensive' threshold including intimate image abuse, bullying[1325] or perpetrating domestic violence. This proposal would give victims and survivors of such behaviour a low cost avenue to seek compensation under the civil standard of proof. This alternative option would be complemented by access to the courts under any new direct right of action.

This proposal would be a narrower cause of action than a statutory tort for invasion of privacy, as it would only apply to individual in a non-business capacity and would be limited to mishandling of personal information. This provision would therefore not cover entities, even where their collection, use or disclosure of information was highly offensive – however, such action by an APP entity could separately breach the APPs. This provision would also not have the breadth of a statutory tort – for example, it would not cover instances where a person's housemate covertly watches them while they are showering, unless they made a recording.

This measure would sit alongside the Online Safety Framework (the Framework) which has, as its primary focus, the ability to swiftly have damaging images taken down. It does not however provide any avenue for victims to pursue compensation. This reform may positively contribute to the deterrence effect of the Framework and current criminal offences for this conduct.

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.

Making damages for emotional distress available for actions for breach of confidence

Another alternative to a statutory tort could be for the states to consider legislating to make damages for emotional distress available in an equitable action for breach of confidence. The equitable action for breach of confidence provides some protection against the misuse or disclosure of confidential information. However, uncertainty remains as to whether an individual can seek

[1324] *Privacy Act* [RSBC 1996], c 373, s 1 (British Columbia).
[1325] The harms arising from cyber-bullying or cyber-abuse amongst adults have been recognised in the Online Safety Act 2021 (n 605) which provides a removal notice scheme for cyber-abuse against adults, among other measures.

damages for emotional distress in an action for breach of confidence in Australia.[1326] This means that an action in breach of confidence may be less effective following a wrongful disclosure (as opposed to being taken to prevent a disclosure), as there is less certainty around the ability of a plaintiff to recover compensation for emotional distress after the information has been disclosed.

As actions in equity are pursued through state courts, Commonwealth legislation is unlikely to be the appropriate vehicle to legislate for damages for emotional distress in an equitable action for breach of confidence. However, having the states legislate for this remedy would help address the uncertainty around being able to seek compensation for emotional distress for an equitable action for breach of confidence.

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.

[1326] ALRC Report 123 (n 778) 50–1.

27. Notifiable Data Breaches Scheme – impact and effectiveness

The Issues Paper sought feedback on the impact of the NDB scheme and whether it is operating effectively,[1327] including by encouraging secure and safe information-handling practices. It also asked whether data breach reporting obligations under other frameworks make it difficult for APP entities to comply with the NDB scheme.

Impact of the NDB scheme

Submissions were largely positive about the impact of the NDB scheme in achieving its policy objective – which is to enable individuals to take action to protect themselves from harm that may result from a data breach. Some submissions said the scheme had fostered transparency and accountability by incentivising entities to assess data breaches early and inform the public of their prevalence.[1328] Several submissions also said it had increased awareness of the importance of information security across industries.[1329] Experian said the scheme had provided clear parameters to measure security practices.[1330] Optus said the scheme had not posed any material compliance challenges.[1331] Similarly, the Financial Services Council said that financial services organisations have been able to implement appropriate controls and processes in response to the scheme's requirements.[1332]

Some submissions provided more critical feedback or indicated the scheme had not had significant impact. Avant Mutual considered that there are misunderstandings about how the scheme operates, which impacts its effectiveness.[1333] Experian noted the main challenge as a multi-national company was adopting common criteria for characterising a data breach and implementing incident management processes to meet the various compliance requirements globally, regionally and domestically.[1334] AGL and Facebook said effective data breach management already formed part of their practices prior to the scheme.[1335] Ai Group said the scheme may only promote a compliance culture as opposed to a proactive leadership and risk management culture. It said the focus should instead be on preventing breaches.[1336]

The Office of the Victorian Information Commissioner noted that the implementation of the NDB scheme has coincided with an increase in voluntary reporting to state privacy regulators.[1337] Further, since the scheme was introduced, Victoria and New South Wales have introduced or proposed their own mandatory data breach schemes.[1338]

[1327] This Chapter completes the impact and effectiveness review of the NDB scheme, which the Issues Paper initiated, to fulfil a commitment in the Regulatory Impact Statement on the Privacy Amendment (Notifiable Data Breaches) Bill 2016.
[1328] Submissions to the Issues Paper: Electronic Frontiers Australia, 14; BSA – the software alliance, 8; Law Institute of Victoria, 18; Office of the Information Commissioner Queensland, 4; Consumer Policy Research Centre, 10; Queensland Law Society, 10.
[1329] Submissions to the Issues Paper: KPMG, 17; ANZ, 16; Optus, 14; Dr Kate Matthews Hunt, 14; Legal Aid Queensland, 17; Griffith University, 20; Calabash Solutions, 11; Data Republic, 18; Gadens, 13; Assured Support, 6; Australian Department of Health, 11; SBS, 9; Australian Financial Markets Association, 16; Law Council of Australia, 25; Privacy108, 18; Karen Meohas, 13; Blancco, 84.
[1330] Submission to the Issues Paper: Experian, 24
[1331] Submission to the Issues Paper: Optus, 14.
[1332] Submission to the Issues Paper: Financial Services Council, 21.
[1333] Submission to the Issues Paper: Avant Mutual, 16.
[1334] Submission to the Issues Paper: Experian, 24.
[1335] Submissions to the Issues Paper: Facebook, 48; AGL Energy Limited, 5.
[1336] Submission to the Issues Paper: Ai Group, 28–9.
[1337] Submission to the Issues Paper: Office of the Victorian Information Commissioner, 10.
[1338] Office of the Victorian Information Commissioner, *Information Security Incident Notification Scheme* (Web Page); NSW Government, *Proposed changes to NSW privacy laws* (Web Page).

Transition from a voluntary to mandatory scheme

Following the initial 712 per cent increase in notifications after the scheme was introduced in 2018,[1339] the rate of increase in the number of data breaches reported to the OAIC has slowed since 2019 and continues to fall.[1340] The OAIC received 446 data breach notifications in the January to June 2021 reporting period, which represented a 16 per cent decrease compared to July to December 2020 (539) and an eleven per cent decrease compared to the first half of 2020 (518).[1341] The notable drop in notifications this year is largely due to a 34 per cent decrease in notifications attributed to human error compared to the previous six months.[1342] While this downward trend may suggest improved internal management of personal information and staff training to minimise human errors, it could also be evidence of underreporting.

The Law Institute of Victoria expressed concern that the number of notifications in Australia are significantly lower than countries that are subject to the GDPR.[1343] The OAIC noted that the number of notifications would invariably be lower than other frameworks because the NDB scheme operates at a higher threshold of serious harm.[1344] The lower numbers may also be attributable to the fact that fewer businesses are required to comply with the NDB scheme than overseas schemes due to the small business exemption.[1345]

Trends in eligible data breaches

Trends by industry

The healthcare and finance (including superannuation) sectors have dominated data breach notifications since the NDB scheme's introduction.[1346] The OAIC's most recent report revealed that these two sectors accounted for the most notifications so far this year (first and second, respectively), followed by professional services, the Australian Government and the insurance sector – together making up the top five reporting industries (see Figure 27.1 below).[1347]

Figure 27.1: Top 5 industry sectors to notify data breaches

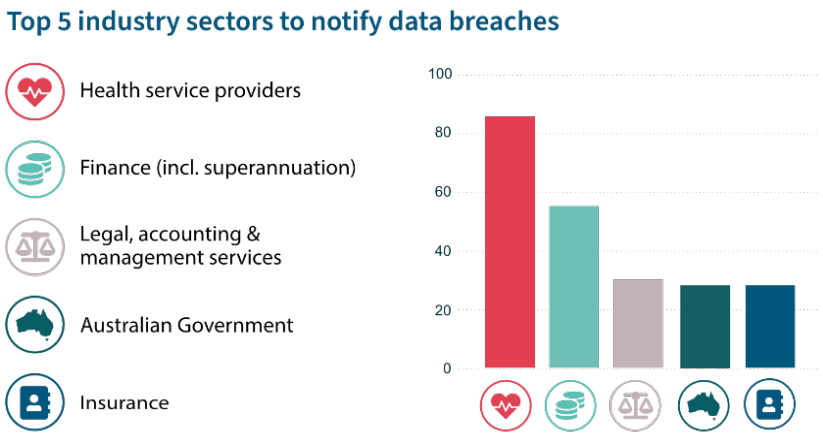


Image reproduced from OAIC, *NDB Report: January–June 2021* (n 971) 1.

[1339] OAIC, *Notifiable Data Breaches scheme 12-month insights report* (Report, 2019) 8 ('*NDB scheme 12-month insights report*').
[1340] 950 notifications were reported in 2018-19 and 1050 in 2019-20. This is an increase of only 11 per cent: OAIC, *Annual Report 2019–20* (n 1236) 13.
[1341] OAIC, *NDB Report: January–June 2021* (n 971) 1; OAIC, *Notifiable Data Breaches Report: July–December 2020* (Report, January 2021) 3; OAIC, *Notifiable Data Breaches Report: January–June 2020* (Report, July 2020) 3 ('*NDB Report: January–June 2020*').
[1342] OAIC, *NDB Report: January–June 2021* (n 971) 5.
[1343] Submission to the Issues Paper: Law Institute of Victoria, 18.
[1344] Submission to the Issues Paper: OAIC, 140.
[1345] Submission to the Issues Paper: OAIC, 140.
[1346] OAIC, 'Notifiable Data Breaches statistics', *Notifiable data breaches* (Web Page) ('*NDB statistics*').
[1347] OAIC, *NDB Report: January–June 2021* (n 971) 7.

The OAIC has said the continued predominance of the healthcare and finance sectors likely reflects the volume and sensitivity of personal information that organisations in these sectors hold.[1348] The two sectors also have long-standing information protection obligations (including duties of confidentiality and strict regulatory frameworks), which may have contributed to their relative maturity and preparedness to meet obligations under the scheme.[1349]

MIGA attributed the high number of notifications in the healthcare sector to the breadth of the scheme's application to health and the broad awareness of the notification requirements within the sector.[1350] Organisations that provide a health service within the meaning of section 6FA are covered by the Act regardless of annual turnover. The OAIC has also said the healthcare sector's lead reporting position is consistent with international trends.[1351]

While healthcare and finance have consistently had the most notifications since 2018, the remaining positions in the top five tend to change, with the education, retail, mining and charity sectors occasionally featuring.[1352] In its submission to the Issues Paper, Google said the OAIC should work closely with the top five reporting industries to provide tailored education on better ways of managing personal information.[1353]

Trends by breach types

'Malicious or criminal attacks' are consistently the largest source of reported data breaches, comprising 65 per cent of all breach notifications in the six months to June 2021.[1354] In this period, 'cyber incidents' made up 66 per cent of malicious or criminal attack-related notifications,[1355] of which ransomware attacks made up 24 per cent (see Figure 27.2 below).[1356] Ransomware-related breach notifications increased by 24 per cent between July to December 2020 and January to June 2021 – up from 37 to 46 notifications.[1357] This increase followed a 150 per cent increase in ransomware notifications between July to December 2019 and January to June 2020.[1358] The Commissioner has recently highlighted these increases, as well as breaches attributed to impersonation fraud, as representing a concerning trend.[1359] The upward trend is also consistent with the Australian Cyber Security Centre's observations of a 15 per cent increase in ransomware attacks between the 2019–20 and 2020–21 financial years.[1360]

Of the top five reporting industries from the previous six months, the healthcare sector reported the most ransomware-related data breaches to the OAIC.[1361] The professional services and finance

[1348] OAIC, *NDB scheme 12-month insights report* (n 1339) 13.
[1349] Ibid.
[1350] Submission to the Issues Paper: MIGA, 3.
[1351] OAIC, *NDB scheme 12-month insights report* (n 1339) 13.
[1352] OAIC, *NDB statistics* (n 1346).
[1353] Submission to the Issues Paper: Google, 12.
[1354] The three sources of breach notifications are malicious or criminal attacks human error and system faults: OAIC, *NDB Report: January–June 2021* (n 971) 14.
[1355] OAIC, *NDB Report: January–June 2021* (n 971) 15.
[1356] Ibid 17.
[1357] Ibid.
[1358] OAIC, *NDB Report: January–June 2020* (n 1341) 15.
[1359] OAIC, 'Data breach report highlights ransomware and impersonation fraud as concerns' (Media Release, 23 August 2021).
[1360] The Australian Cyber Security Centre received 500 ransomware cybercrime reports in the last financial year – more than one a day on average: Australian Cyber Security Centre, *Annual Cyber Threat Report: 1 July 2020 to 30 June 2021* (Report, 2021) 30.
[1361] OAIC, *NDB Report: January–June 2021* (n 971) 27.

sectors also experienced ransomware-related data breaches this year,[1362] consistent with the reported targeting of industries with the ability to pay large ransom amounts.[1363]

Figure 27.2: Cyber incident breakdown – All sectors

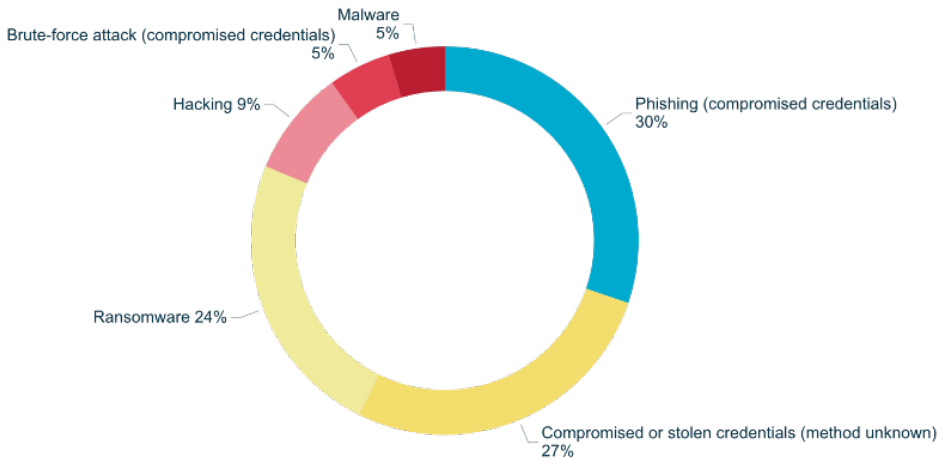


Image reproduced from OAIC, *NDB Report: January–June 2021* (n 971) 17.

APP entities that identify ransomware on their systems should promptly conduct an assessment under section 26WH of the Act to determine if there are reasonable grounds to believe an eligible data breach has occurred. As the Commissioner has said recently, it is insufficient to rely on the absence of data exfiltration or access to avoid this obligation.[1364] A suspicion that a breach *may* have occurred is enough to trigger the assessment requirement. If an entity forms a reasonable belief that any individual to whom relevant personal information affected by the attack relates is at risk of serious harm, such as the harm following public disclosure of their personal information kept on the entity's network, then the entity must prepare a statement and provide a copy to the OAIC.[1365]

Timely reporting of these and other cyber incidents are crucial to ensure the Commissioner can direct its information security guidance where it is most needed and alert other regulators and bodies where necessary. New information sharing provisions proposed in the OP Bill will enable the Commissioner to share information or documents with an enforcement body, alternative complaint body, or other privacy regulators for the purposes of the Commissioner or the receiving body exercising any of their respective functions and powers (subject to safeguards).[1366]

Effectiveness of the NDB scheme

Overall, submitters supported the NDB scheme as effective in achieving its policy objective of enabling individuals to take action to protect themselves from harm resulting from a data breach. However, some submissions said the scheme would be more effective with additional OAIC guidance and education,[1367] and with certain reforms, including:

[1362] 5 and 1, respectively: OAIC, *NDB Report: January–June 2021* (n 971) 27.

[1363] See, eg, David Claughton and Nikolai Beilharz, 'JBS Foods pays $14.2 million ransom to end cyber attack on its global operations', *ABC News* (online, 10 June 2021); Adam Langenberg, 'Ransomware attack to blame for Federal Group's casino pokies outage in Tasmania', *ABC News* (online, 13 April 2021); James Purtill, 'Australian organisations are quietly paying hackers millions in a 'tsunami of cyber crime'', *ABC News* (online, 16 July 2021) .

[1364] See Ry Crozier, 'Australian businesses stop reporting ransomware attacks over exfiltration doubts', *IT News* (online, 23 August 2021).

[1365] *Privacy Act* (n 2) s 26WK.

[1366] Exposure Draft, OP Bill (n 1) s 33A.

[1367] Submissions to the Issues Paper: Clubs Australia, 5; Karen Meohas, 13; Privcore, 4; KPMG, 17; Cyber Security Cooperative Research Centre, 15; Communications Alliance, 13.

- harmonising domestic and international frameworks
- assigning responsibility for multi-party breaches
- ensuring timely assessment and notification
- revisiting the serious harm threshold, and
- addressing the impact of breaches on individuals and mitigating harm.

Harmonising with domestic schemes

Some submissions were concerned about overlapping reporting obligations and said that alignment of the NDB scheme with other domestic schemes, including the APRA information security standard,[1368] proposed state and territory schemes, and notification of cyber security incidents under the Security Legislation Amendment (Critical Infrastructure) Bill 2020 ('Critical Infrastructure Bill')[1369] should be considered.[1370]

Some submissions expressed concern about the overlap between the NDB scheme and the data breach scheme in the MHR Act. Avant Mutual and the Australian Medical Association said that complying with both the NDB scheme and the MHR scheme was administratively burdensome, requiring different processes and procedures depending on which scheme applies.[1371] The Australian Digital Health Agency supported harmonisation in favour of the NDB scheme, noting that the definition of 'breach' in the MHR scheme requires notification even where there is no risk of harm.[1372]

The NSW Information and Privacy Commission (NSWIPC) and Queensland Office of the Information Commissioner said harmonisation of the NDB scheme with state and territory mandatory schemes as they emerge is important for national consistency and to decrease compliance burden on entities.[1373] The NSWIPC also noted that some provisions of the NDB scheme apply to NSW Government agencies.[1374]

Harmonising with international schemes

Some submissions supported international consistency to the extent that it is feasible, noting that complete harmonisation would be difficult to achieve.[1375] Gadens submitted that 60 per cent of respondents to a survey they conducted had experienced significant difficulties complying with both the NDB scheme and international frameworks, particularly small and medium entities looking to reach overseas markets.[1376]

Most submissions did not specify which aspects of the NDB scheme should be amended to harmonise with overseas regimes, aside from being in favour of the GDPR's distinction between data processors and data controllers, discussed further below and in Chapter 21. Experian said that harmonisation could be achieved by making it easier to formally share information about data breaches across schemes.[1377] Microsoft said there was benefit in a coordinated regional mechanism

---

[1368] *Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 1 of 2018* ('*APRA Prudential Standard CPS 234*').
[1369] Submissions to the Issues Paper: Griffith University, 20; Office of the Information Commissioner Queensland, 4.
[1370] Submissions to the Issues Paper: Queensland Law Society, 10; ANZ, 16; Western Union, 4; Avant Mutual, 16; Australian Medical Association, 12.
[1371] Submissions to the Issues Paper: Avant Mutual, 16; Australian Medical Association, 12.
[1372] Submission to the Issues Paper: Australian Digital Health Agency, 1.
[1373] Submissions to the Issues Paper: New South Wales Information and Privacy Commission, 5; Office of the Information Commissioner Queensland, 4.
[1374] Submission to the Issues Paper: New South Wales Information and Privacy Commission, 4.
[1375] Submissions to the Issues Paper: Facebook, 48; Google, 13; Snap Inc., 6; ANZ, 16.
[1376] Submission to the Issues Paper: Gadens, 14.
[1377] Submission to the Issues Paper: Experian, 24. See also Submission to the Issues Paper: Privacy108, 18.

for data breach notifications.[1378] Griffith University suggested the OAIC implement an online 'notify us' tool as is used in New Zealand.[1379]

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?

Assigning responsibility for multi-party breaches

As the scheme applies to APP entities that 'hold' personal information,[1380] which includes information in their control (if not physical possession), it is possible for more than one entity to have notification obligations in relation to the same eligible data breach. However, the scheme incentivises entities to avoid multiple notifications where they can, by relieving entities of the requirement to assess and notify a data breach if another entity has already done so.[1381]

Submissions from businesses and not-for-profits, including Microsoft and Atlassian said the scheme should do more to resolve reporting obligations when multiple entities are involved.[1382] Some pointed to common scenarios that might give rise to multi-party breaches, such as when an entity engages cloud service providers or online recruitment services.[1383] Gadens said that third party entities that do not have direct contractual arrangements with the main organisation should be expressly required to assist the reporting entity if the breach originates from their actions.[1384]

Some submissions were in favour of introducing a distinction in the Act between data controllers and processors, on the basis that this would reduce delays in breach notifications that arise when entities must determine between themselves which entity will notify.[1385] The Information Technology Industry Council said that only data controllers should be required to notify individuals, but Atlassian said that splitting responsibility would likely be more complex than merely assigning responsibility to one party.[1386]

The scheme's current approach to multi-party breaches serves a protective function by ensuring that if one APP entity fails to notify, the other APP entities are still responsible for notifying. This recognises that it is better for individuals to occasionally be notified more than once about a data breach than to not be notified at all. This rationale also accounts for the difficulty in providing a clear mechanism to distinguish responsibility, as each multi-party breach will be unique in the number and type of entities and contractual arrangements involved. The scope of the Act also makes it difficult to provide such a mechanism because notification obligations cannot be imposed on an entity that is not covered by the Act (such as small businesses) even if a data breach originates from them. There may also be some instances where APP entities elect to jointly notify individuals (for example, by providing contact details for each entity), such as for reputational reasons.[1387]

[1378] Submission to the Issues Paper: Microsoft, 5–6.
[1379] Submission to the Issues Paper: Griffith University, 20.
[1380] *Privacy Act* (n 2) sub-s 26WE(1)(a).
[1381] Ibid ss 26WJ, 26WM.
[1382] Submissions to the Issues Paper: Avant Mutual, 17; Privacy108, 18; KPMG, 17; ANZ, 16; Law Council of Australia, 26; Queensland Law Society, 10; Gadens, 14; Microsoft, 1–2; Atlassian, 3.
[1383] Submissions to the Issues Paper: KPMG, 17; Gadens, 13–14.
[1384] Submission to the Issues Paper: Gadens, 13–14.
[1385] Submissions to the Issues Paper: Records and Information Management Professionals of Australasia, 6; Australian Banking Association, 8; BSA | The Software Alliance, 8; Microsoft, 1–2; Information Technology Industry Council, 1.
[1386] Submissions to the Issues Paper: Information Technology Industry Council, 4; Atlassian, 3.
[1387] *Privacy Act* (n 2) sub-s 26WK(4).

Ensuring timely assessment and notification

Submitters were divided on whether the current notification and assessment time periods are adequate and appropriate. Some submissions, including from not-for-profit organisations and the OAIC recommended the scheme clarify or specify timeframes for notification.[1388] Palo Alto Networks suggested that instead of requiring entities to notify 'as soon as practicable', as per the current requirement, entities should report eligible data breaches within 7-10 business days, or at least 'as soon as is reasonably practicable' or 'without undue delay'.[1389]

Submissions from businesses said the current requirements allow the appropriate amount of flexibility, and recognise that what constitutes a 'practicable' timeframe will vary depending on the breach and the entity.[1390] IDCARE expressly opposed a 72-hour reporting timeframe, as is partly required under the GDPR, on the basis that entities are unlikely to have a good understanding of the breach at that point.[1391] However, some also said, in consensus with submissions in favour of change,[1392] that further clarification was necessary about when the notification time period commences.[1393]

The OAIC's submission referred to its January to June 2020 report on the NDB scheme, which indicated that almost three-quarters of APP entities notified the regulator within 30 days of becoming aware of a suspected data breach, including the time taken to assess the breach as eligible for notification.[1394] This figure has decreased to 72 per cent in the six months to June 2021.[1395] The OAIC has observed an increasing trend in which entities conclude their assessment within 30 days as required but take several more weeks or months to notify the OAIC – on the basis that this is 'as soon as is practicable' and therefore in accordance with the current reporting requirements.[1396] From January to June 2021, approximately 15 per cent of reporting entities took more than 60 days to notify the OAIC of an eligible data breach from when they first became aware of an incident (see Figure 27.3 below).[1397] Twenty seven entities took longer than 120 days.[1398]

Figure 27.3: Days taken to notify the OAIC of data breaches – All sectors

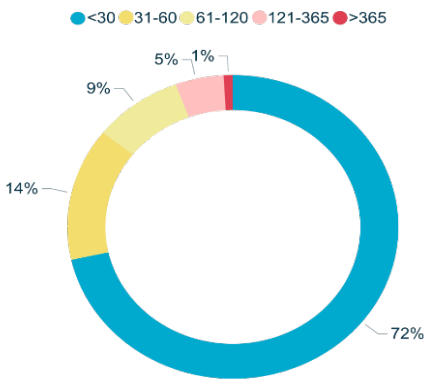


Image reproduced from OAIC, *NDB Report: January–June 2021* (n 971) 13.

[1388] Submissions to the Issues Paper: Electronic Frontiers Australia, 14; Australian Privacy Foundation, 39; Consumer Policy Research Centre, 10; OAIC, 142–4.
[1389] Submission to the Issues Paper: Palo Alto Networks, 5.
[1390] Submission to the Issues Paper: Information Technology Industry Council, 4. See also Submissions to the Issues Paper: AGL Energy Limited, 5; ANZ, 16; Google, 12.
[1391] Submission to the Issues Paper: IDCARE, 7.
[1392] Submission to the Issues Paper: Palo Alto Networks, 5.
[1393] Submissions to the Issues Paper: Information Technology Industry Council, 4; Snap Inc., 6.
[1394] OAIC, *NDB Report: January–June 2020* (n 1341) 19. See also Submission to the Issues Paper: OAIC, 142.
[1395] OAIC, *NDB Report: January–June 2021* (n 971) 12.
[1396] *Privacy Act* (n 2) sub-ss 26WK(2)(b), 26WL(3).
[1397] OAIC, *NDB Report: January–June 2021* (n 971) 13.
[1398] Ibid 12.

To safeguard the effectiveness of the scheme, the OAIC recommended in its submission that entities should be required to assess, investigate and notify a data breach to the OAIC as soon as practicable, but no later than 30 days, with notification to individuals as soon as practicable thereafter but no later than 5 days. The OAIC also considered that a civil penalty provision should attach to notification timeframes with an ability for the IC to issue infringement notices.[1399]

In light of the current proportion of entities notifying the OAIC within the 30 day timeframe and individuals shortly thereafter, it is not clear that changing the legislated timeframe is warranted at this time. However, this may require further consideration if the trend of entities taking several months to comply with their notification obligations continues to increase. Entities that fail to notify individuals in a timely manner risk undermining the policy objective of the scheme. Delays in assessment and notification make it difficult for individuals to mitigate the likelihood that they might suffer financial or other forms of serious harm.

Proposal 24.1 would introduce a new civil penalty provision for any interference with privacy, including where an APP entity has failed to notify either the OAIC or affected individuals as soon as practicable, which would allow the IC to address lack of timely notification without the need for it to be serious or repeated.[1400]

Revisiting the serious harm threshold

Submissions also had differing views about the appropriateness of the current threshold that triggers reporting obligations under the NDB scheme. Some submissions were concerned the threshold – 'likely to result in serious harm' – was too high or too rigid to appreciate the variability in risk.[1401] The Consumer Policy Research Centre said requiring entities to notify less serious breaches might provide insights to the OAIC on inadequate information handling and security practices, to prevent significant breaches from occurring in the first place.[1402] Some submissions expressed concern about the effectiveness of self-assessment by entities and their ability to determine whether a reasonable person would consider the breach would be likely to result in serious harm.[1403]

Some submitters were concerned that any lowering of the threshold would significantly increase compliance burden on businesses.[1404] A small number of submitters said the GDPR's standard for when individuals should be notified – 'likely to result in a serious risk to the rights and freedoms of natural persons' – should be adopted to ensure that small breaches that do not affect anyone are not reported.[1405] Avant Mutual proposed an exception to the obligation to notify where doing so would pose a serious threat to the life, health or safety of an individual.[1406]

The current threshold ensures individuals are only notified of breaches that are likely to result in serious harm. The scheme purposefully sets a high threshold to ensure individuals do not experience notification fatigue and to avoid unnecessary regulatory and reputational costs for entities. There may also be little benefit in lowering the threshold where APP 11 already operates as a preventative obligation, requiring entities to take reasonable steps to keep information secure. The current threshold also does not prevent entities from choosing to notify the OAIC and individuals about data

[1399] Submission to the Issues Paper: OAIC, 144.
[1400] *Privacy Act* (n 2) sub-s 13(4A).
[1401] Submissions to the Issues Paper: Cyber Security Cooperative Research Centre, 14; Queensland Law Society, 10; Electronic Frontiers Australia, 14.
[1402] Submission to the Issues Paper: Consumer Policy Research Centre, 11.
[1403] Submissions to the Issues Paper: Dr Kate Matthews Hunt, 14; Cyber Security Cooperative Research Centre, 14.
[1404] Submission to the Issues Paper: Information Technology Industry Council, 4.
[1405] Submissions to the Issues Paper: Palo Alto Networks, 5; Snap Inc., 6; Information Technology Industry Council, 4; AusPayNet, 13.
[1406] Submission to the Issues Paper: Avant Mutual, 17.

breaches that do not meet the threshold, such as in the interests of maintaining good public relations.

Addressing the impact of breaches on individuals and mitigating harm

Some submissions said the NDB scheme should place more emphasis on the steps taken by an entity to remedy or mitigate a data breach.[1407] IDCARE said there is confusion on what measures are effective and what can be done proactively ahead of notification.[1408] The OAIC recommended that entities be required to take reasonable steps to mitigate the adverse impacts or risk of harm that may arise for individuals as a result of a data breach.[1409] The OAIC has observed that some entities are already taking responsibility for the costs and impacts of data breaches and supporting individuals, including by paying for a credit monitoring service, which alerts affected individuals if there are changes to their credit report; monitoring the dark web to identify if personal information compromised in a data breach is being traded online; assisting individuals to replace compromised credentials, such as passports and drivers licences; and engaging providers such as IDCARE to provide post-incident support to individuals.

Proposal – statement to set out steps taken by entities in response to a breach

In recognition that individuals would benefit from further information about how an entity has dealt with an eligible data breach involving their personal information, the Act could be amended so that an entity would be required to set out what steps it has taken or intends to take in response to the breach. This requirement would bring the NDB scheme in line with the New Zealand approach.[1410]

The proposal would be consistent with the overarching policy rationale of the scheme by ensuring individuals have relevant information to protect themselves from harm. Individuals would benefit from knowing, for example, that an entity has set up a dedicated support line or website they can access for more information about the breach and actions they might take. It would also assist individuals to know whether the entity has contacted the relevant government agencies to notify them of a data breach involving their tax file numbers or Medicare information.

Greater transparency about what actions entities are taking in response to a data breach may also inform the OAIC's regulatory response, including the guidance it provides to entities about best-practice data breach responses and cyber security generally, which entities can benchmark themselves against.

In recognition that APPs 1 and 11 already require entities to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and to keep information secure, the proposal would not require entities to take positive steps to mitigate harm as recommended by the OAIC. The proposal would also not affect the remedial action exception in section 26WF, which relieves entities from notification obligations where they have taken action before serious harm occurs to individuals, such that serious harm is not likely to occur. Relatedly, Chapter 24 proposes a reform to section 52 determinations to permit the IC to require an entity to take reasonable steps to mitigate potential future loss or damage resulting from an interference with privacy.

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.

[1407] Submissions to the Issues Paper: OAIC, 144; Salesforce, 4; IDCARE, 6; Ai Group, 29; Privcore, 4.
[1408] Submission to the Issues Paper: IDCARE, 6.
[1409] Submission to the Issues Paper: OAIC, 144–5.
[1410] *Privacy Act* (NZ) (n 29) sub-ss 117(1)(b), (2)(b).

28. Interactions with other schemes

The final chapter of the Issues Paper addressed the Act's interaction with other schemes and pieces of legislation that relate to privacy, such as the MHR Act, FOI Act, Archives Act, the Online Safety Act, and state and territory privacy laws.[1411] The chapter also examined the OAIC's relationship with other regulators, including the ACCC, ACMA, IGIS and ONDC – particularly in circumstances where privacy breaches are capable of amounting to breaches of other legislation.

The Issues Paper sought feedback on whether there should continue to be separate privacy protections to address specific risks and concerns, whether there is a need for greater harmonisation of privacy protections under Commonwealth law and whether the compliance obligations in certain sectors are proportionate and appropriate to public expectations.

Submissions to the Issues Paper expressed a high level of interest in these issues, particularly about the complexity of Commonwealth privacy schemes, the roles of regulators, and inconsistency between Commonwealth, state and territory privacy laws. These submissions came from a range of stakeholders, including government departments, regulators, industry peak bodies, consumer groups, technology companies and healthcare organisations.[1412]

Interaction between the Act and other Commonwealth schemes

How the Act interacts with other Commonwealth schemes

Generally, the Act provides a baseline of protection upon which more specific requirements can be imposed through the operation of other legislation. Subsequent legislation may specify whether it will operate concurrently with the Act, or override it.[1413] In the absence of such provisions, the Act contains a number of mechanisms that govern interactions with other laws, which operate in addition to general rules of interpretation.[1414]

The broadest such mechanism is the 'authorised by law' exception.[1415] A number of the APPs provide an exception if an APP entity is 'required or authorised by or under an Australian law or a court/tribunal order' to act contrary to the APPs – for example, when disclosing information for a secondary purpose.[1416] An 'Australian law' is broadly defined to include a Commonwealth, state or territory Act, regulation or other instrument made under such an Act.[1417] An APP entity will be 'authorised' when permitted to do something under another law, provided clear language is used.[1418]

There are also a large number of secrecy and non-disclosure provisions across Commonwealth legislation that are specific to certain schemes, notably in service-delivery portfolios, such as taxation and the payment of government benefits.[1419] These have not been considered in depth as their objective is to facilitate those programs (many of which pre-date general privacy laws) rather than being directed at protecting privacy.

[1411] See *MHR Act* (n 744); *Online Safety Act* (n 605).
[1412] See, eg, Submissions to the Issues Paper: ADHA; AFMA; Ai Group; Allens Hub for Technology, Law and Innovation; Atlassian; ACCC; Consumer Policy Research Centre; Facebook; illion; KPMG; MIGA; OAIC; Telstra.
[1413] See, eg, *MHR Act* (n 744) Division 4 – Interaction with the Privacy Act 1988.
[1414] See, eg, *Acts Interpretation Act* (n 104) ss 15AA, 15AB.
[1415] This discussion is intended to cover all formulations of this phrase mentioned in OAIC, APP Guidelines (n 21) [B.128].
[1416] See, eg, *Privacy Act* (n 2) sch 1 APP 6.2(b).
[1417] *Privacy Act* (n 2) sub-s 6(1) 'Australian Law'. See below for further discussion of state and territory privacy laws.
[1418] OAIC, APP Guidelines (n 21) [B.130]–[B.132]. See *Coco v The Queen* (1994) 179 CLR 427.
[1419] See, eg, ALRC, Secrecy Laws and Open Government in Australia (Report No 112, March 2010), which outlines many of these provisions.

Complexity is increasing

Submissions noted that Commonwealth privacy laws spanning different government portfolios impose complex compliance requirements upon APP entities that are subject to multiple schemes.[1420] Privacy protections in different pieces of legislation also tend to be structured differently, and the OAIC is given varying roles in relation to each scheme.[1421] Although each scheme benefits from tailored additional privacy protections, this results in a lack of consistency.

The ALRC identified fragmentation of Commonwealth privacy laws as an issue in Report 108 – expressing concern about the associated costs, confusion and information-sharing issues.[1422] In the years since, new laws have been introduced that add to this framework, such as the CDR, My Health Records legislation and state and territory privacy laws.[1423]

The following example illustrates the level of complexity that APP entities may have to grapple with, by outlining how a number of frameworks may apply to a single APP entity.

Case study

A bank collects a client's personal information as part of processing a home loan application.

- As an APP entity, the bank must generally comply with the APPs in respect of how this personal information is collected, used and disclosed.
- To assess the clients' suitability for a home loan and predict their ability to repay the loan amount applied for, the bank needs to perform a credit check through a credit reporting body. As a credit provider, the bank must comply with Part IIIA of the Act and the Privacy (Credit Reporting) Code 2014 when handling this credit reporting information.
- To confirm the client's taxable income, the bank collects Tax File Number information and must comply with the TFN Rule.[1424]
- If AI is used to help determine whether to lend, the bank should also consider the Department of Industry, Science, Energy and Resources' AI Ethics Principles in addition to legal considerations.[1425]
- A year later, the client wants to refinance their home loan. They ask the bank to share their information with other banks through the CDR system in order to find the best deal for their financial situation. When sharing this information, the bank must comply with the CDR Privacy Safeguards and the CDR rules, in addition to the above frameworks.
- More generally, the bank must also comply with APRA Prudential Regulation CPS 234 in respect of its cybersecurity practices, including security of personal information – to ensure that it can continue to meet its obligations to shareholders.
- In future, if the bank is designated as a critical infrastructure entity, further cyber security obligations may apply under the Critical Infrastructure Bill.[1426]

[1420] See Submissions to the Issues Paper: Australian Banking Association, 1, 4; Consumer Policy Research Centre, 11–12; Centre for Cyber Security Research and Innovation, 2; Australian Communications Consumer Action Network, 6.

[1421] See, eg, the CDR privacy safeguards in *CCA* (n 67) Div 5 as compared to credit reporting provisions in *Privacy Act* (n 2) Pt IIIA, as compared to the Data Availability and Transparency Bill 2020, cls 28, 37–8 (*'DAT Bill'*). The privacy protections in the forthcoming Digital Identity legislation are also currently subject to consultation. See Digital Transformation Agency, *Digital Identity Legislation – Consultation Paper* (Web Page, 2020), 41.

[1422] ALRC Report 108 (n 53) [13.2]–[13.16].

[1423] See, eg, *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth); *MHR Act* (n 744); *Information Privacy Act 2014* (ACT).

[1424] OAIC, *Your Tax File Number* (Web Page, 2020); Privacy (Tax File Number) Rule 2015.

[1425] Australian Government – Department of Industry, Science, Energy and Resources, *AI Ethics Principles* (Web Page, November 2019).

[1426] Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth) (*'Critical Infrastructure Bill'*).

Additional protections are warranted, but consistency should be encouraged

Submissions generally supported creating specific legislation to impose more stringent privacy protections where justified for high privacy risk activities.[1427] For example, the MHR scheme is supported by additional legislated privacy obligations which reflect community expectations that a large-scale repository of highly sensitive health information requires additional safeguards.[1428] Submissions supported a tiered approach to risk management when additional legislation is developed – linking greater oversight and enforcement powers to the level of privacy risk.[1429]

Despite this general support, submissions also highlighted inconsistencies across different schemes and referred to 'fragmentation' or 'differential standards' in reference to how the Act interacts with a number of initiatives, including CDR and the OP code.[1430] Submissions from industry stakeholders highlighted the regulatory burden associated with complying with multiple laws, especially where certain sectors are subject to higher levels of privacy regulation.[1431] Consumer advocacy groups called for greater consistency across privacy-related legislation on the basis that it would simplify regulatory requirements, minimise unforeseen impacts on innovation and support the digital economy to recover from the impacts of COVID-19.[1432]

In light of these concerns, submissions generally advocated for a cautious approach to introducing additional legislation, or recommended creating greater consistency.[1433] Others went further to propose models to harmonise or simplify how additional or scheme-specific Commonwealth privacy protections are implemented.[1434] Options discussed included reviewing laws to centralise stronger protections within the Act, introducing codes or rule-making powers, or addressing additional concerns in separate legislation.[1435]

Specific interactions of concern to submitters

Several submissions addressed how particular Commonwealth schemes interact only with specific aspects of the Act and recommended reform options to reduce these overlaps. Telstra and Optus both indicated that Part 13 of the Tel Act imposes additional obligations on carriage service providers when handling personal information.[1436] Part 13 of the Tel Act includes prohibitions on carriage service providers using or disclosing information relating to the content or substance of communications.[1437] The Communications Alliance advocated for the repeal of most of Part 13 of the Tel Act on the basis of duplication and inconsistency.[1438]

Submitters also highlighted overlap between APP 7, and the requirements of the Spam Act and the DNCR Act, with ACMA advocating for common principles for consent and opt-outs across these

---

[1427] Submissions to the Issues Paper: Anonymous 6, 2–3; Australian Privacy Foundation, 39; OAIC, 147–9; Salinger Privacy, 9–10.
[1428] Submissions to the Issues Paper: Australian Digital Health Agency, 2. See also re credit reporting, Legal Aid Queensland, 17–8.
[1429] Submission to the Issues Paper: Minderoo Tech and Policy Lab – University of Western Australia School of Law, 10–13.
[1430] Submissions to the Issues Paper: Atlassian, 1; Facebook, 6; KPMG, 17, 22; elevenM, 3.
[1431] Submissions to the Issues Paper: Ai Group, 6; Optus, 15–16.
[1432] Submissions to the Issues Paper: Consumer Policy Research Centre, 14; See also Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 50.
[1433] See, eg, Submissions to the Issues Paper: Australian Digital Health Agency, 2; Facebook, 48.
[1434] Submissions to the Issues Paper: Ai Group, 6; elevenM, 3; AusPayNet, 5; MIGA, 5.
[1435] Submissions to the Issues Paper: Australian Digital Health Agency, 3; Minderoo Tech and Policy Lab – University of Western Australia School of Law, 10–13, OAIC, 147.
[1436] Submissions to the Issues Paper: Optus, 15–16; Telstra Ltd and Telstra Health Pty Ltd, 12–13, 19.
[1437] *Telecommunications Act 1979* (Cth) ss 276–78.
[1438] Submission to the Issues Paper: Communications Alliance, 10–11.

frameworks.[1439] This interaction is discussed further in Chapter 16 (Direct marketing, targeted advertising and profiling).

In relation to security of personal information obligations under APP 11, submissions highlighted that APRA Prudential Standard 234 provides more detailed cybersecurity obligations for APRA-regulated entities such as banks and insurance brokers than apply under the Act.[1440] This standard also requires regulated entities to notify APRA of certain information security incidents, including those notified to the OAIC under the NDB scheme.[1441] If enacted, the Critical Infrastructure Bill would introduce additional security obligations and data breach notification requirements for critical infrastructure entities, most of which are APP entities.[1442] The Voluntary Internet of Things Code of Practice also provides guidance on product security, both in respect of personal information and more broadly.[1443]

Proposal

Privacy law design guide for new privacy-related legislation

To assist with addressing concerns raised by submitters regarding inconsistency and overlap between Commonwealth privacy law frameworks, the Attorney-General's Department could develop a non-binding privacy law design guide to assist Australian Government departments when developing schemes which require additional privacy protections or otherwise seek to override the APPs.

This guide could provide information on the types of matters to be considered by departments during the policy development and legislative process – such as factors relevant to determining when privacy protections that go beyond those set out in the APPs are warranted,[1444] how additional protections should be drafted, and relevant oversight and enforcement mechanisms recommended to apply to such schemes. An example of this type of guide is the AGD's existing Guide to Framing Commonwealth Offences, Infringement Notice and Enforcement Powers, and the NZ Legislation Guidelines.[1445] Such guides are policy-neutral but are intended to guide departments and parliamentary committees on the creation of consistent legislation.[1446]

This proposal recognises that different privacy protections are justified in certain circumstances, but increasing consistency will support APP entities' compliance capacity, reduce regulatory impost, and facilitate easier sharing of personal information and anonymised data.[1447] The proposal would also contribute to greater uniformity of the various privacy laws and schemes within the IC's jurisdiction.[1448]

Several submissions suggested creating greater consistency through legislation. For example, Queensland Law Society suggested that, 'a master set of privacy and data law principles, capable of cross-referencing and legislative adaptation' would be appropriate where schemes wanted to

---

[1439] Submissions to the Issues Paper: ACMA, 5–6; Gadens, 8; OAIC, 45. See also, ALRC Report 108 (n 53), Chapter 71 – Telecommunications.
[1440] Submission to the Issues Paper: Gadens, 14.
[1441] APRA Prudential Standard CPS 234 (n 1368) cls 35–6.
[1442] Critical Infrastructure Bill (n 1426).
[1443] Department of Home Affairs, *Code of Practice – Securing the Internet of Things for Consumers*, (Web Page, 2020); See also, Submission to the Issues Paper: Centre for Media Transition – UTS, 17.
[1444] See Submission to the Issues Paper: Legal Aid Queensland, 17–8.
[1445] AGD, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, (n 1179); New Zealand Legislation Design and Advisory Committee, *Legislation Guidelines: 2018 Edition*, (Report, 2018).
[1446] See, eg, the reference of the Guide to Framing Commonwealth Offences (n 1179) by the Parliamentary Joint Committee on Human Rights, *Guidance note on offence provisions and civil penalties,* (Web Page, 2014).
[1447] See, eg, Submission to the Issues Paper: Faculty of Engineering and IT - University of Technology Sydney.
[1448] See Submission to the Issues Paper: OAIC, 146–7.

impose stronger privacy protections.[1449] Electronic Frontiers Australia suggested a similar layered approach of increased protections based on increased sensitivity.[1450]

The Centre for Cyber Security Research and Innovation called for the development of a Unified Data Protection Code, and a central Digital Data Authority, noting that 'amending the Privacy Act, as a stand-alone legislation, cannot fully resolve the existing core problem in this area, namely, the fragmentation of and inconsistencies within the legal regime'.[1451] Other stakeholders also supported more coordinated government-wide strategy for data initiatives, including the Ai Group, the Consumer Policy Research Centre and the Australian Banking Association.[1452]

To support the law design guide, OAIC guidance could set out information on how the Act interacts with other schemes in greater detail.[1453] Enhanced guidance would help respond to concerns of submitters who called for a greater degree of sectoral guidance about how to comply with the Act.[1454] The guidance could also be shared on the websites of other regulators or sectoral EDR 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.

Interactions between the OAIC and other regulators

Another concern raised in submissions was that privacy-related litigation is being pursued by other regulators, leading to overlap between the functions of the OAIC and other regulators.

Role of the OAIC and other regulators

The OAIC has enforcement and complaint-handling functions under the Act, as well as Acts listed in the AIC Act.[1455] The OAIC is also the privacy regulator under other legislation, such as the CDR scheme under the CCA.[1456]

Privacy complaint handling functions are also undertaken by EDR schemes which operate in certain sectors.[1457] These schemes are approved by the IC under section 35A of the Privacy Act. More detail on the IC's complaint handling function and EDR schemes is set out in Chapter 24 (Enforcement).[1458]

To enhance cooperation with other regulators and provide greater transparency about regulators' roles and interactions, the OAIC has entered into memoranda of understanding (MoUs) with other regulators, including the ACMA, ADHA, IGIS and ACCC.[1459] MoUs of this kind are common among Data Protection regulators overseas such as the UK ICO.[1460] Despite these MoUs, the OAIC noted

[1449] Discussed with reference to why justified in the context of credit reporting - Submissions to the Issues Paper: Queensland Law Society, 10.
[1450] Submission to the Issues Paper: Electronic Frontiers Australia, 16.
[1451] Submission to the Issues Paper: Centre for Cyber Security Research and Innovation, 13.
[1452] Submissions to the Issues Paper: Ai Group, 30; Australian Banking Association, 1; Consumer Policy Research Centre, 14. Work on an overarching government digital economy strategy is underway: Australian Government – Department of the Prime Minister and Cabinet, Digital Economy Strategy (Web Page, 6 May 2021).
[1453] Existing guidance includes: 'Authorised by law' in OAIC, APP Guidelines (n 21) [B.128]–[B.137]; in respect of interaction with the MHR Act – OAIC, Guide to health privacy — OAIC (Web Page, September 2019); extensive guidance on the CDR – OAIC, June 2020, Guidance and advice — OAIC (Web Page, June 2020).
[1454] Submission to the Issues Paper: Salesforce, 4.
[1455] *AIC Act* (n 1228) s 9.
[1456] See, eg, *CCA* (n 67) ss 56EQ, 56ER, 56GA. A more exhaustive list of OAIC responsibilities is contained in Submission to the Issues Paper: OAIC, 146–7.
[1457] Current privacy EDR schemes include the Australian Financial Complaints Authority, state-based Energy and Water Ombudsmen, and the Telecommunications Industry Ombudsman ('*TIO*'). These schemes are well-utilised – the TIO handled 4,328 complaints involving privacy issues in Financial Year 2020. See, Submission to the Issues Paper: TIO, 1.
[1458] Decisions to recognise EDR schemes are also made in accordance with guidelines found at OAIC, *Guidelines for recognising external dispute resolution schemes,* (Web Page, 2013).
[1459] Submission to the Issues Paper, OAIC, 147; Full list of MOUs can be found at OAIC, *MOUs* (Web Page, 2020).
[1460] UK ICO, *Working with other bodies* (Web Page, 2021).

that it is prevented from sharing certain information about investigations with other regulators due to confidentiality provisions in section 29 of the AIC Act.[1461] The OP Bill will enhance the OAIC's ability to share information with other regulators.

Enforcement by other regulators concerning personal information

Submissions noted the incidence of other regulators taking enforcement action in relation to businesses' personal information handling practices.[1462] These cases have been brought by the ACCC against online platforms under the misleading or deceptive conduct provisions of the ACL, and by ASIC in relation to security of personal information obligations under the *Corporations Act 2001* (Cth).[1463]

In the first of these cases, under the ACL, the Federal Court ordered HealthEngine, an online healthcare booking service, to pay $2.9 million for engaging in misleading conduct, which included sharing details of more than 135,000 patients with third-party private health insurance brokers, without adequately notifying customers.[1464] In the ACCC's more recent case against Google under the ACL, the Federal Court found that Google misled consumers about how they collected personal location data through Android mobile devices.[1465] The third case by ASIC alleges that RI Advice Group, a financial services license holder, failed to have adequate cyber security systems.[1466]

Under the current division of regulatory responsibilities, the ACCC can take action in relation to data practices which may infringe the ACL. If these data practices also breach the Privacy Act, the OAIC and ACCC collaborate regarding appropriate enforcement action as per their MoU.[1467] While Oracle's submission queried whether the ACCC should, concurrently with the OAIC, be empowered to take action to enforce the Act where the conduct would constitute a breach of both the ACL and the Act,[1468] the ACCC and OAIC submissions supported the current division of responsibility between the regulators.[1469] The ACCC submission also emphasised the importance of ensuring that the OAIC has the full suite of enforcement and investigative tools it needs.[1470] The OP Bill will enhance the OAIC's enforcement mechanisms, and increase the maximum civil penalty for serious and/or repeated interference with privacy to more closely align with penalties available under the ACL.[1471]

Submitters also raised concerns about other regulators' roles in relation to privacy, including the ONDC and the ACMA. The Australian Privacy Foundation described the issue as one of 'regulatory balkanisation', which 'confuses consumers, enables exploitation by APP entities and fosters incapacitation on the part of regulators'.[1472] Submissions proposed fewer options in relation to these relationships, but suggested that one regulator could act as a point of focus for certain types of

---

[1461] Submission to the Issues Paper: OAIC, 148.
[1462] See, eg, Submission to the Issues Paper: Oracle, 6.
[1463] See, eg, *ACCC v Google LLC (No 2)* [2021] FCA 367.
[1464] *ACCC v HealthEngine Pty Ltd* [2020] FCA 1203; See also, ACCC, *Media Release* - *HealthEngine to pay $2.9 million for misleading reviews and patient referrals* (Web Page, 20 August 2020).
[1465] *Australian Competition and Consumer Commission v Google LLC (No 2)* [2021] FCA 367.
[1466] *ASIC v RI Advice Group Ltd*; discussed in Submission to the Issues Paper: Assured Support, 6. See also, ASIC, *Media Release – ASIC commences proceedings against RI Advice Group Pty Ltd for alleged failure to have adequate cyber security systems* (Web Page, 21 August 2020).
[1467] OAIC, *MOU with ACCC – Exchange of Information* (Web Page, August 2020) cls 6.4, 7.2(a).
[1468] See, eg, Submission to the Issues Paper: Oracle, 15.
[1469] Submissions to the Issues Paper: OAIC, 89, 119–29, 146–50; ACCC, 5.
[1470] Submission to the Issues Paper: ACCC, 7–8.
[1471] Under the ACL, penalties are significantly higher than under the Act. For example, the maximum civil penalty for a serious and repeated interference with privacy under the Act is $220,000 (s 13G) compared to a maximum civil penalty for a corporation under the ACL of $10,000,000, three times the value of the benefit received, or 10% of the annual turnover in the preceding 12 months: *CCA* (n 67) sch 2, s 224.
[1472] Submission to the Issues Paper: Australian Privacy Foundation, 40.

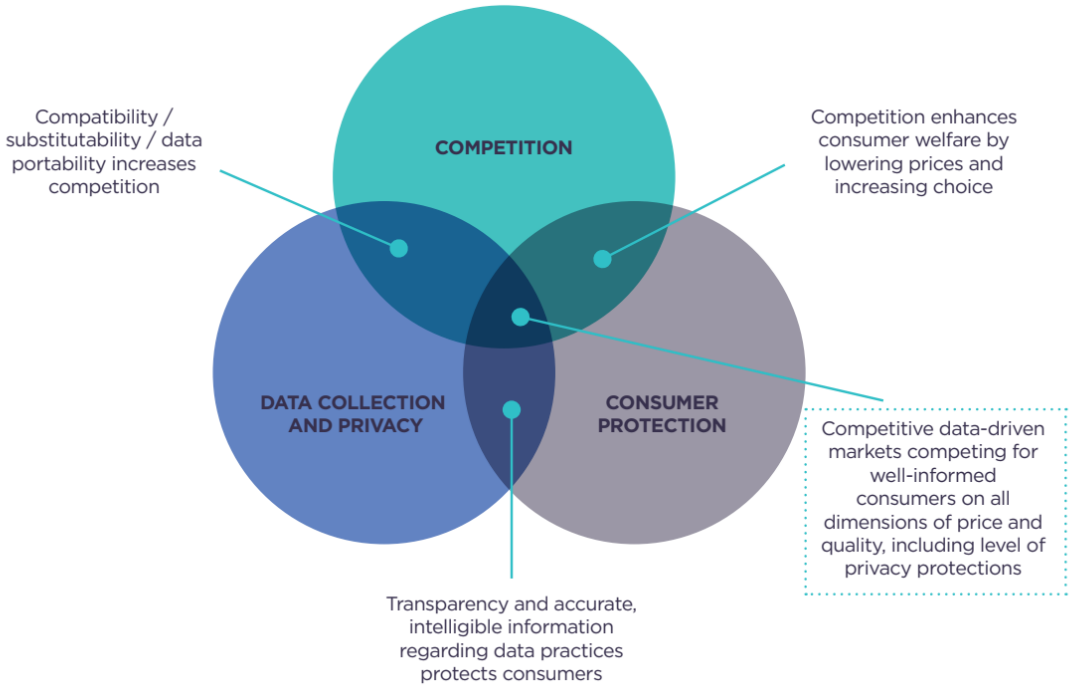
complaints – such as where data breaches need to be notified to multiple regulators.[1473] Despite the perceived overlap between regulatory frameworks, submitters noted the value of approved EDR schemes such as the TIO and the AFCA to resolve sectoral complaints that may also involve breaches of the APPs.[1474]

Proposal

Continue implementing methods to increase transparency between regulators

In light of existing MoUs and a number of changes to the Act that will be implemented through the OP Bill,[1475] the OAIC and other regulators will continue to work collaboratively to ensure enforcement action is brought under the most appropriate framework, lowering the risk of duplicative investigations. However, MoUs continue to provide important regulatory clarity in areas where there is a risk of regulatory overlap, and assist regulators engaging with one another on regulatory priorities. This approach recognises the inherent overlap between consumer law, competition law, and privacy law.[1476]

Figure 28.1: 'Overlapping issues in data protection, competition and consumer protection'



© Commonwealth of Australia. Image reproduced from ACCC, DPI Report (n 2), 5. Adapted by the ACCC from European Data Protection Supervisor, Privacy and competitiveness in the age of big data, March 2014. Image also appears in Submission to the Issues Paper, ACCC, 4.

For example, in consumer law, privacy policies and notices can constitute representations about how consumers can expect their information to be handled. When this information is accurate and effectively presented, consumers can make informed choices, which enhance their welfare. In competition law, privacy laws have the potential to either lessen or increase barriers to market entry

[1473] Submissions to the Issues Paper: IDCARE, 7. This dual requirement to notify regulators for data breaches may occur for APRA-related entities under APRA Prudential Standard CPS 234 (n 1368), or entities participating in data sharing under the forthcoming DAT Bill (n 1421) pt 3.3; or for critical infrastructure entities under the forthcoming Critical Infrastructure Bill (n 1426) pt 2B.

[1474] Submission to the Issues Paper: Telecommunications Industry Ombudsman, 1.

[1475] These changes include amendments to information sharing provisions which are intended to facilitate cooperation between regulators.

[1476] See diagram in Submission to the Issues Paper: ACCC, 4; See also, Submission to the Issues Paper: Consumer Policy Research Centre, 4.

and competition.[1477] In corporate law, privacy and cyber security obligations may form part of more general duties that company directors owe to their shareholders, such as the duty to exercise their powers and discharge their duties with due care and diligence.[1478] These duties complement APP 11 obligations to secure personal information and may encourage organisations to take further steps to protect against data breaches.

Provided that individuals are not disadvantaged by virtue of forum and cases do not 'fall through the gaps' of different frameworks, this overlap is evidence of the different legal frameworks responding to the growth in importance of personal information handling in the digital economy. It is important therefore that any proposal does not curtail the activities of other regulators in respect of data handling practices that may infringe other laws. Recognition and understanding of the intersection between competition law, consumer law and privacy is an area about which regulators globally are continuing to explore and develop their understanding.[1479]

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

Interaction with state and territory privacy laws

Submissions also considered that inconsistencies between state and Commonwealth privacy laws cause confusion and increase regulatory burden on APP entities subject to multiple privacy frameworks, such as healthcare providers and higher education providers.[1480] Many submissions identified priority areas for harmonisation between state and territory laws, but there was little consensus about how this should be achieved.[1481]

Overview of state and territory privacy legislation

The Act does not generally cover state and territory public sectors, which are mostly covered by state and territory privacy laws.[1482] Some states and territories also have separate health privacy laws and human rights legislation that include references to privacy.[1483]

Although state and territory privacy laws are relatively similar to the Act, there are a number of key differences, including:

- key definitions, such as the definitions of personal information and health information
- restrictions on disclosure of personal information outside the state or territory
- grounds for refusing requests to access and correct personal information

---

[1477] International Competition Network (ICN) Steering Group, *Scoping paper - Competition law enforcement at the intersection between competition, consumer protection and privacy* (Web Page, 2 December 2020) 3. The ACCC has been leading Task 2 of this project, which involves surveying ICN members about real-world examples of issues arising from the intersection between competition, consumer protection and privacy in competition law enforcement cases.

[1478] See R Falk, 'The board's role in cyber security assurance', *Australian Institute of Company Directors* (Web Page, 29 July 2020); Department of Home Affairs, Australia's Cyber Security Strategy 2020 (Web Page, 2020) [36]; *Corporations Act 2001* (Cth) s 180.

[1479] Federal Trade Commission (US), *International Competition Network Addresses Enforcement and Policy Challenges of the Digital Economy at United States-Hosted 19th Annual Conference* (Web Page, September 2020).

[1480] See, eg, Submissions to the Issues Paper: Australian Institute of Health and Welfare, 3; Benevolent Society, 3; Griffith University, 20–1; Ramsay Australia, 12.

[1481] See for examples of priority areas, Submissions to the Issues Paper: Australian Digital Health Agency, 3; Australian Council on Children and the Media, 5.

[1482] *Privacy and Personal Information Protection Act 1998* (NSW); *Privacy and Data Protection Act 2014* (Vic); *Information Privacy Act 2009* (Qld); *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2014* (ACT); *Information Act 2002* (NT). The Western Australian Government has committed to introducing privacy and responsible information sharing legislation for the WA public sector. Extensive public consultation on a proposed legislative model was undertaken in late 2019. South Australia has an administrative scheme under the Information Privacy Principles Instruction (SA).

[1483] *Human Rights Act 2004* (ACT) s 12; *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13; *Human Rights Act 2019* (Qld) s 25; *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT).

- voluntary or mandatory data breach notification schemes
- whether the legislation extends to government contractors
- exceptions to protections, such as permitted health situations, and
- availability of emergency declaration mechanisms.

How the Act operates in relation to state and territory laws

One objective of the Act is to 'provide the basis for nationally consistent regulation of privacy and the handling of personal information'.[1484] However, section 3 expressly preserves state and territory privacy laws by stating that the Act does not affect the operation of a state or territory law that makes provisions with respect to personal information handling and which is capable of operating concurrently with the Act.[1485]

As with Commonwealth laws, the 'authorised by or under an Australian law' exception permits state and territory laws to authorise acts inconsistent with certain APPs. For example, a state law may permit disclosure of personal information for a secondary purpose under APP 6.2 where this would not otherwise be permitted.[1486] Contracting provisions also govern the extent to which state and territory privacy laws, if any, apply. Commonwealth contractors are required to comply with the APPs, but if an APP entity is a contractor for a state or territory, the Act will not apply to the extent of that contract.[1487]

State and territory authorities and state-owned corporations can be brought into the scope of the Act if the State requests it through Commonwealth regulations.[1488] This has been done for a small number of state entities, including Essential Energy and the South Australian Department of Health and Wellbeing, in respect of SA/NT Datalink.[1489]

Need for greater interoperability in certain sectors

Submitters expressed concern about inconsistency and gaps between the Act and state and territory privacy laws particularly in sectors subject to both state and Commonwealth laws, such as universities and healthcare.[1490] Health information, data breach notification and coverage of contractors were identified as priority areas by submissions along with consent requirements, collection notices, children's privacy, cross-border disclosure, and the fees and grounds for refusing access and correction requests.[1491]

Treatment of health information

Health organisations in particular emphasised the challenges they face working across jurisdictions. For example, the Australian Digital Health Agency noted that the same health information could be subject to different privacy requirements 'depending on where it is collected, who collects it, where it is stored, and how it is shared' and expressed concern that these issues were 'a significant hindrance to achieving interoperability in the health system'.[1492]

The Australian Department of Health outlined that inconsistencies include the definition of 'health information', whether the legislation covers the deceased, emergency declaration mechanisms, and

[1484] *Privacy Act* (n 2) sub-s 2A(3).
[1485] *Privacy Act* (n 2) s 3.
[1486] OAIC, APP Guidelines (n 21) [B.128]; *Privacy Act* (n 2) sub-s 6(1), sch 1 APP 6(2).
[1487] *Privacy Act* (n 2) sub-s 7B(5), s 95B.
[1488] *Privacy Act* (n 2) s 6F.
[1489] *Privacy Regulation* (n 219) reg 8.
[1490] See Submissions to the Issues Paper: Australian Institute of Health and Welfare, 3; Griffith University, 7.
[1491] See, eg, Submissions to the Issues Paper: Australian Council on Children and the Media, 5; Australian Digital Health Agency, 3; Australian Medical Association, 12–13; Avant Mutual, 17–18; Dr Kerin Robinson, 1–2; Karen Meohas, 14.
[1492] Submission to the Issues Paper: Australian Digital Health Agency, 3.

the scope of health-related exceptions.[1493] It also indicated that Privacy Impact Assessment processes for interjurisdictional health projects would be far less onerous if all states and territories were subject to obligations comparable to the APPs.[1494]

Ramsay Australia and Telstra Health explained that this complexity affects not only clinicians, but also researchers, and suppliers of health data management systems across Australian jurisdictions.[1495] Submitters from the data industry noted that differences between jurisdictions lead to compliance costs with little corresponding benefit, and that uniform definitions would be easier to apply and interpret.[1496]

Legislative coverage of government contractors

Submitters also expressed concern about coverage of government contractors where South Australia and Western Australia have not enacted privacy legislation.[1497] Additionally, entities that contract with state and territory governments in multiple jurisdictions are subject to a wide range of obligations imposed by legislation and contractual clauses. The Benevolent Society noted that this creates ambiguities for charities that handle sensitive information of vulnerable people.[1498]

Case study – Contracting with governments across Australia

A company that is an APP entity has developed database software. It provides the software to a number of clients, including federal, state and territory governments.

- Outside of government contracts, the company will need to comply with the APPs as an organisation.[1499]
- Where the company provides their software to an Australian Government agency, they need to comply with the APPs as if they were that agency in respect of the contract.[1500]
- Where the company provides their software to a state government, they are not required to comply with the APPs, but depending on the state, may be required to comply with state privacy laws and contractual privacy provisions in respect of the contract.[1501]
- If the software is provided to a state which has no privacy legislation and there are no privacy obligations in the contractual arrangements with the company, no privacy obligations will apply.[1502]

Differences between these laws may mean that the database software needs to be programmed differently to comply with privacy requirements in each jurisdiction. Alternatively, the company may expend resources to analyse and comply with each of the laws that apply. While the company may adopt practices that meet the most rigorous requirements of the various jurisdictions, this may mean that their policies exceed legal requirements in other jurisdictions, with the company expending unnecessary resources in respect of those contracts.

[1493] Submission to the Issues Paper: Australian Department of Health, 9, 12. Health-related exceptions include permitted general situations under the *Privacy Act* (n 2) s 16A.

[1494] Submission to the Issues Paper: Australian Department of Health, 12.

[1495] Submissions to the Issues Paper: Ramsay Australia, 12; Telstra Ltd and Telstra Health Pty Ltd, 7.

[1496] Submission to the Issues Paper: illion, 7. See also re uniform definitions, Records and Information Management Professionals Australasia, 2.

[1497] Submission to the Issues Paper: Privacy 108, 3, 18.

[1498] Submission to the Issues Paper: Benevolent Society, 3–4.

[1499] See *Privacy Act* (n 2) s 6C. Slightly different obligations apply to agencies and organisations under the APPs, such as when collection is allowed for a secondary purpose under APP 3.

[1500] *Privacy Act* (n 2) s 95B.

[1501] *Privacy Act* (n 2) sub-s 7B(5). See, eg, *Privacy and Data Protection Act 2014* (Vic) s 17.

[1502] *Privacy Act* (n 2) sub-s 7B(5). Procurement rules and standard contractual clauses safeguard against this situation where no state privacy laws operate. See, Government of Western Australia – Department of Finance, *Government Procurement – Request Conditions and General Conditions of Contract* (Web Page, December 2020) 72.

Data breach notification requirements

The lack of mandatory data breach notification schemes in states and territories was also identified as an area of concern, with IDCARE noticing a growing volume of requests for assistance from state and territory agencies that are not subject to mandatory NDB schemes.[1503]

Proposal

In light of the issues raised by submitters resulting from differences between state and federal privacy laws, a Commonwealth, state and territory government officials working group could be established to focus on harmonising those aspects of privacy laws that are of key concern. It would not seek complete uniformity of all privacy principles across jurisdictions. Areas of focus could include key definitions, the application of privacy laws to state and territory contractors, and the treatment of health information.

While the OAIC recommended that harmonisation of privacy protections should be a key goal in the design of any federal, state or territory laws that purport to address privacy issues, many submitters went further to recommend that state and territory privacy laws be explicitly harmonised with the Commonwealth regime.[1504] Models that were proposed included a national privacy law, national health privacy law, or a model law in the style of workplace health and safety legislation, but there was little consensus among submitters about how to achieve consistency.[1505]

Accordingly, a model for longer-term harmonisation should be subject to further discussion between jurisdictions through the proposed working group.

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?

[1503] Submission to the Issues Paper: IDCARE, 7. NSW has since released an exposure draft of the Privacy and Personal Information Protection Amendment Bill 2021, which proposes to introduce mandatory data breach notification in NSW and cover most NSW state-owned corporations. See NSW Department of Communities and Justice, *Proposed changes to NSW privacy laws* (Web Page, May 2021).

[1504] Submissions to the Issues Paper: OAIC, 150. See, eg, Submission to the Issues Paper: Privacy 108, 18.

[1505] Submissions to the Issues Paper: Benevolent Society, 2; MIGA, 3–4, Minderoo Tech and Policy Lab – University of Western Australia School of Law, 10–13; Privacy 108, 18.