



Australian Government
Attorney-General's Department

Privacy Act Review | Report 2022

© Commonwealth of Australia 2022

ISBN (Online): 978-1-921241-41-3

ISBN (Print): 978-1-921241-42-0

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.dpmc.gov.au/government/commonwealth-coat-arms).

Table of contents

1. Executive summary	1
2. List of proposals	5
Part 1: Scope and application of the Privacy Act	17
3. Objects of the Act	18
4. Personal information, de-identification and sensitive information	23
5. Flexibility of the APPs	47
6. Small business exemption	52
7. Employee records exemption	64
8. Political exemption	72
9. Journalism exemption	84
Part 2: Protections	93
10. Privacy policies and collection notices	94
11. Consent and online privacy settings	102
12. Fair and reasonable test	110
13. Additional protections	122
14. Research	133
15. Organisational accountability	140
16. Children's privacy	146
17. People experiencing vulnerability	158
18. Rights of the individual	166
19. Automated decision-making	188
20. Direct marketing, targeting and trading	194
21. Security, Destruction and Retention of Personal Information	221
22. Controllers and processors of personal information	230
23. Overseas data flows	234
24. Cross-Border Privacy Rules and domestic certification	247
Part 3: Regulation and enforcement	251
25. Enforcement	252
26. A direct right of action	272
27. A statutory tort for serious invasions of privacy	280
28. Notifiable data breaches scheme	288
29. Interactions with other schemes	299
30. Further review	304
Attachment A – Consultation	305
Attachment B – Terms of Reference	311

Abbreviations

2020 ACAP survey	OAIC Australian Community Attitudes to Privacy Survey 2020
7-Eleven determination	Commissioner initiated investigation into 7- Eleven Stores Pty Ltd (Privacy) [Corrigendum dated 12 October 2021] [2021] AICmr 50 [29 September 2021]
AAT	Administrative Appeals Tribunal
ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACCI	Australian Chamber of Commerce and Industry
ACL	Australian Consumer Law
ACMA	Australian Communications and Media Authority
ACT	Australian Capital Territory
ACSC	Australian Cyber Security Centre
ADMA	Association for Data-driven Marketing & Advertising
ADHA	Australian Digital Health Agency
ADM	Automated Decision-Making
Adtech final report	ACCC Digital advertising services inquiry: Final Report
AFCA	Australian Financial Complaints Authority
AFP	Australian Federal Police
AGD	Attorney-General's Department
AHRC	Australian Human Rights Commission
AHRC Report	AHRC Human Rights and Technology: Final Report
AI	Artificial Intelligence
AIC Act	Australian Information Commissioner Act 2010 (Cth)
ALRC	Australian Law Reform Commission
ALRC Report 108	ALRC, For your Information: Australian Privacy Law and Practice (Report No 108, 12 August 2008)
ALRC Report 123	ALRC, Serious Invasions of Privacy in the Digital Era (Report No 123, 3 September 2014)
APC	Australian Press Council
APEC	Asia-Pacific Economic Cooperation
APP Guidelines	Australian Privacy Principles Guidelines (July 2019)
APPs	Australian Privacy Principles
ASIC	Australian Securities and Investments Commission
Bill C-27	Bill C-27 Digital Charter Implementation Act 2022 (Canada)
CAIDE and MLS	Centre for AI and Digital Ethics and Melbourne Law School
Castan Centre	Castan Centre for Human Rights Law and the Centre for Commercial Law and Regulatory Studies, Monash University
CBPR	Cross-Border Privacy Rules
CCA	Competition and Consumer Act 2010 (Cth)

CCPA	California Consumer Privacy Act of 2018
CDR	Consumer Data Right
Clearview determination	Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54 (14 October 2021)
CSIRO	Commonwealth Scientific and Industrial Research Organisation
Cyber Security Strategy	2023-2030 Australian Cyber Security Strategy
DAT Act	Data Availability and Transparency Act 2022 (Cth)
DNCR Act	Do Not Call Register Act 2006 (Cth)
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
ED	Emergency Declaration
EDPB	European Data Protection Board
EU	European Union
FCFCOA	Federal Circuit and Family Court of Australia
FOI Act	Freedom of Information Act 1982 (Cth)
FPO	Federal Privacy Ombudsman
FRT	Facial Recognition Technology
GDPR	General Data Protection Regulation (European Union)
HREC	Human Research Ethics Committee
IAB	Interactive Advertising Bureau
IC	Information Commissioner
ICCPR	International Covenant on Civil and Political Rights
IGEA	Interactive Games and Entertainment Association
IGIS	Inspector-General of Intelligence and Security
IMC	Independent Media Council
IoT	Internet of Things
IP address	Internet Protocol address
MHR Act	My Health Records Act 2012 (Cth)
MIGA	Medical Insurance Group Australia
MoU	Memorandum of Understanding
NDB scheme	Notifiable Data Breaches scheme
NHMRC	National Health and Medical Research Council

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, SC 2000, c 5 (Canada)
Privacy Enforcement Bill	Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022
Privacy Enforcement Act	Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022
SCCs	standard contractual clauses
Spam Act	Spam Act 2003 (Cth)
SOCI Act	Security of Critical Infrastructure Act 2018 (Cth)
the Act	Privacy Act 1988 (Cth)
UK	United Kingdom
UK ICO	Information Commissioner's Office (UK)

1. Executive summary

This Report is the culmination of two years of extensive consultation and review of the *Privacy Act 1988* (Cth) (Review of the Act). The Review was instigated following the Australian Competition and Consumer Commission's (ACCC) 2019 *Digital Platforms Inquiry* final report (DPI Report) which made several privacy recommendations. The Review commenced in October 2020 with the release of an [Issues Paper](#), followed by a [Discussion Paper](#) in 2021 which put forward proposals for reforming the Act for consultation. The Review has considered whether the Act and its enforcement mechanisms are fit for purpose in an environment where Australians now live much of their lives online¹ and their information is collected and used for a myriad of purposes in the digital economy.

While the digital economy has generated significant benefits, including consumer convenience,² improved efficiencies³ and new employment opportunities,⁴ it has also resulted in large amounts of information about people being generated, used, disclosed and stored. These troves of information may be used beneficially to improve government services, innovate new commercial services and modes of delivery, market goods and services and facilitate communication.

Throughout the Review, the vulnerability of people's information in the digital age has been highlighted, including recently in relation to several high-profile data breaches, exposing millions of Australians to privacy risks including identity fraud, reputational damage and blackmail.⁵ These harms challenge the community's trust in new applications of technology, which the Productivity Commission recently noted 'is critical for future uptake, as businesses and governments need to maintain their social licence to deliver digital and data-enabled services.'⁶

The challenge of realising the benefits of data-driven technology while protecting individuals' privacy is one that countries are grappling with globally. While different countries take different approaches to privacy and data protection regulation, there have been significant developments in data protection laws internationally in recent years to respond to the technological developments in personal information handling. These include the European Union (EU),⁷ the United Kingdom (UK),⁸ Brazil,⁹ Japan,¹⁰ Singapore¹¹ and California.¹² Canada's federal parliament is also currently considering significant reforms to its data protection laws.¹³ The proposals in this Report are designed to better align Australia's laws with global standards of information privacy protection and properly protect Australians' privacy. The Review considers that these proposed changes are likely to enhance cross border data flows with Australia as a trusted trading partner, and have resultant economic benefits for Australian businesses and the economy.

The proposals in this Report draw from stakeholder feedback (refer Attachment A for details) and analysis of other sources, including research papers, international data protection and privacy laws and reports which consider privacy issues. Consideration of the benefits and limitations and costs associated with proposals put forward in the Discussion Paper led to some proposals being reworked, some not being pursued and, in other cases, new proposals being put forward. As such, some proposals have not had the benefit of stakeholder feedback and will require further consultation prior to implementation. Where wording is suggested in particular proposals, the legislative drafting process would determine the precise wording of any amendments to the Act.

- 1 Consumer Policy Research Centre, [Data and Technology Consumer Survey](#) (Report, December 2020); ABS, [Household Use of Information Technology Survey](#) (Report, March 2018); ACMA, [Communications Report 2018-19](#) (Report, February 2020) 23; ACCC, [DPI Report](#) 379; OECD, [Data-Driven Innovation Big Data for Growth and Well-Being](#) (Report, October 2015) 20; IDC, [The Digitization of the World From Edge to Core](#) (Report, November 2018); ACCC, [Internet Activity Report](#) (Report, June 2021) 1.
- 2 Productivity Commission, [Data Availability and Use](#) (Final Report, May 2017), Chapter 2.
- 3 OECD, [The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines](#) (Report, December 2010) 8-9; Consumer Policy Research Centre, [Consumer Data and the Digital Economy](#) (Report, July 2018) 20; Productivity Commission, [Data Availability and Use](#) (Final Report, May 2017), Chapter 2.
- 4 World Economic Forum, [Future of Jobs Report 2020](#) (Report, October 2020).
- 5 Josh Taylor, 'Optus reveals at least 2.1 million ID numbers exposed in massive data breach', [The Guardian](#) (online, 3 October 2022); Jake Lapham 'Sydney teenager charged after allegedly blackmailing 93 Optus customers affected by data breach', [ABC](#) (online, 6 October 2022); Colin Kruger and Nick Bonyhady, 'Medibank cyberattack could be costly 'on multiple fronts'', [The Sydney Morning Herald](#) (online, 22 October 2022); Emilia Terzon, 'Australian Clinical Labs accused of 'sitting on' hack that saw patient data posted to the dark web', [ABC](#) (online, 28 October 2022).
- 6 Productivity Commission, [5-year Productivity inquiry: Australia's data and digital dividend](#) (Interim Report, August 2022).
- 7 The General Data Protection Regulation ('GDPR') came into force in the EU and the UK on 2 May 2018, updating Directive 95/46/EC and harmonising data protection laws across the EU. See also, the [Digital Services Act 2022](#) (EU) and European Commission, [Proposal for an Artificial Intelligence Act 2022](#) (EU).
- 8 [Data Protection Act 2018](#) (UK).
- 9 [General Data Protection Law](#), Law No. 13.709/2018 (Brazil).
- 10 [The Act on the Protection of Personal Information](#), Act No. 57 of 2003 as amended in 2020 (Japan).
- 11 [Personal Data Protection Act 2012](#) (Singapore).
- 12 [California Consumer Privacy Act 2018](#) (California) ('CCPA').
- 13 [An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts \(Digital Charter Implementation Act 2022\)](#), 1st session, 44th Parliament (Canada) ('[Bill C-27](#)').

1.1 Key themes and proposals

1.1.1 Scope and application of the Act

Flexibility of the Act

A common theme in submissions to the Review was that the principles-basis of the Act should be retained but supplemented with more detailed prescription where required. This Report proposes new principles, such as the fair and reasonable test, as well as more detailed rules to provide greater certainty where needed. This is proposed via different mechanisms, including more detailed Office of the Australian Information Commissioner (OAIC) guidance, specific legislated requirements and APP codes. Noting the significant societal events that occurred over the two years of the Review, consultation supported proposals to introduce greater flexibility in APP code-making and emergency declarations to increase their usefulness in emergency situations.

What is protected by the Act

Stakeholder feedback revealed considerable confusion about what ‘personal information’ is currently protected by the Act. The Report proposes changes to clarify that personal information is an expansive concept which includes technical and inferred information, such as IP addresses and device identifiers, where it relates to a reasonably identifiable individual. It also proposes that some security protections should apply to personal information that has been de-identified, in recognition of the fact that de-identified information can be re-identified.

Exemptions from the Act

Many submitters called for the current exemptions from the Act to be removed or narrowed, including the small business, employee records, political, and journalism exemptions. The gap in privacy protections for Australians as a result of these exemptions compared to other countries was highlighted. In contrast, those who currently fall within these exemptions expressed strong concern about their removal, particularly about the burden of compliance in relation to the small business and employee records exemption. On balance, this Report proposes that the need for Australians’ information to be adequately protected in the digital age justifies at least some recalibration of all of the exemptions to address contemporary privacy risks and meet current community expectations.

This Report proposes that small businesses should, in the future, be covered by the Act. The community expects that if they provide their personal information to a small business they will keep it safe. However, further extensive consultation would need to occur with small business to determine the best way for small businesses to meet their obligations under the Act, proportionate to the privacy risks they typically face. An impact analysis should be undertaken to better understand the impact of removing the exemption on small businesses, which would inform an appropriate package of support that could be provided to small business. This would be designed to ensure that small business would be in a strong position to comply with obligations under the Act, prior to the exemption being removed. Furthermore, as this Report also proposes enhanced privacy protections under the Act, further consideration should be given to whether modifications to various proposals (such as organisational accountability requirements) are required so that they can be adapted to the small business context in a proportionate manner.

This Report also proposes changes to the other exemptions under the Act, again to reflect current community expectations and modern privacy risks. It will be important to collaborate with those entities currently subject to the exemptions to ensure that they will be well placed to meet their changed obligations under the Act.

1.1.2 Protections under the Act

There was very strong support for increasing the protections for personal information under the Act. Stakeholder feedback strongly suggested that individuals should have more transparency and control over how their personal information is handled. The proposals in this Report are designed to address these issues, whilst ensuring entities are not stifled from innovating or prospering in a digital economy. In particular, the proposals would facilitate overseas disclosures of personal information whilst ensuring the information disclosed overseas is protected.

Notice and consent

This Report proposes that the quality of privacy collection notices and consents obtained from individuals should be improved. However, it does not propose significantly increasing the circumstances in which notices should be provided or consent obtained. An over-reliance on notice and consent can place an unrealistic burden on individuals to understand the risks of complicated information handling practices and may not result in improved privacy outcomes.

Fair and reasonable test and additional protections

This Report proposes a new 'fair and reasonable' test to underpin the activities of APP entities when handling personal information. This test was generally supported by submitters to ensure entities' handling of personal information is within individuals' reasonable expectations and is not harmful. There was also significant support for additional protections to apply where entities engage in high privacy risk practices, including for children and for people experiencing vulnerability. This Report proposes that all entities covered by the Act should conduct a Privacy Impact Assessment before commencing an activity which is likely to have a significant impact on the privacy of individuals and that additional privacy protections should apply to children. The Report also recognises that the flexible nature of the Australian Privacy Principles should allow entities to take greater care in how they comply with the Act where vulnerabilities are identified.

Security, destruction and notifiable data breaches

Recent large-scale data breaches have highlighted the vast amount of personal information that is collected and retained by entities, and the need for entities to put in place stronger protections to prevent unauthorised access to Australians' information. The best way to protect personal information is for entities to minimise the amount of personal information they collect and retain. The Act already requires entities to only collect what is reasonably necessary and to destroy personal information when it is no longer required. This requirement would be reinforced through enhanced OAIC guidelines for entities on the reasonable steps they should take to destroy or de-identify personal information so that they can be in a better position to meet their obligations. In addition, this Report proposes that entities should determine, and periodically review, the period of time for which they retain personal information. There should be a further review of legal provisions outside of the Privacy Act that require certain forms of personal information to be retained. This further work should determine if those requirements appropriately balance the intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information.

The Report also proposes enhancements to the Notifiable Data Breach scheme (NDB scheme) so that, when a data breach occurs, quick action can be taken to minimise harm to affected individuals. Proposed new data breach reporting obligations, including notifying the Information Commissioner (IC) within 72 hours of becoming aware of a data breach, would assist with this objective. The Report also proposes further work to better facilitate reporting processes for entities with multiple reporting obligations.

Direct marketing, targeting and trading

The Report makes several proposals to address potential harms arising from direct marketing, targeted advertising and online content, and entities trading in personal information. Submitters expressed concern about technological developments which enable the use of information relating to individuals to target them with marketing and personalised content without necessarily identifying them. As this information may not be 'personal information', the capacity of the Act to address this practice is limited. To respond to this gap, this Report includes proposals to regulate 'targeting' which would capture the collection, use or disclosure of information which relates to an individual (irrespective of whether they are identified or reasonably identifiable) for tailoring services, content, information, advertisements or offers provided to them or withheld from them (either on their own, or as a member of some group or class).

Individuals' control over their personal information

This Report proposes a number of individual rights modelled on the European Union's *General Data Protection Regulation* (GDPR) 'data subject rights' (such as rights to object, to request erasure and to have search results de-indexed).¹⁴ Exceptions would apply for countervailing public interests, other legal interests and to recognise where it would be technically impossible or unreasonable to comply with an individual's request. Transparency requirements for automated decisions that use personal information and have a significant effect on individuals are also proposed. Entities would need to provide information about types of personal information used in automated decisions-making systems and how such decisions are made.

14 GDPR arts 12-23.

Controllers and processors and overseas data transfers

Consultation highlighted the problematic nature of compliance with the Act for entities that process personal information under the direction of another entity. This Report proposes introducing the concepts of controllers and processors into the Act. Measures are also proposed to support entities disclosing personal information overseas, including introducing a mechanism to prescribe countries' laws and binding schemes as providing substantially similar protection and making standard contractual clauses available to APP entities.

1.1.3 Regulation and enforcement

Enforcement of the Act

Submitters emphasised the importance of effective enforcement to foster compliance with requirements under the act. This Report proposes significant reforms to strengthen the enforcement of the Act including new civil penalties and new powers for the IC in relation to investigations, public inquiries and determinations. To address concerns about the appropriate resourcing requirements of the OAIC, the Report proposes that the feasibility of industry funding models be further explored.

Direct right of action and statutory tort for serious invasions of privacy

Individuals having more agency to seek redress for interferences with their privacy, through increasing the avenues available to individuals to seek remedies in the courts, was a strong theme supported throughout the Review. This Report proposes a direct right of action to enable individuals to seek remedies in the courts for breaches of the Act which cause harm. A statutory tort for serious invasions of privacy, as put forward by ALRC Report 123, is also proposed for adoption in federal legislation to address the current gap in mechanisms available to Australians to seek compensation in the courts for breaches of privacy which fall outside the Act.

Interacting privacy frameworks

The Review sought feedback on how to reduce the regulatory burden associated with multiple privacy and reporting obligations under different legislative frameworks. Proposals aimed at streamlining obligations and minimising duplication are put forward, including developing a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy obligations and establishing a Commonwealth, state and territory working group to work on harmonising key issues in privacy laws.

2. List of proposals

3. Objects of the Act

Proposal 3.1 Amend the objects of the Act to clarify that the Act is about the protection of personal information.

Proposal 3.2 Amend the objects of the Act to recognise the public interest in protecting privacy.

4. Personal information, de-identification and sensitive information

Proposal 4.1 Change the word ‘about’ in the definition of personal information to ‘relates to’. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.

Proposal 4.2 Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance.

Proposal 4.3 Amend the definition of ‘collection’ to expressly cover information obtained from any source and by any means, including inferred or generated information.

Proposal 4.4 ‘Reasonably identifiable’ should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.

Proposal 4.5 Amend the definition of ‘de-identified’ to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.

Proposal 4.6 Extend the following protections of the Privacy Act to de-identified information:

- (a) APP 11.1 – require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information:
 - (a) from misuse, interference and loss; and
 - (b) from unauthorised re-identification, access, modification or disclosure.
- (b) APP 8 – require APP entities when disclosing de-identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information, including ensuring that the receiving entity does not re-identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification.
- (c) Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice.

Proposal 4.7 Consult on introducing a criminal offence for malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit, with appropriate exceptions.

Proposal 4.8 Prohibit an APP entity from re-identifying de-identified information obtained from a source other than the individual to whom the information relates, with appropriate exceptions. In addition, the prohibition should not apply where:

- (a) the re-identified information was de-identified by the APP entity itself - in this case, the APP entity should simply comply with the APPs in the ordinary way.
- (b) the re-identification is conducted by a processor with the authority of an APP entity controller of the information.

Proposal 4.9 Sensitive Information

- (a) Amend the definition of sensitive information to include ‘genomic’ information.
- (b) Amend the definition of sensitive information to replace the word ‘about’ with ‘relates to’ for consistency of terminology within the Act.
- (c) Clarify that sensitive information can be inferred from information which is not sensitive information.

Proposal 4.10 Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent. Define ‘geolocation tracking data’ as personal information which shows an individual’s precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.

5. Flexibility of the APPs

Proposal 5.1 Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney-General has directed or approved that a code should be made:

- (a) where it is in the public interest for a code to be developed, and
- (b) where there is unlikely to be an appropriate industry representative to develop the code.

In developing an APP code, the Information Commissioner would:

- (a) be required to make the APP Code available for public consultation for at least 40 days, and
- (b) be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.

Proposal 5.2 Amend the Act to enable the Information Commissioner to issue a temporary APP code for a maximum 12 month period 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.

Proposal 5.3 Amend the Act to enable Emergency Declarations to be more targeted by prescribing their application in relation to:

- (a) entities, or classes of entity
- (b) classes of personal information, and
- (c) acts and practices, or types of acts and practices.

Proposal 5.4 Ensure the Emergency Declarations are able to be made in relation to ongoing emergencies.

Proposal 5.5 Amend the Act to permit organisations to disclose personal information to state and territory authorities under an Emergency Declaration, provided the state or territory has enacted comparable privacy laws to the Commonwealth.

6. Small business exemption

Proposal 6.1 Remove the small business exemption, but only after:

- (a) an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act
- (b) appropriate support is developed in consultation with small business
- (c) in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and
- (d) small businesses are in a position to comply with these obligations.

Proposal 6.2 In the short term:

- (a) prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption, and
- (b) remove the exemption from the Act for small businesses that obtain consent to trade in personal information.

7. Employee records exemption

Proposal 7.1 Enhanced privacy protections should be extended to private sector employees, with the aim of:

- a) providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for
- b) ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information
- c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and

- d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm.

Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.

8. Political exemption

Proposal 8.1 Amend the definition of 'organisation' under the Act so that it includes a 'registered political party' and include registered political parties within the scope of the exemption in section 7C.

Proposal 8.2 Political entities should be required to publish a privacy policy which provides transparency in relation to acts or practices covered by the exemption.

Proposal 8.3 The political exemption should be subject to the following requirements:

- (a) Political acts and practices covered by the exemption must be fair and reasonable.
- (b) Political entities must not engage in targeting based on sensitive information or traits which relates to an individual, with an exception for political opinions, membership of a political association, or membership of a trade union.

The political exemption should include a savings clause as per Recommendation 41-2 of ALRC Report 108.

Proposal 8.4 The political exemption should be subject to a requirement that individuals must be provided with the means to:

- (a) opt-out of their personal information being used or disclosed for direct marketing by a political entity, and
- (b) opt-out of receiving targeted advertising from a political entity.

Proposal 8.5 The political exemption should be subject to a requirement that political entities must:

- (a) take reasonable steps to protect personal information held for the purpose of the exemption from misuse, interference and loss, as well as unauthorised access, modification or disclosure
- (b) take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for a purpose covered by the political exemption, and
- (c) comply with the NDB scheme in relation to an eligible data breach involving personal information held for a purpose covered by the political exemption.

Proposal 8.6 The OAIC should develop further guidance materials to assist political entities to understand and meet their obligations.

9. Journalism exemption

Proposal 9.1 To benefit from the journalism exemption a media organisation must be subject to:

- (a) privacy standards overseen by a recognised oversight body (the ACMA, APC or IMC), *or*
- (b) standards that adequately deal with privacy.

Proposal 9.2 In consultation with industry, and the ACMA, the OAIC should develop and publish criteria for adequate media privacy standards and a template privacy standard that a media organisation may choose to adopt.

Proposal 9.3 An independent audit and review of the operation of the journalism exemption should be commenced three years after any amendments to the journalism exemption come into force.

Proposal 9.4 Require media organisations to comply with security and destruction obligations in line with the obligations set out in APP 11.

Proposal 9.5 Require media organisations to comply with the reporting obligations in the NDB scheme. There will need to be some modifications so that a media organisation would not need to notify an affected individual if the public interest in journalism outweighs the interest of affected individuals in being notified.

10. Privacy policies and collection notices

Proposal 10.1 Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place.

Proposal 10.2 The list of matters in APP 5.2 should be retained. OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the individual in the circumstances, need to be addressed in a notice.

The following new matters should be included in an APP 5 collection notice:

- (a) if the entity collects, uses or discloses personal information for a high privacy risk activity —the circumstances of that collection, use or disclosure
- (b) that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and
- (c) the types of personal information that may be disclosed to overseas recipients.

Proposal 10.3 Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.

11. Consent and privacy default settings

Proposal 11.1 Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.

Proposal 11.2 The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.

Proposal 11.3 Expressly recognise the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Proposal 11.4 Online privacy settings should reflect the privacy by default framework of the Act.

APP entities that provide online services should be required to ensure that any privacy settings are clear and easily accessible for service users.

12. Fair and reasonable personal information handling

Proposal 12.1 Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.

Proposal 12.2 In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account:

- (a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances
- (b) the kind, sensitivity and amount of personal information being collected, used or disclosed
- (c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency
- (d) the risk of unjustified adverse impact or harm
- (e) whether the impact on privacy is proportionate to the benefit
- (f) 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, and
- (g) the objects of the Act.

The EM would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include:

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

Proposal 12.3 The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed.

13. Additional protections

Proposal 13.1 APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks.

- (a) A Privacy Impact Assessment should be undertaken prior to the commencement of the high-risk activity.
- (b) An entity should be required to produce a Privacy Impact Assessment to the OAIC on request.

The Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals'. OAIC guidance should be developed which articulates factors that may indicate a high privacy risk, and provides examples of activities that will generally require a Privacy Impact Assessment to be completed. Specific high risk practices could also be set out in the Act.

Proposal 13.2 Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies.

Proposal 13.3 The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks. Practice-specific guidance could outline the OAIC's expectations for compliance with the Act when engaging in specific high-risk practices, including compliance with the fair and reasonable personal information handling test.

Proposal 13.4 Include an additional requirement in APP 3.6 to the effect 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. OAIC guidelines could provide examples of reasonable steps that could be taken.

14. Research

Proposal 14.1 Broad consent for research

Introduce a legislative provision that permits *broad consent* for the purposes of research:

- (a) Broad consent should be available for all research to which the research exceptions in the Act (and proposed by this chapter) will also apply.
- (b) Broad consent would be given for 'research areas' where it is not practicable to fully identify the purposes of collection, use or disclosure of personal or sensitive information at the point when consent is being obtained.

Proposal 14.2 Consult further on broadening the scope of research permitted without consent for both agencies and organisations.

Proposal 14.3 Consult further on developing a single exception for research without consent and a single set of guidelines, including considering the most appropriate body to develop the guidelines.

15. Organisational Accountability

Proposal 15.1 An APP entity must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. If an APP entity wishes to use or disclose personal information for a secondary purpose, it must record that secondary purpose at or before the time of undertaking the secondary use or disclosure.

Proposal 15.2 Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.

16. Children

Proposal 16.1 Define a child as an individual who has not reached 18 years of age.

Proposal 16.2 Existing OAIC guidance on children and young people and capacity¹⁵ should continue to be relied upon by APP entities. An entity must decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis. If that is not practical, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise.

The Act should codify the principle that valid consent must be given with capacity. Such a provision could state that 'the consent of an individual is only valid if it is reasonable to expect that an individual to whom the APP entity's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.'

Exceptions should be provided for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary their interests (including, but not limited to confidential healthcare advice, domestic violence, mental health, drug and alcohol, homelessness or other child support and community services).

Proposal 16.3 Amend the Privacy Act to require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a child.

In the context of online services, these requirements should be further specified in a Children's Online Privacy Code, which should provide guidance on the format, timing and readability of collection notices and privacy policies.

Proposal 16.4 Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances.

Proposal 16.5 Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'. To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the UK Age Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services.

The code developer should be required to consult broadly with children, parents, child development experts, child-welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted.

The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service.

17. People experiencing vulnerability

Proposal 17.1 Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.

Proposal 17.2 OAIC guidance on capacity and consent should be updated to reflect developments in supported decision-making.

Proposal 17.3 Further consultation should be undertaken to clarify the issues and identify options to ensure that financial institutions can act appropriately in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent.

¹⁵ OAIC, [APP Guidelines](#) (July 2019) [B.55]–[B.61].

18. Rights of the Individual

Access and Explanation

Proposal 18.1 Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features:

- (a) an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act)
- (b) an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual
- (c) an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual
- (d) the entity may consult with the individual about the format for responding to a request, and the format should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information
- (e) an organisation may charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual

Objection

Proposal 18.2 Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons.

Erasure

Proposal 18.3 Introduce a right to erasure with the following features:

- (a) An individual may seek to exercise the right to erasure for any of their personal information.
- (b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.

In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.

Correction

Proposal 18.4 Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control.

De-indexing

Proposal 18.5 Introduce a right to de-index online search results containing personal information which is:

- (a) sensitive information [e.g. medical history], or
- (b) information about a child, or
- (c) excessively detailed [e.g. home address and personal phone number], or
- (d) inaccurate, out-of-date, incomplete, irrelevant, or misleading.

The search engine may refer a suitable request to the OAIC for a fee. The right should be jurisdictionally limited to Australia.

Exceptions

Proposal 18.6 Introduce relevant exceptions to all rights of the individual based on the following categories:

- (a) **Competing public interests:** such as where complying with a request would be contrary to public interests, including freedom of expression and law enforcement activities.
- (b) **Relationships with a legal character:** such as where complying with the request would be inconsistent with another law or a contract with the individual.
- (c) **Technical exceptions:** such as where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request.

Response

Proposal 18.7 Individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them.

Privacy policies should set out the APP entity's procedures for responding to the rights of the individual.

Proposal 18.8 An APP entity must provide *reasonable assistance* to individuals to assist in the exercise of their rights under the Act.

Proposal 18.9 An APP entity must take reasonable steps to respond to an exercise of a right of an individual. Refusal of a request should be accompanied by an explanation for the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC.

Proposal 18.10 An organisation must acknowledge receipt of a request to exercise a right of an individual within a reasonable time and provide a timeframe for responding.

An agency and organisation must respond to a request to exercise a right within a reasonable timeframe. In the case of an agency, the default position should be that a reasonable timeframe is within 30 days, unless a longer period can be justified.

19. Automated decision making

Proposal 19.1 Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.

Proposal 19.2 High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act. This should be supplemented by OAIC Guidance.

Proposal 19.3 Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect.

This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.

20. Direct marketing, targeting and trading

Proposal 20.1 Amend the Act to introduce definitions for:

- (a) **Direct marketing** – capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material.
- (b) **Targeting** – capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class).
- (c) **Trading** – capture the disclosure of personal information for a benefit, service or advantage.

Proposal 20.2 Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.

Proposal 20.3 Provide individuals with an unqualified right to opt-out of receiving targeted advertising.

Proposal 20.4 Introduce a requirement that an individual's consent must be obtained to trade their personal information.

Proposal 20.5 Prohibit direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests.

Proposal 20.6 Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.

Proposal 20.7 Prohibit trading in the personal information of children.

Proposal 20.8 Amend the Act to introduce the following requirements:

- (a) Targeting individuals should be fair and reasonable in the circumstances.
- (b) Targeting individuals based on sensitive information (which should not extend to targeting based on political opinions, membership of a political association or membership of a trade union), should be prohibited, with an exception for socially beneficial content.

Proposal 20.9 Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.

21. Security, retention and destruction

Proposal 21.1 Amend APP 11.1 to state that ‘reasonable steps’ include technical and organisational measures.

Proposal 21.2 Include a set of baseline privacy outcomes under APP 11 and consult further with industry and government to determine these outcomes, informed by the development of the Government’s 2023-2030 Australian Cyber Security Strategy.

Proposal 21.3 Enhance the OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre.

Proposal 21.4 Amend APP 11.1 so that APP entities must also take reasonable steps to protect de-identified information.

Proposal 21.5 The OAIC guidance in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information.

Proposal 21.6 The Commonwealth should undertake a review of all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information.

This further work could also be considered by the proposed Commonwealth, state and territory working group at Proposal 29.3 as a key issue of concern where alignment would be beneficial.

However, this review should not duplicate the recent independent review of the mandatory data retention regime under the *Telecommunications (Interception and Access) Act 1979* and the independent reviews and holistic reform of electronic surveillance legislative powers.

Proposal 21.7 Amend APP 11 to require APP entities to establish their own maximum and minimum retention periods in relation to the personal information they hold which take into account the type, sensitivity and purpose of that information, as well as the entity’s organisational needs and any obligations they may have under other legal frameworks. APP 11 should specify that retention periods should be periodically reviewed. Entities would still need to destroy or de-identify information that they no longer need.

Proposal 21.8 Amend APP 1.4 to stipulate that an APP entity’s privacy policy must specify its personal information retention periods.

22. Controllers and processors of personal information

Proposal 22.1 Introduce the concepts of APP entity controllers and APP entity processors into the Act.

Pending removal of the small business exemption, a non-APP entity that processes information on behalf of an APP entity controller would be brought into the scope of the Act in relation to its handling of personal information for the APP entity controller. This would be subject to further consultation with small business and an impact analysis to understand the impact on small business processors.

23. Overseas data flows

Proposal 23.1 Consult on an additional requirement in subsection 5B(3) to demonstrate an 'Australian link' that is focused on personal information being connected with Australia.

Proposal 23.2 Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).

Proposal 23.3 Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.

Proposal 23.4 Strengthen the informed consent exception to APP 8.1 by requiring entities to consider the risks of an overseas disclosure and to inform individuals that privacy protections may not apply to their information if they consent to the disclosure.

Proposal 23.5 Strengthen APP 5 in relation to overseas disclosures by requiring APP entities, when specifying the countries in which recipients are likely to be located if practicable, to also specify the types of personal information that may be disclosed to recipients located overseas.

Proposal 23.6 Introduce a definition of 'disclosure' that is consistent with the current definition in APP Guidelines. Further consideration should be given to whether online publications of personal information should be excluded from the requirements of APP 8 where it is in the public interest.

24. CBPR and domestic certification

Nil proposals.

25. Enforcement

Proposal 25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses:

- (a) Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision.
- (b) Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties.

Proposal 25.2 Amend section 13G of the Act to remove the word 'repeated' and clarify that a 'serious' interference with privacy may include:

- (a) those involving 'sensitive information' or other information of a sensitive nature
- (b) those adversely affecting large groups of individuals
- (c) those impacting people experiencing vulnerability
- (d) repeated breaches
- (e) wilful misconduct, and
- (f) serious failures to take proper steps to protect personal data.

The OAIC should provide specific further guidance on the factors that they take into account when determining whether to take action under section 13G.

Proposal 25.3 Amend the Act to apply the powers in Part 3 of the *Regulatory Powers (Standard Provisions) Act 2014* to investigations of civil penalty provisions in addition to the Information Commissioner's current investigation powers.

Proposal 25.4 Amend the Act to provide the Information Commissioner with the power to undertake public inquiries and reviews into specified matters on the approval or direction of the Attorney-General.

Proposal 25.5 Amend subparagraph 52(1)(b)(iii) and paragraph 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.

The OAIC should publish guidance on how entities could achieve this.

Proposal 25.6 Give the Federal Court and the Federal Circuit and Family Court of Australia the power to make any order it sees fit after a civil penalty provision relating to an interference with privacy has been established.

Proposal 25.7 Further work should be done to investigate the effectiveness of an industry funding model for the OAIC.

Proposal 25.8 Further consideration should be given to establishing a contingency litigation fund to fund any costs orders against the OAIC, and an enforcement special account to fund high cost litigation.

Proposal 25.9 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.

Proposal 25.10 The OAIC should conduct a strategic internal organisational review with the objective of ensuring the OAIC is structured to have a greater enforcement focus.

Proposal 25.11 Amend subsection 41(dc) of the Act so that the Information Commissioner has the discretion not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme.

26. A direct right of action

Proposal 26.1 Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in this chapter.

27. A statutory tort for serious invasions of privacy

Proposal 27.1 Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123.

Consult with the states and territories on implementation to ensure a consistent national approach.

28. Notifiable data breaches scheme

Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.

Proposal 28.2

- (a) Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours.
- (b) Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable.
- (c) Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.

Proposal 28.3 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.

However, this proposal would not require the entity to reveal personal information, or where the harm in providing this information would outweigh the benefit in providing this information.

Consider further a requirement that entities should take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.

Proposal 28.4 Introduce a provision in the Privacy Act to enable the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach. The provision would contain safeguards to ensure that only limited information could be made available for designated purposes, and for a time limited duration.

29. Interactions with other schemes

Proposal 29.1 The Attorney-General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.

Proposal 29.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.

Proposal 29.3 Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

30. Further review

Proposal 30.1 Conduct a statutory review of any amendments to the Act which implement the proposals in this Report within three years of the date of commencement of those amendments.

Contents | Part 1:

3.	Objects of the Act	18
4.	Personal information, de-identification and sensitive information	23
5.	Flexibility of the APPs	47
6.	Small business exemption	52
7.	Employee records exemption	64
8.	Political exemption	72
9.	Journalism exemption	84

Part 1: Scope and application of the Privacy Act

3. Objects of the Act

The objects clause of the Act was introduced to outline the underlying purpose of the Act and to provide assistance with interpretation.¹⁶ The Commissioner is obliged to have due regard to the objects of the Act in performing the functions and exercising the powers that the Act confers.¹⁷

The DPI Report recommended that the Government consider whether the objectives of the Privacy Act should place a greater emphasis on privacy protections for consumers, and whether it remains appropriate for the objectives to require the protection of privacy to be balanced with the interests of businesses in carrying out their functions or activities.¹⁸

Digitalisation and technological innovation have had a significant impact on the ways in which personal information is exchanged and used, as well as the volume of information handled.¹⁹ Our society is increasingly networked: decisions made by one individual about their personal information can impact the privacy of others.²⁰ At the same time, the community expects that personal information will be protected.²¹ If the objects clause is to properly support the ‘constant interpretation and application’ of Australia’s principles-based framework to ‘new technologies and contexts’,²² it needs to accurately describe the intent of the Act.

3.1 The current objects

The first two objects in paragraphs 2A(a) and (b) of the Act are to promote the protection of the privacy of individuals, while recognising that this protection should be balanced with the interests of entities in carrying out their functions or activities.

The Review’s October 2021 Discussion Paper canvassed whether any changes should be made to these objects and noted two areas where submitters raised concerns:

- the scope of the Act, and
- the application of the balancing exercise.

It proposed clarifying that the Act is concerned with protecting the personal information of individuals (that is, informational privacy), and not more general notions of privacy. It also proposed that public interest considerations could guide which subjective interests of entities are to be reconciled with the protection of the privacy of individuals.

3.2 The scope of the Act

Privacy is not defined in the Act. It is a concept that can be broadly construed and may be understood as comprising a number of related concepts including informational privacy, bodily privacy, privacy of communications, and territorial privacy.²³

Most submitters who commented on Proposal 1.1 (a) supported it,²⁴ stating that it was more accurate and would clarify that the Act is concerned with the protection of personal information and not privacy more broadly.²⁵

¹⁶ Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 217

¹⁷ Privacy Act s 29.

¹⁸ ACCC, [DPI Report](#) 477.

¹⁹ Ibid 3, 437; Submission to the Discussion Paper: [OAIC](#), 26.

²⁰ Submission to the Discussion Paper: [Centre for Media Transition](#), 5. See also Salomé Viljoen, ‘A Relational Theory of Data Governance’ (2021) 131 *The Yale Law Journal* 573, cited in Submission to Discussion Paper: [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 10.

²¹ Submission to the Discussion Paper: [OAIC](#), 26. See also, Deloitte, [Australian Privacy Index 2021](#) (Report, May 2021) 7.

²² Submission to the Discussion Paper: [elevenM](#), 6.

²³ [ALRC Report 108](#), [1.31], 142, citing David Banisar, *Privacy and Human Rights 2000: An International Survey of Privacy Law and Developments* (Privacy International, 2000). See also Submissions to the Discussion Paper: [Helen Gregorczyk, University of Queensland](#), 1; [ResMed](#), 2; Submission to the Issues Paper: [OAIC](#), 21; [Kimberlee Weatherall](#), 3.

²⁴ Submissions to the Discussion Paper: [Research Australia](#), 7; [ResMed](#), 2; [Department of Health](#), 3; [Public Health Association of Australia](#), 1; [Australian Communications Consumer Action Network](#), 6; [Law Council of Australia](#), 6; [Shopping Centre Council of Australia](#), 6; [Population Health Research Network](#), 2-3; [Federal Chamber of Automotive Industries](#), 6; [Equifax](#), 6; [Woolworths Group](#), 5; [Australian Collectors & Debt Buyers Association](#), 3; [KPMG](#), 11; [Megan Richardson](#), 1; [Australian Super](#), 1; [Australian Council on Children and the Media](#), 2. See also Submission to the Discussion Paper: [OAIC](#) 26-28; [EWON](#), 2 (submission supported by the [Energy and Water Ombudsman SA](#), [Energy and Water Ombudsman \[Victoria\]](#) and [Energy and Water Ombudsman Queensland](#)).

²⁵ Submissions to the Discussion Paper: [ResMed](#), 2; [Research Australia](#), 7; [Population Health Research Network](#), 2-3; [KPMG](#), 11; [Australian Super](#), 1; [Megan Richardson](#), 1.

Others considered that while it was correct that the Act primarily promotes the privacy of individuals through protecting personal information or data protection, there is no need (and it is not helpful) to narrow the objective of promoting the protection of privacy.²⁶ It was said that the proposed amendment could lead to arguments about whether it is appropriate to take broader privacy considerations into account in interpreting the Act.²⁷ Noting the Discussion Paper's proposals in relation to automated decision-making (ADM) and profiling, it was also submitted that the ambit of the Act may extend beyond information privacy.²⁸

Several submitters said that if the proposed statutory tort for serious invasions of privacy is enacted, the proposed amendment would be inaccurate.²⁹

3.2.1 Proposal

Given the focus of the Act is to provide a framework for the handling and protection of personal information, the objects of the Act should be amended to more clearly reflect this. The Act implements Australia's international obligations in relation to privacy *in part*³⁰ by providing a framework for regulating the collection, use, storage, disclosure and destruction of personal information. It does not cover all aspects of privacy as the term is commonly understood. As outlined in Chapter 27, it is proposed that the Commonwealth consult with the states and territories on introducing a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123 which included enacting the tort in a standalone Commonwealth Act.

3.1 Amend the objects of the Act to clarify that the Act is about the protection of personal information.

3.3 Balancing the protection of privacy and other interests

A range of stakeholders were supportive of the proposed amendment to paragraph 2A(b), including submitters from industry, charity and research organisations.³¹ It was considered that the proposal would help clarify the balancing exercise, particularly where the activities of an entity are harmful or not in the public interest,³² and that it was important to give due weight to public interest activities, including research.³³

Others offered qualified support, submitting that further guidance is needed as to what functions or activities would be considered to be 'undertaken in the public interest'³⁴ or proposing additional criteria,³⁵ or additional factors to be taken into account in applying the test,³⁶ or submitting that privacy should also be recognised as a human right,³⁷ or a public good.³⁸

26 Submission to the Discussion Paper: [Helen Gregorczyk, University of Queensland](#), 1; Castan Centre for Human Rights Law and Centre for Commercial Law and Regulatory Studies ([Castan Centre](#)), 3; [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 8. See also, Submission to the Discussion Paper: [NSW Council for Civil Liberties](#), 4.

27 Submissions to the Discussion Paper: [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 8.

28 Submissions to the Discussion Paper: [Castan Centre](#), 3-4. See also, Submission to the Discussion Paper: [Helen Gregorczyk, University of Queensland](#), who cites the prohibition on direct marketing

29 Submissions to the Discussion Paper: [Megan Richardson](#), 1; [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 7-8; [Castan Centre](#), 4.

30 [ALRC Report 108](#), [5.120].

31 Submissions to the Discussion Paper: [Ramsay Health Care Australia](#), 3; [Privcore](#), 5; [Chartered Accountants ANZ](#), 3; [Shopping Centre Council of Australia](#), 6; [Australian Collectors & Debt Buyers Association](#), 3; [Obesity Policy Coalition](#), 3; [Foundation for Alcohol Research and Education](#), 6; [Australian Council on Children and the Media](#), 2; [Australian Communications Consumer Action Network](#), 6; [EWON](#), 1; [ResMed](#), 2; [Australian Institute of Health and Welfare](#), 3; [Department of Health](#), 3; [CSIRO](#), 2; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 1; [Law Council of Australia](#), 6; [Research Australia](#), 7; [Public Health Association of Australia](#), 1. See also Submission to the Discussion Paper: [Population Health Research Network](#), 3; [Geoscience Australia](#), 7.

32 Submissions to the Discussion Paper: [Foundation for Alcohol Research and Education](#), 6; [Obesity Policy Coalition](#), 3; [Public Health Association of Australia](#), 2, who supported clarifying that the protection of individuals' privacy should only be balanced against the interests of entities in carrying out their functions or activities to the extent that they are undertaken in the public interest

33 Submissions to the Discussion Paper: [CSIRO](#), 2; [Australian Institute of Health and Welfare](#), 3. See also Submission to the Discussion Paper: [Geoscience Australia](#), 7, [ResMed](#), 2.

34 Submissions to the Discussion Paper: [Federal Chamber of Automotive Industries](#), 6; [Calabash Solutions](#), 3; [Social Services Portfolio](#), 7. See also Submissions to the Discussion Paper: [Chartered Accountants ANZ](#), 3; [Public Interest Advocacy Centre](#).

35 Submission to the Discussion Paper: [Privacy 108](#) proposed adding the words 'and for public benefit', 4.

36 Submission to the Discussion Paper: [Electronic Frontiers Australia](#), 4.

37 Submissions to the Discussion Paper: [Digital Rights Watch](#), 6 [Centre for Media Transition](#), 6. See also, Submission to the Discussion Paper: [Privacy 108](#), 4.

38 Submissions to the Discussion Paper: [Minderoo Tech & Policy Lab, UWA Law School](#), 5; [OAIC](#): the public interest in privacy should also be recognised, 28.

Many other submitters did not support the proposal.³⁹ They said that it was unclear and confusing⁴⁰ and went too far, disrupting the balance.⁴¹ The OAIC stated that 'it is open to interpret the public interest in the economic wellbeing of the country as conceivably capturing any commercial practices, which may undermine the benefits of the proposal.'⁴²

Minderoo Tech and Policy Lab pointed out that the proposed balancing of individuals' privacy with the functions or activities of entities carried out in the public interest could have the effect of minimising the protection of privacy as 'any individual interest, no matter how strong, is apt to be counterbalanced by collective interests. While individual interests may win out in particular cases, the overall tendency is likely to be in favour of the collective good.'⁴³

Submitters also said that the objects should recognise the interests of entities in carrying out their legitimate functions or activities,⁴⁴ and that these can be beneficial and align with public interests.⁴⁵

A number of submitters considered that the relevant public interest that the objects clause should recognise is the public interest in protecting privacy itself.⁴⁶ It was pointed out that strong privacy protections build trust which is necessary for economic growth and innovation.⁴⁷ Privacy protections were also cited as critical to the functioning of democracy,⁴⁸ and for facilitating the participation of individuals in all aspects of public life.⁴⁹ Individual choices about privacy can impact others. Managing privacy protection has been described as akin to dealing with an oil spill, or passive smoking.⁵⁰ Advances in data analytics has meant that information collected from one large cohort is increasingly used to make inferences about other individuals, regardless of whether they have consented, or are even aware of it.⁵¹

The OAIC provided a number of examples of individual privacy decisions which impact other people and the community at large, including the use and disclosure of genetic information, the disclosure of aggregated location data, and targeting driven by personal information shared online.⁵² Minderoo Tech and Policy Lab submitted that although claims to privacy are exercised by individuals it is best understood as a public interest, analogous to the capacity to contract and the right to vote.⁵³

- 39 Submissions to the Discussion Paper: [Castan Centre](#), 4; [Australian Privacy Foundation](#), 3; [Experian Australia](#), 5; [Equifax](#), 6-7; [Woolworths Group](#), 5; [KPMG](#), 11; [Optus](#), 9-10; [Australian Retail Credit Association](#), 3; [Australian Banking Association](#), 2; [Business Council of Australia](#), 4; [Association for Data-driven Marketing & Advertising \(ADMA\)](#), 6; [Insurance Council of Australia](#), 3; [Communications Alliance Ltd](#), 6; [Free TV Australia](#), 36; [MIGA](#), 1; [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 4 (submission supported by [Heart Research Australia](#)). See also Submissions to the Discussion Paper: [ANZ](#) 3, 6; [Michael Douglas, UWA Law School](#), 1. Many concerns pertained to the formulation.
- 40 Submissions to the Discussion Paper: [Business Council of Australia](#), 4; [Experian Australia](#), 5; [Insurance Council of Australia](#), 3; [Equifax](#), 6-7; [Woolworths Group](#), 5; [Optus](#), 10; [Communications Alliance Ltd](#), 6; [ANZ](#), 3, 6; [MIGA](#), 1; [ADMA](#), 6.
- 41 Submissions to the Discussion Paper: [Australian Banking Association](#), 2; [Business Council of Australia](#), 4; [Experian Australia](#), 5; [Optus](#), 10.
- 42 Submission to the Discussion Paper: [OAIC](#) 28. See also Submissions to the Discussion Paper: [Castan Centre](#), 4 and [Minderoo Tech & Policy Lab, UWA Law School](#), 5.
- 43 Submission to the Discussion Paper: [Minderoo Tech & Policy Lab, UWA Law School](#), 5. See also Submission to the Discussion Paper: [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 9.
- 44 Submissions to the Discussion Paper: [MIGA](#), 1 (in addition to activities undertaken in the public interest); [ANZ](#), 6. See also Submission to the Discussion Paper: [Michael Douglas, UWA Law School](#), 1; [Free TV Australia](#), 36; [KPMG](#), 12; [Castan Centre](#), 4; [Woolworths Group](#), 5. Submitters also proposed a 'legitimate interests' basis for processing information: [DIGI](#), 6; [Communications Alliance Ltd](#), 7.
- 45 Submissions to the Discussion Paper: [Australian Retail Credit Association](#), 2-4; [Insurance Council of Australia](#), 3; [Communications Alliance Ltd](#), 6-7. See also, [Submission to the Discussion Paper: Business Council of Australia](#), 4.
- 46 Also, or alternatively, a collective or societal interest in privacy, Submissions to the Discussion Paper: [OAIC](#), 28; [Minderoo Tech & Policy Lab, UWA Law School](#), 5; [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 9; [elevenM](#), 8; [Australian Privacy Foundation](#), 4. See also, Submissions to the Discussion Paper: [Electronic Frontiers Australia](#), 4; [Professor David Lindsay](#), 12; [Megan Richardson](#), 1. [Communications Alliance Ltd](#), 6.
- 47 Submission to the Discussion Paper: [elevenM](#), 8.
- 48 Submission to the Discussion Paper: [NSW Council for Civil Liberties](#), 4.
- 49 Submission to the Discussion Paper: [Minderoo Tech & Policy Lab, UWA Law School](#), 5; [elevenM](#), 8.
- 50 Examples given, respectively, by Australian Privacy Commissioner Angelene Falk and Victorian Information Commissioner Sven Bluemmel, as cited by Anna Johnston in [Why privacy is a public good in need of better protection](#) (Web Page, 10 August 2020).
- 51 Submissions to the Discussion Paper: [Centre for Media Transition](#), 5-6; [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 10. See also Submission to the Issues Paper: [Minderoo Tech & Policy Lab, UWA Law School](#), 2-4. [Prof Kimberlee Weatherall](#), 3; [OAIC](#), 24-25.
- 52 Submission to the Issues Paper: [OAIC](#), 24-25.
- 53 Submission to the Discussion Paper: [Minderoo Tech & Policy Lab, UWA Law School](#), 5.

The OAIC recommended amending the objects of the Act to recognise the public interest in privacy, stating:

Recognising the public interest in privacy and the important role that the Privacy Act plays in protecting individuals would help to frame the application and interpretation of the rights and obligations in the legislation, including the proposed fair and reasonable test ... It will also guide and inform the Information Commissioner's regulatory priorities and discretion in exercising their powers and selecting regulatory outcomes.⁵⁴

3.3.1 Proposal

In light of the feedback about the confusion likely to result from the amendment to paragraph 2A(b) proposed in the Discussion Paper, and the need for modernised privacy legislation to promote digital trust,⁵⁵ it is proposed that the objects of the Act be amended to recognise the public interest in protecting privacy. This would assist with 'ensuring that the Act can address instances where privacy-affecting acts and practices have undesirable public policy outcomes, even if the privacy harms to any one individual are not significant.'⁵⁶

The protection of privacy sits alongside other important interests: this is recognised in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and reflected in paragraph 2A(b) of the objects.⁵⁷ These interests are sometimes, but not always, in tension. The Act provides the framework by which entities assess whether impacts on individuals' privacy rights are necessary, reasonable and proportionate to achieving their legitimate functions and other public interests.⁵⁸ Paragraph 2A(b) of the objects should continue to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities. The recognition of a public interest, as well as individual interest, in privacy will inform the balancing exercise,⁵⁹ retaining sufficient flexibility for 'countervailing interests to be given the weight they deserve'.⁶⁰

It is important to note that the protection of privacy and the interests of entities in carrying out their functions and activities, including private commercial activities, are not necessarily in conflict.⁶¹ As the OAIC's submission put it: it is not a zero-sum game.⁶² Businesses that use data in a fair and responsible manner may serve the public interest indirectly, and deliver benefits to individuals and the broader economy, as well as their own commercial interests.⁶³ Entities can benefit from the consumer confidence and economic growth that strong data protection engenders.⁶⁴

3.2 Amend the objects of the Act to recognise the public interest in protecting privacy.

3.4 A right to privacy

A number of submitters continued to call for the objects clause to recognise a 'right to privacy'.⁶⁵ While the reforms to the Act which will be proposed in this paper are directed at ensuring greater weight is given to the protection of individuals' privacy, as noted in the Discussion Paper, Article 17 of the ICCPR does not confer an absolute right to privacy.⁶⁶

⁵⁴ Submission to the Discussion Paper: [OAIC](#), 27 [1.7].

⁵⁵ See, World Economic Forum, [Digital Trust Initiative](#) (Web Page, 2022).

⁵⁶ Submission to the Issues Paper: [OAIC](#), 25.

⁵⁷ Submission to the Issues Paper: [OAIC](#), 21-22.

⁵⁸ Submission to the Issues Paper: [OAIC](#), 22.

⁵⁹ Submission to the Discussion Paper: [OAIC](#), 28.

⁶⁰ Submission to the Discussion Paper: [Castan Centre](#), 4, who submitted that the current wording of the Act is preferable to the formulation proposed in the Discussion Paper.

⁶¹ Submission to the Discussion Paper: [Communications Alliance Ltd](#), 6.


⁶² Submission to the Issues Paper: [OAIC](#), 22.

⁶³ Submissions to the Discussion Paper: [Australian Retail Credit Association](#), 2; [Communications Alliance Ltd](#), 6.

⁶⁴ Submission to the Issues Paper: [OAIC](#), 22.

⁶⁵ Submission to the Discussion Paper: [Digital Rights Watch](#), 2.5; [Australian Privacy Foundation](#), 2-3; [Lived Experience Australia](#), 3; [NSW Council for Civil Liberties](#), 4; [Centre for Media Transition](#), 6; [Professor David Lindsay](#), 12; [elevenM](#), 5-6; [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 4. See also Submission to the Discussion Paper: [Privacy 108](#), 2.4.

⁶⁶ [Discussion Paper](#), 20.



In 2019 the Australian Human Rights Commission (AHRC) commenced a major project 'Free and Equal: An Australian conversation on human rights' which is intended to inform 'a comprehensive reform agenda to modernise human rights protection for all.'⁶⁷ As part of this, the AHRC released its Discussion Paper: A model for positive human rights reform. That Discussion Paper noted that existing legislative protections often frame human rights in the negative rather than the positive, and proposed a number of possible reforms to strengthen the protection of human rights. It is anticipated that the future work by the AHRC will inform what further steps may be taken to recognise and protect privacy in Australia.

⁶⁷ AHRC, [Discussion paper: A model for positive human rights reform \(2019\)](#) (Web Page, 29 August 2019).

4. Personal information, de-identification and sensitive information

The Privacy Act is principles-based, and the definition of ‘personal information’ is a pillar of this design. The definition of personal information is central to the regime of the Act⁶⁸ and the concept that delineates its scope.⁶⁹ The definition needs to be broad enough to capture all types of personal information and the circumstances where such information is created, collected and used.

However, a consequence of a principles-based definition is the danger that entities are not clear about how to apply it to information in practice. Feedback to the Review explained the current scope of personal information can be uncertain.⁷⁰ This lack of understanding was also noted by the ACCC in its DPI Report.⁷¹ The widespread adoption of digital technology and the opportunities it has created for large scale collection, use and disclosure of information arising out of individuals’ communicating with each other, transacting, consuming, creating content and engaging in all manner of daily activities in digital contexts, has generated questions about how the definition applies to information in our economy today.

Before commencing discussion of ‘personal information’ it is important to set the definition in context in the Act. The Act does not prohibit the collection, use and disclosure of personal information. Rather, the Act requires that the principles around personal information handling set out in the APPs must be followed. This includes only collecting reasonably necessary information and only using or disclosing it for the purposes for which it was collected unless the individual consents or another exception applies.⁷² The definition of personal information is intentionally broad. Keeping the breadth of this definition is all the more important in the digital age having regard to the sheer volume and speed at which information is shared and linked. A broad definition ensures that APP entities keep privacy and risk-based personal information handling at the forefront of their minds when conducting their functions or activities.

4.1 What is personal information? The two-limbed test

Section 6 of the Privacy Act defines personal information as follows:

personal information means information or an opinion about 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.

Individual is defined as a ‘natural person’.

The current definition of personal information has two required limbs:

- the information is about an individual, and
- the individual is identified or reasonably identifiable.

The Explanatory Memorandum to the Privacy Bill 1988 (Cth) explained that the potential information⁷³ that could be protected under the Act is ‘infinite’, and would include things like the person’s physical description, residence, place of work, business and business activities, employment, investments and property holdings, relationships to other persons, recreational interests and political, philosophical or religious beliefs.⁷⁴ Personal information held by APP entities will not be covered by the Act unless that information is in a physical or electronic record.⁷⁵

68 ALRC Report 108, 293.

69 Submission to the Issues Paper: OAIC, 27.

70 See for example Submissions to the Discussion Paper: Australian Digital Health Agency, 1; OAIC, 30; Australian Genomics, 1-2; Deloitte Australia, 5-6; Castan Centre, 5.

71 For example, ACCC, DPI Report 393.

72 See Privacy Act sch 1, APP 3 and 6.

73 For the purposes of this chapter information means ‘information or an opinion’, unless the contrary intention is apparent.

74 Explanatory Memorandum, Privacy Bill 1988 (Cth) 11.

75 Privacy Act s 6, see definition of ‘holds’ and ‘record’.

4.1.1 Rationale for reforms to personal information and de-identified information

The Act needs to be flexible enough to apply to the range of activities and information that may engage the diverse range of APP entities.⁷⁶ At the same time, the Act needs to be clear to the wide variety of readers who have to apply it. The Act should not be overly technical, nor require expertise to interpret and apply. It needs to give effect to community expectations and common sense.

ALRC Report 108⁷⁷ preceded the 2012 reforms that created the current definition of personal information in the Act. The Report recommended the definition of personal information cover an individual who is 'reasonably identifiable.' It acknowledged that the definition would continue to give rise to theoretical uncertainty. Accordingly, ALRC Report 108 also recommended practical guidance be developed by the predecessor to the OAIC.⁷⁸ The OAIC publishes guidance on 'What is personal information?' on its website and in its *Australian Privacy Principles Guidelines*.⁷⁹ Notwithstanding this guidance and the lack of direct criticism of that guidance from stakeholders, it is clear from submissions and the consultations conducted as part of this Review that there is considerable confusion and uncertainty about how to interpret the definition.

There are two categories of uncertainty about the definition. First, stakeholders raised concerns that it is unclear which types of information can be personal information. For example, there is confusion about whether technical information that records service details about a device is the personal information of the owner of the device.⁸⁰ Further, there is uncertainty about whether inferred information about an individual, for example in an online profile, will be personal information.⁸¹ Second, stakeholders would welcome clarity about how to 'reasonably identify' an individual and correspondingly how to know when an identifiable individual becomes 'de-identified'.⁸²

The proposals in this chapter seek to clarify the definition of personal information without undermining the flexibility of the Act. The two categories of uncertainty would be clarified through proposals that address the two limbs of the test for personal information:

- Reforms to clarify the types of information that can be personal information by:
 - replacing 'about' an individual in the definition of personal information to 'relates to'. This would not significantly change the definition, but would make it clearer that technical and inferred information can be personal information
 - adding a non-exhaustive list of information that can be personal information to aid interpretation of the definition, and
 - amending the definition of 'collects' to make clear that inferred information is collected at the point the inference is made.
- Reforms to clarify when an individual will be reasonably identifiable from information by:
 - introducing a list of factors to consider when determining whether an individual is reasonably identifiable
 - amending the definition of de-identify to make clear that whether information remains de-identified can change depending on the context, and
 - extending protections to de-identified information that are proportionate to the risk of the information being re-identified.

The discussion in this chapter sets out a framework for thinking about personal information that could be included in explanatory materials to legislative amendments and developed and refined in future OAIC guidance.

⁷⁶ Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 52; see also [ALRC Report 108](#), 300.

⁷⁷ [ALRC Report 108](#).

⁷⁸ *Ibid* 309.

⁷⁹ OAIC, [What is personal information?](#) (Web Page, 5 May 2017); OAIC, [APP Guidelines](#) (July 2019) [B.88]–[B.93].

⁸⁰ See for example Submissions to the Discussion Paper: [Australian Data and Insights Association \(ADIA\)](#), 4; [Public Health Association of Australia](#), 2; [Free TV Australia](#), 36; [Financial Services Council](#), 5.

⁸¹ See for example Submissions to the Discussion Paper: UNSW Allens Hub for Technology, Law and Innovation, the Deakin University Centre for Cyber Security Research and Innovation and the IEEE Society on Social Implications of Technology ([UNSW Allens Hub](#), [Deakin CSRI](#) and [IEEE SSIT](#)), 3–4; [Equifax](#), 7; [Google](#), 1–2.

⁸² See for example Submissions to the Discussion Paper: Interactive Advertising Bureau Australia ([IAB](#)), 13; [Retail Drinks Australia](#), 11; [Australian Department of Health](#), 3–4.

4.2 Proposed changes to clarify the types of personal information

4.2.1 Information that ‘relates to’ an individual

The Discussion Paper proposed replacing the test that for information to be personal information it must be ‘about’ an individual, with a test that the information must ‘relate to’ an individual. This Report recommends proceeding with this proposal.

Recommendation 16(a) in the ACCC’s DPI Report was to update the definition of ‘personal information’ to clarify it captures technical data such as IP addresses, device identifiers, location data and any other online identifiers that identify an individual.⁸³ The ACCC considered there was uncertainty whether these types of information constitute personal information following the decision of *Privacy Commissioner v Telstra Corporation Ltd* (Grubb case).⁸⁴

In the Grubb case, the issue before the Administrative Appeals Tribunal (AAT) was whether telecommunications metadata was personal information which Mr Grubb had a right to access. The AAT determined the case on the basis that it did not think the data was ‘about’ Mr Grubb, but was about the way that Telstra delivers a call or message and the service Telstra provided to Mr Grubb.⁸⁵ The Privacy Commissioner appealed to the Full Court of the Federal Court of Australia, but this appeal was dismissed. The Full Court did not rule on whether the specific metadata in dispute before the AAT was about Mr Grubb as that question was not put before them, but their Honours did conclude that whether information is ‘about’ an individual would ‘require an evaluative conclusion, depending upon the facts of any individual case’.⁸⁶

Since the Grubb decision, there has been confusion around whether technical information is or can be personal information.⁸⁷ The OAIC considers it would be concerning if technical information could not be captured by the definition, given that ‘online and device identifiers are increasingly being used to track individuals and are rivalling names and addresses as key identifiers’.⁸⁸ The ACCC in its DPI Report considered that there would be significant benefits to updating the definition of personal information to cover the realities of how data is collected from individuals in the digital economy and to align the Australian privacy regime with overseas standards.⁸⁹

The Discussion Paper proposal to replace the word ‘about’ in the definition of ‘personal information’ with the words ‘that relates to’ would better highlight that there needs to be a relationship between the information and the individual. This change would not have the intention of significantly expanding the meaning of the word ‘about’ which was always intended to be very expansive.⁹⁰ Together with the other proposals in this chapter, and discussion in an Explanatory Memorandum enacting the reforms, this change would clarify that personal information includes technical information, inferred information and any other information where that information relates to the individual, in the sense it can be seen to provide details about their activities or their identity and the connection is not too tenuous or remote. It would also bring the Act into line with terminology and practice in international data protection regimes, such as the GDPR, and other Commonwealth legislation such as the Consumer Data Right.⁹¹

83 ACCC, [DPI Report](#) 458.

84 [2017] 249 FCR 24. ACCC, [DPI Report](#) 458-459.

85 *Re: Telstra Corp Ltd and Privacy Commissioner* [2015] 254 IR 83.

86 *Privacy Commissioner v Telstra Corporation Ltd* [2017] 249 FCR 24, at [62]–[63].

87 Submission to the Discussion Paper: [OAIC](#), 30.

88 *Ibid.*

89 ACCC, [DPI Report](#) 458.

90 Explanatory Memorandum, Privacy Bill 1988 [Cth] 11-12

91 [Discussion Paper](#), 26-27. See *Competition and Consumer Act 2010* [Cth] s 56AI(3), [Explanatory Memorandum](#), Treasury Laws Amendment (Consumer Data Right) Bill 2019 [Cth] [1.106]–[1.108]

This proposal was generally supported by technology industry groups,⁹² advertising industry associations,⁹³ online platforms,⁹⁴ academics,⁹⁵ civil society and consumer groups,⁹⁶ archivists,⁹⁷ professional services,⁹⁸ financial services,⁹⁹ medical indemnity insurers,¹⁰⁰ health researchers,¹⁰¹ regulators,¹⁰² and the European Commission.¹⁰³ Many of those who supported a change to 'relates to' agreed that the change is necessary to remedy confusion caused by the Grubb decision.¹⁰⁴ Deloitte noted that organisations are increasingly collecting a range of technical information related to individuals, such as IP addresses, device identifiers and location data to facilitate profiling. This information facilitates the creation of online profiles that cause a privacy risk.¹⁰⁵ However, these identifiers may not be treated as falling within the current definition if APP entities do not follow OAIC guidance to 'err on the side of caution' when applying the definition.¹⁰⁶

A smaller number of submitters thought that the existing definition remains appropriate, or expressed concerns about the breadth of 'relates to'. These submissions tended to come from fundraising,¹⁰⁷ financial services,¹⁰⁸ the gaming industry,¹⁰⁹ telecommunications,¹¹⁰ industry bodies,¹¹¹ research bodies,¹¹² and media.¹¹³ However there was no consensus among these submissions as to what 'about' in the current definition means.

The proposed change to the definition would bring Australia closer to the terminology used in GDPR jurisdictions.¹¹⁴ Guidance in these jurisdictions further highlight that this change would not expand the definition beyond how it is currently intended to operate. The United Kingdom's *Data Protection Act 2018* s 3(2) defines 'personal data' as any information *relating to* an individual. However, the UK Information Commissioner's Office (UK ICO) in their guidance on the meaning of 'relates to' in the GDPR uses the word 'about' interchangeably.¹¹⁵

Several submitters were cautious about the compliance costs or regulatory burden of the proposal due to an assumed expansion of the definition.¹¹⁶ However, Calabash Solutions also noted that benefits flowing from the definition would include increased consumer trust, reduced risk of harm in the event of a data breach, and better interoperability with overseas regimes.¹¹⁷ The OAIC considered that the regulatory impact of this change would likely be low.¹¹⁸ Telstra suggested that the extent to which the definition currently captures technical information should be clarified in OAIC Guidance instead of being express in the Act itself.¹¹⁹

92 Submissions to the Discussion Paper: [ACT | The App Association](#), 2; [Australian Information Security Association](#), 5.

93 Submissions to the Discussion Paper: [ADMA](#), 7.

94 Submissions to the Discussion Paper: [Snap Inc.](#), 3; [DIGI](#), 6-7; [Meta](#), 5; [Amazon Web Services](#), 2.

95 Submissions to the Discussion Paper: [Castan Centre](#), 5; [Dr Katharine Kemp](#), UNSW Sydney, 7; [Minderoo Tech & Policy Lab](#), UWA Law School, 2; [Kimberlee Weatherall](#), [Tom Manousaridis](#), [Melanie Trezise](#), 11; [Michael Douglas](#), UWA Law School, 2; [Professor John V Swinson](#), 1.

96 Submissions to the Discussion Paper: [Electronic Frontiers Australia](#), 4; [NSW Council for Civil Liberties](#), 6; [CHOICE](#), 7; [Financial Rights Legal Centre and Financial Counselling Australia](#), 1-3; [Uniting Church in Australia](#), [Synod of Victoria and Tasmania](#), 1; [Foundation for Alcohol Research and Education](#), 6-7; [Law Council of Australia](#), 7; [Obesity Policy Coalition](#), 3; [Governance Institute of Australia](#), 1; [Public Interest Advocacy Centre](#), 8-9; [Digital Rights Watch](#), 2.

97 Submissions to the Discussion Paper: [Australian Society of Archivists](#), 2-3.

98 Submissions to the Discussion Paper: [Deloitte Australia](#), 5; [elevenM](#), 9; [Privacy 108](#), 4; [Calabash Solutions](#), 3; [Salinger Privacy](#), 3-4.

99 Submissions to the Discussion Paper: [FinTech Australia](#), 4; [National Australia Bank](#), 2-3; [Equifax](#), 2.

100 Submissions to the Discussion Paper: [Avant Mutual](#), 5.

101 Submissions to the Discussion Paper: [Australian Genomics](#), 1; [Population Health Research Network](#), 4.

102 Submissions to the Discussion Paper: [OAIC](#), 13; [Office of the Victorian Information Commissioner \(OVIC\)](#), 1; [ACCC](#), 3.

103 Submission to the Discussion Paper: [European Commission](#), 1.

104 Submissions to the Discussion Paper: [Castan Centre](#), 5; [elevenM](#), 9; [Professor David Lindsay](#), 13; [OAIC](#), 30; [Equifax](#), 7.

105 Submissions to the Discussion Paper: [Deloitte Australia](#), 5.

106 OAIC, [What is personal information?](#) (Web Page, 5 May 2017).

107 Submissions to the Discussion Paper: [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 4; [Garvan Institute of Medical Research and Garvan Research Foundation](#), 4; [CARE Australia](#), 1.

108 Submission to the Discussion Paper: [Australian Financial Markets Association](#), 3.

109 Submission to the Discussion Paper: Interactive Games & Entertainment Association ([IGEA](#)), 6-7.

110 Submissions to the Discussion Paper: [Optus](#), 10; Telstra Corporation Limited ([Telstra](#)), 8.

111 Submissions to the Discussion Paper: [Business Council of Australia](#), 6; [IAB](#), 13.

112 Submissions to the Discussion Paper: [CSIRO](#), 2; [Garvan Institute of Medical Research and Garvan Research Foundation](#), 4.

113 Submissions to the Discussion Paper: Australian Broadcasting Corporation ([ABC](#)), 3; Special Broadcasting Service ([SBS](#)), 16.

114 Submissions to the Discussion Paper: [Guardian Australia](#), 16; [Snap Inc.](#), 3; [ACT | The App Association](#), 2; [elevenM](#), 11; [European Commission](#), 1; GDPR art 4(1); Organisation for Economic Co-operation and Development (OECD), [OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data](#), [2013], cl 2, See also [California Consumer Privacy Act 2018](#) (California), § 1798.140(1)(o).

115 UK ICO, [What is personal data?](#) (Web Page, October 2022).

116 See for example Submissions to the Discussion Paper: [Calabash Solutions](#), 3; [CSIRO](#), 3.

117 Submission to the Discussion Paper: [Calabash Solutions](#), 3.

118 Submission to the Discussion Paper: [OAIC](#), 30.

119 Submission to the Discussion Paper: [Telstra](#), 8.

Several submitters also thought 'household' level information should be personal information that is protected. That is, information that identifies a household rather than an individual (such as a shared household computer's search history).¹²⁰ However, the definition with or without the change to 'relates to' should be sufficiently flexible to apply to household data in circumstances where the evaluative exercise determines it should. For example, household data may 'relate to' an individual because the household is small and the inference can be drawn that it relates to one of the members due to the content of the material.

4.2.2 The words 'relates to' would still require a connection to the individual

Technical information about an individual's activities may be viewed as related to the individual notwithstanding that technically the data can also be viewed as being about the individual's service usage. That information is directly used to engage with the individual and records activities and services accessed by the individual.

However, not all information able to be linked to an individual will 'relate to' them. For example, while an address in Sydney may be the personal information of the resident, facts about Sydney will clearly not be. The link to the individual of information about their city is too tenuous.

Likewise, coordinates giving longitude and latitude will not relate to an individual just because it is possible an individual could occupy that geographic space. There needs to be a real connection, such as using those coordinates to locate and proceed to identify an individual, or holding the location together with the knowledge that this is the home of an individual.

Further, the information that flight QF123 has landed in Sydney does not relate to an individual. It could potentially relate to an individual if a person's ticket stub was found, or if it is known who the pilot was, but the information is only able to relate to individuals with further specific external information.

The above examples highlight the importance of context to determining if information relates to a specific individual. If a context of surrounding information is able to create a connection, then the information may relate to the individual. However, just because information may relate to an individual it will not automatically be personal information. Relating to an individual means the connection needs to be a real, not too tenuous or remote, connection which says something about a *specific* individual (not any individual). The second limb of the definition must also be satisfied and the connection must be to an identified or reasonably identifiable individual (see further discussion below).

Concerns that the change to 'relates to' would make the definition of personal information too broad should be addressed when enacting the change. 'Relates to' could be defined in the Act as a connection to the individual that is not too tenuous or remote and which requires an evaluative exercise based on the context and circumstances of the particular case.

The OAIC should publish guidance on the relevant context and circumstances APP entities should have regard to when considering if information relates to an individual. The OAIC could have regard to the following relevant considerations in drafting guidance:¹²¹

- the extent to which the APP entity or a third party seeks to collect and use or is likely to use information to learn about or to evaluate an individual, or to treat them in a certain way, or seek to influence their behaviour or decisions
- the extent to which the information records an individual's features, activities or preferences, and
- the extent to which the information is part of a record about one individual in particular, and not aggregated with other individuals' data.

4.1 Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.

120 Submissions to the Discussion Paper: [Minderoo Tech & Policy Lab, UWA Law School](#), 6; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 3; [elevenM](#), 12-13.

121 Submissions to the Discussion Paper: [Salinger Privacy](#), 4; [Castan Centre](#), 5.

4.2.3 List of the types of information capable of being personal information

The Discussion Paper also proposed including a non-exhaustive list of the types of information capable of falling within the definition of personal information.

The Discussion paper suggested that this non-exhaustive list 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.¹²²

This proposal was intended to provide APP entities with assistance in identifying what types of information can be capable of falling within the definition. After reviewing stakeholder feedback, a list appears warranted due to the continued confusion about the scope and content of the definition.¹²³

Any list would *not* be a prescriptive list of information that would always be personal information. Such a list would defeat the purpose of the principles-based and technology neutral definitions in the Act.¹²⁴ The purpose of a list would be to aid APP entities when they first encounter a new scenario by confirming that they would need to determine whether the information meets the definition, but would not replace the test itself.

A list was generally supported by submissions from privacy advocates, research bodies, charitable groups, and professional services.¹²⁵ These submissions recognised the value of a list that expands upon the widely accepted examples of personal information currently available in OAIC guidance and explanatory materials.¹²⁶ A list in the legislation itself could ensure the definition is clear, particularly by APP entities who may not refer to guidance. A listing mechanism would also reflect similar lists in other jurisdictions.¹²⁷

Businesses supported the intention of this proposal but generally recommended that a list may be better placed in guidance, must keep pace with technological change by remaining technology neutral, and listed categories should not be treated as exhaustive.¹²⁸ The OAIC held similar concerns and recommended that the list be included in the Explanatory Memorandum to amending legislation.¹²⁹ Businesses were also concerned that a list could create ambiguities or reduce flexibility, particularly if expressed in a way that takes the definition's focus away from assessing whether an individual is reasonably identifiable.¹³⁰

Concerns about the utility of listing information in the Act in the face of changing technology could be mitigated by using technologically neutral terms so that it does not become easily outdated.¹³¹ More specific examples of particular technologies or practices could then be dealt with in OAIC guidance.

In addition to the categories suggested in the Discussion Paper, further consideration of this reform has identified there could be benefit in specifying other types of information for clarity. This includes inferred information, technical information and information commonly understood as personal information to ensure there is no confusion generated by their absence.

On balance, a non-exhaustive list of the types of information that can be personal information, framed at a high level and consistent with the principles-based, technology-neutral nature of the definition, would be beneficial. The list could include the following:

122 [Discussion Paper](#), 27.

123 See for example Submissions to the Discussion Paper: [Deloitte Australia](#), 6; [elevenM](#), 10-11; [BSA | The Software Alliance](#), 7-8.

124 Submission to the Discussion Paper: [elevenM](#), 11.

125 Submissions to the Discussion Paper: [Digital Rights Watch](#), 7-8; [Castan Centre](#), 5; [Australian Institute of Health and Welfare](#), 3; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 1; [elevenM](#), 10; [Calabash Solutions](#), 3; [Privacy 108](#), 4; Dr Lisa Eckstein, Professor Dianne Nicol, Professor Margaret Otlowski, Professor Ainsley Newson ([Eckstein et al.](#)), 1.

126 See examples of personal information in OAIC, [What is personal information?](#) [Web Page, 5 May 2017]; OAIC, [APP Guidelines](#) (July 2019) [B.85]–[B.90]; Explanatory Memorandum, Privacy Bill 1988 (Cth) 11.

127 See for example the lists in: GDPR art 4; CCPA § 1798.140(1)(o); *Privacy Act 1985* (Canada), s 3.

128 See for example Submissions to the Discussion Paper: [ANZ](#), 3; [National Australia Bank](#), 1-2; [Meta](#), 18; [Optus](#), 10; [Experian](#), 6.

129 Submission to the Discussion Paper: [OAIC](#), 31.

130 Submissions to the Discussion Paper: [Atlassian](#), 6; [Meta](#), 18; [IAB](#), 13-14.

131 Submission to the Discussion Paper: [elevenM](#), 11

- i. name, date of birth or address¹³²
- ii. an identification number, online identifier, or pseudonym
- iii. contact information
- iv. location data
- v. technical or behavioural data in relation to an individual's activities, preferences, or identity
- vi. inferred information, including predictions of behaviour or preferences, and profiles generated from aggregated information
- vii. one or more features specific to the physical, physiological, genetic, mental, behavioural, economic, cultural or social identity or characteristics of a person

However, it should be made clear that information of the types in the list will only be personal information where it relates to an identified or a reasonably identifiable individual.¹³³ This condition would link the list to where the focus should remain: on the test in the definition.

Listing information that is not personal information

Several submitters canvassed the idea of introducing a definition or list of the types of information that are clearly *not* personal information, to encourage use of data that has limited privacy implications.¹³⁴ These submitters suggested categories such as business contact details, addresses, household data, aggregated data, and publicly available information.¹³⁵ Although this approach has been taken in some jurisdictions,¹³⁶ this is not recommended.

An exclusive list would be counter-productive because the information would not necessarily never be personal information. In each case it will depend on the definitions in the Act. The risk of misinterpreting an inclusive list is that APP entities will take more steps to protect personal information. The risk of an exclusive list is that entities will not apply privacy protections to information that should be protected. Adopting an inclusive list is consistent with the intended preventative approach to the regulation of privacy and recommended by the ALRC.¹³⁷ APP entities should be encouraged to identify and address privacy issues themselves in a flexible, principles-based regime and the OAIC should develop guidance to avoid misinterpretation.

Where a particular type of information, practice, or industry requires further guidance on when in a specific context information can be personal information, that clarification should be left to targeted OAIC guidance or an industry APP Code rather than amending the list that will apply to all contexts. Too much specificity would risk the list becoming out-dated, ambiguous or confusing when applied across the economy.¹³⁸

4.2 Include a non-exhaustive list of information that may be personal information to assist APP entities to identify the types of information that could fall within the definition.

Supplement this list with more specific examples in the explanatory materials and OAIC guidance.

¹³² Contact information or a person's name will not always necessarily identify an individual. However, in a digital economy the likelihood of such information being able to be linked to an individual is high. An APP entity should therefore pay attention to its handling of this information to ensure compliance with the Act when required.

¹³³ Submissions to the Discussion Paper: [Atlassian](#), 6; [Meta](#), 18; [IAB](#), 13-14; [elevenM](#), 11.

¹³⁴ Submissions to the Discussion Paper: [Google](#), 1; [Free TV Australia](#), 25; [Population Health Research Network](#), 4; [Geoscience Australia](#), 5.

¹³⁵ Submissions to the Discussion Paper: [Google](#), 1; [illion](#), 2; [Privacy 108](#), 5-6.

¹³⁶ For example: *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3); *CCPA* § 1798.140(2)-(3); *Information Act 2002* (NT) s 4A(2).

¹³⁷ [ALRC Report 108](#), 248.

¹³⁸ See for example Submissions to the Discussion Paper: [Business Council of Australia](#), 6; [Amazon Web Services](#), 2-3; [ANZ](#), 7.

4.2.4 Define ‘collection’ to clearly cover inferred information

The Discussion Paper proposed bringing OAIC guidance on inferences into the Act’s definition of ‘collection’ to ensure that personal information that is inferred or generated by APP entities triggers obligations under APPs 3, 4 and 5.¹³⁹

This proposal attracted less engagement than proposals 2.1-2.3 but was supported by academics, charitable groups, professional services, and some other businesses.¹⁴⁰ Opposition to this proposal came from the Australian Retail Credit Association,¹⁴¹ and a medical indemnity insurer.¹⁴²

ANZ and Optus’ submissions accurately noted that inferences already captured the moment that the inference meets the definition of personal information.¹⁴³ For example, if personal information is unintentionally generated and recorded from external data and is therefore ‘unsolicited’, APP 4 would likely apply. APPs 5-13 would apply as if the entity had collected the information under APP 3, which includes the entity taking reasonable steps to provide notice or otherwise ensure individuals are aware of the matters listed in APP 5.2.

Including ‘inferred’ in the definition of ‘collect’ would remove confusion about when the APPs begin to have effect for collection and use of inferred personal information, including in data analytics and machine learning processes: the collection would be from the point it is generated.¹⁴⁴ This would enhance trust in entities who use these techniques in the Australian economy. It would also clarify that reasonable steps to give notice apply where personal information is inferred from unidentified information, such as when actively inferring identity from data about geolocation.

Submitters who use techniques such as machine learning were concerned about the potential effect of this change on innovation, or about the potential for the exposure of trade secrets or proprietary data analysis techniques if data subject rights were exercised in respect of inferred information.¹⁴⁵ Accordingly, the proposed right of access and explanation should contain exceptions for commercially sensitive material (see Chapter 18). However, the information generated by a commercially sensitive process itself would still be personal information if it meets the definition.

Submitters were concerned about the potential for inferred information to cause practical challenges for notification and consent, or lead to ‘notification fatigue’.¹⁴⁶ For example a doctor forming an opinion about a patient’s health which would be sensitive information and require notification and consent under the APPs.¹⁴⁷ However, this tension already exists. Collection of inferred and generated information occurs at the point of inference or generation. APP 5 would require notice (and, if applicable, consent) at the time of collection, or as soon as practicable afterwards. The APPs are flexible. The steps to give notice or otherwise ensure the individual is aware of relevant matters are those steps that are reasonable in the circumstances (if any). If the inference made is a natural inference that the individual would expect or it is inseparable from the original information, for example a diagnosis that an individual has a disease from test results, then APP 5 notice would not likely be required.

4.3 Amend the definition of ‘collects’ to expressly cover information obtained from any source and by any means, including inferred or generated information.

139 Such as the requirements to assess whether the APP entity can collect personal information by reference to their functions or activities, seek consent to collect sensitive information, and provide notice of the matters outlined in APP 5. See definition of ‘collects’ in s 6 of the Act; OAIC, [APP Guidelines](#) [July 2019] [B.27-B.28].

140 Submissions to the Discussion Paper: [Centre for Media Transition](#), 6-7; [Minderoo Tech & Policy Lab](#), [UWA Law School](#), 5; [Professor John V Swinson](#), 1; [Uniting Church in Australia](#), [Synod of Victoria and Tasmania](#), 2; [Calabash Solutions](#), 3; [Deloitte Australia](#), 7; [elevenM](#), 13; [Privacy 108](#), 5; [ANZ](#), 4.

141 Submission to the Discussion Paper: [Australian Retail Credit Association](#), 4-5. ARCA submitted that the introduction of inferred information into personal information and collection of personal information will affect the definition of ‘identification information’. Reform of credit reporting is outside the terms of reference of the Review, however it is considered unlikely this issue will arise. The definition of credit information in s 6N of the Act provides that such information includes personal information which is, among other things, ‘identification information’. Identification information is a prescriptive subset of information of the broader category of personal information. The Review does not consider that expressly clarifying that the larger group of information does include certain information, would impact the current content of the defined smaller group.

142 Submission to the Discussion Paper: [Avant Mutual](#), 2-3.

143 Submissions to the Discussion Paper: [ANZ](#), 10; [Optus](#), 10.

144 Submission to the Discussion Paper: [Professor John V Swinson](#), 2.

145 Submissions to the Discussion Paper: [ACT | The App Association](#), 2-3; [Meta](#), 18-19; [Optus](#), 10.

146 Submissions to the Discussion Paper: [Insurance Council of Australia](#), 5; [Communications Alliance Ltd](#), 11.

147 Submission to the Discussion Paper: [Australian Medical Association](#), 6.

4.3 When is an individual identified or reasonably identifiable?

The second limb of the definition is that an individual must be 'identified or reasonably identifiable' for any information that relates to an individual to be 'personal information'. The phrase, 'identified or reasonably identifiable', was introduced into the definition of personal information in the Act in 2012 and replaced 'identity is apparent, or can reasonably be ascertained'. The Explanatory Memorandum for the amendment stated that whether an individual is reasonably identifiable must be 'based on factors which are relevant to the context and circumstances' of the information.¹⁴⁸ The Explanatory Memorandum considered the amendment was required to ensure the definition remained 'sufficiently flexible and technology-neutral to encompass changes in the way that information that identifies an individual is collected and handled' and to capture a broader range of information, including some online identifiers.¹⁴⁹

The Discussion Paper proposed to define 'reasonably identifiable' to cover circumstances in which an individual could be identified, *directly or indirectly* to emphasise that information may become reasonably identifiable indirectly through linking it with other information.

This idea of information that can be linked with a particular individual is an essential concept for personal information. Generally, linked information is information that can be associated with other information by way of a 'link' that is a common attribute or identifier. In the privacy context, that common attribute may be the individual themselves, for example linking a name and date of birth on a driver's licence with a birth certificate to make a fuller picture of a known person; more information is now available about a directly identified individual.

Or the linkage might serve to identify an individual, for example a date of birth with a particular location or workplace may identify only one individual, even if, for example, the name of that person is unknown. The linkage of the information indirectly identifies an individual.

The IC's determinations in the *Clearview* and *7-Eleven* cases discuss that, generally speaking, an individual is 'identifiable' where they are 'distinguished from all others in a group'.¹⁵⁰ They do not necessarily need to be identified from the specific information being handled – an individual can be identifiable where the information can be linked with other information that identifies them or where the linkage forms an ensemble that identifies them.¹⁵¹ The test does not require that an individual's legal identity be known provided the information could be linked back to the specific person that it relates to. These determinations are reflected in current OAIC guidance.¹⁵²

Some might consider their phone number would be personal information. However, as the ALRC pointed out in Report 108, this is not always the case.¹⁵³ A phone number as a bare set of numbers is not personal information. It is only when it is linked to an individual that the numbers fall within the definition. In most cases a phone number would likely be stored with a linked name, but this example highlights the importance of 'linking' to the definition. OAIC guidance explains that reasonable identification does not require that the individual has been identified through linked information in fact at a particular point in time, but rather that the information 'is able to be linked with other information that could ultimately identify the individual'.¹⁵⁴ Where the identification is reasonable to achieve with information that relates to an individual in all the circumstances (including through linking), the information will be personal information.

The digital economy makes it easier to build up large datasets about individuals which may begin as unidentified information, but risks becoming identified as digital technologies facilitate linkages. Identification may occur inadvertently in some cases as datasets or profiles are built up over time.¹⁵⁵ APP entities engaging in activities involving data must have regard to the risk of identification over time. There was sound support for a need to emphasise that the assessment of identifiability extends to matters that in context can be used to indirectly identify an individual.¹⁵⁶

¹⁴⁸ Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 53.

¹⁴⁹ Ibid.

¹⁵⁰ *Commissioner initiated investigation into Clearview AI, Inc. (Privacy)* [2021] AICmr 54 (Clearview Determination); *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy)* AICmr 54 (7-Eleven Determination).

¹⁵¹ 7-Eleven [Determination](#), [28]–[29]; Clearview [Determination](#), [95]–[96].

¹⁵² OAIC, [APP Guidelines](#) (July 2019) [B.105].

¹⁵³ [ALRC Report 108](#), 308.

¹⁵⁴ OAIC, [What is personal information?](#) (Web Page, 5 May 2017).

¹⁵⁵ OAIC, [Guide to data analytics and the Australian privacy Principles](#) (Web Page, 21 March 2018).

¹⁵⁶ See for example Submissions to the Discussion Paper: [Deloitte Australia](#), 8; [Eckstein et al.](#), 2; [Salinger Privacy](#), 14; [The Benevolent Society](#), 2-3; [NSW Council for Civil Liberties](#), 7.

Opposition to a proposal to clarify 'reasonably identifiable' with the words 'directly or indirectly' mainly focused on the need for further guidance¹⁵⁷ or a view the amendment is not necessary because it is already contained within the idea of 'reasonably'.¹⁵⁸

Whilst it is important that entities understand that a person can be identified both directly and indirectly, on balance, further amending the definition of 'personal information' to include these new terms may not solve the lack of clarity. New terms may have unclear limits and would themselves require further guidance.¹⁵⁹ Instead, the proposed change from 'about' to 'relates to' (above), the factors to consider when an individual is reasonably identifiable (below), and a new program of OAIC guidance and outreach would all address the key issue: it is the context of the information, including linkable information, that determines identifiability.

4.3.1 The identifiability spectrum

Many submitters spoke of the difficulty in determining the point at which an individual becomes 'identifiable', or conversely 'de-identified'.¹⁶⁰ Submitters had a range of different approaches to these common concepts.¹⁶¹ Stakeholders also disagreed on what standard should be used to satisfy 'reasonably identifiable'.¹⁶² These areas of confusion and lack of consistency in application were also evident from the ACCC's DPI Inquiry.¹⁶³

The terms 'identified', 'reasonably identifiable' and 'de-identified' in the Act conceive of identification on a spectrum. The spectrum begins at information unrelated to an individual, then moves through various degrees of unidentified information before reaching reasonable identifiability in the middle. On the other side of the spectrum are the degrees of de-identification until an individual can no longer be distinguished and the information can no longer be linked with other information.

Digital Rights Watch suggested that the qualifier 'reasonably' be dropped from the definition on the basis that it may weaken its scope, or because it lacks international equivalents.¹⁶⁴ Overseas case law indicates courts have implied reasonableness into the assessment of identifiability under international privacy laws.¹⁶⁵ Recital 26 of the GDPR indicates that in determining whether an individual is identifiable, 'account should be taken of all the means *reasonably* likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly'. Stakeholders highlighted that given the nature of the assessment requiring consideration of the availability of other information, if the reasonableness qualifier were removed, Australian courts may nonetheless imply reasonableness when gauging identifiability.¹⁶⁶

The diagram below is a visual representation of the identifiability spectrum. It re-iterates the two limbs that are required to meet the definition of personal information – that it must relate to the individual, and the individual must be identified or reasonably identifiable.

157 Submissions to the Discussion Paper: [Australian Banking Association](#), 2; [IAB](#), 17; [ANZ](#), 8.

158 Submissions to the Discussion Paper: [IGEFA](#), 7; [Population Health Research Network](#), 3-4.

159 Submissions to the Discussion Paper: [ANZ](#), 8; [Australian Banking Association](#), 2.

160 Submissions to the Discussion Paper: [ANZ](#), 8-9; [IAB](#), 16-17; [Digital Rights Watch](#), 7.

161 For example compare Submissions to the Discussion Paper: [Deloitte Australia](#), 5-6; [Avant Mutual](#), 2; [IAB](#), 16-17; [Castan Centre](#), 6; [illion](#), 2; [ADMA](#), 10-11; [elevenM](#), 11-13.

162 Submissions to the Discussion Paper: [Free TV Australia](#), 28; [Population Health Research Network](#), 4; [ACCC](#), 3; [Australian Medical Association](#), 2-3; [Deloitte Australia](#), 8-9; [elevenM](#), 11-12; [ANZ](#), 8-9.

163 ACCC, [DPI Report](#) 408.

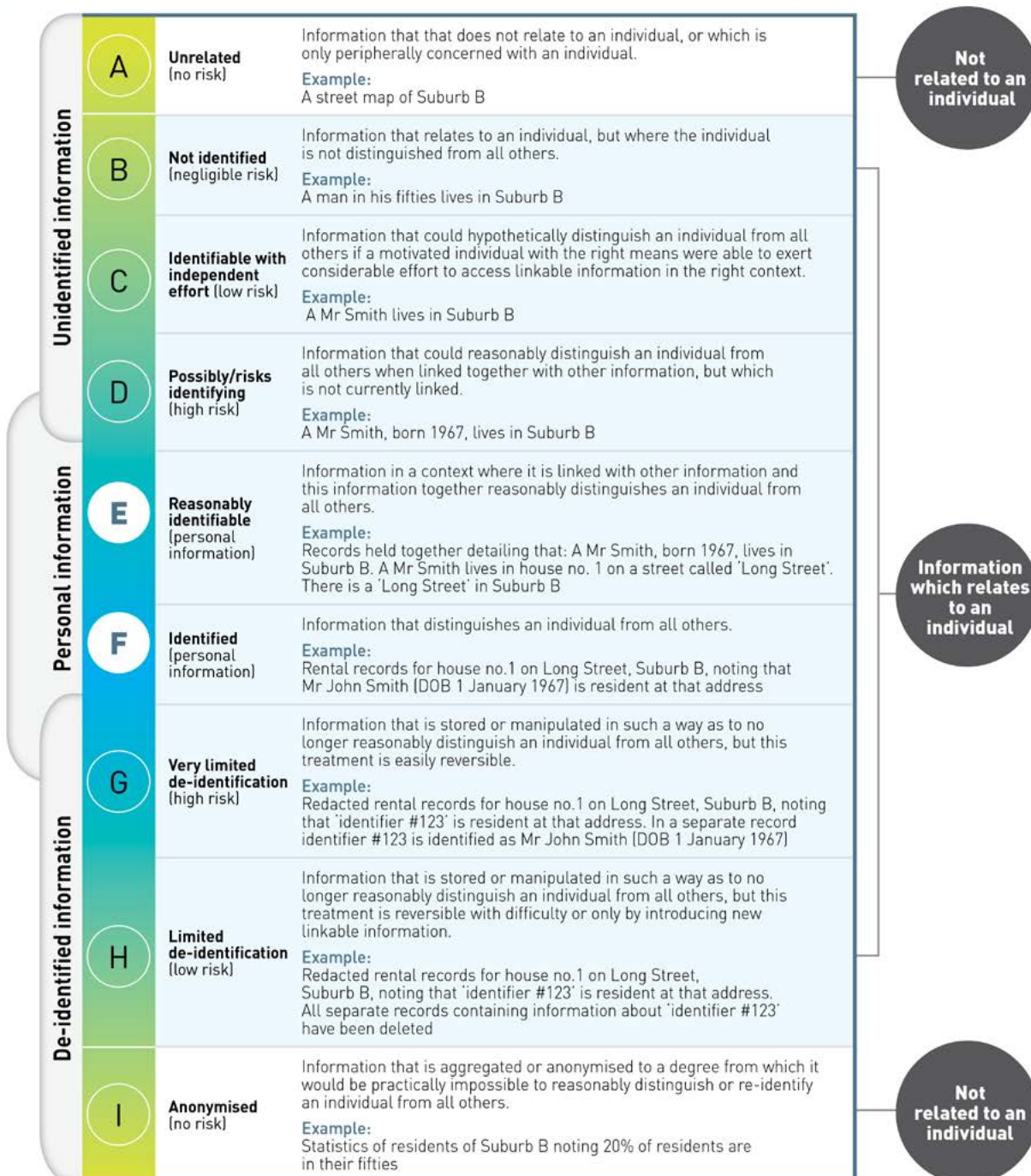
164 Submission to the Discussion Paper: [Digital Rights Watch](#), 7. See also [Castan Centre](#), 6.

165 For example, in the US there is a requirement for 'actual or imminent, not conjectural or hypothetical' risks of harm in litigation: See *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). Refer Ian Ballon, *E-Commerce and Internet Law: Treatise with Forms* (Thomson/West Publishing, 2d Ed, 2019) ch 26, 26.15; and *In re Hulu Privacy Litigation*, No. C 11-03764 LB (N.D. Cal. Apr. 28, 2014).

166 Attorney-General's Department, *Academics, research centres and civil society roundtable*, 24 November 2021.

Diagram 1: Spectrum of Identifiability

Spectrum of Personal Information



- Information located along **E and F** is personal information in the *Privacy Act*
- Information along **D and G** has a high risk of being personal information, and at the higher end may fall into the definition depending on how it is handled. The OAIC generally recommends erring on the side of caution if there is uncertainty about whether information is captured, such that **D and G** should also be treated as personal information.
- Information located along **G, H and I** is 'de-identified information' in the *Privacy Act*.
- Information located along **B and C** is information which relates to an individual, but where the individual is not identified or reasonably identifiable.
- Information along **A and I** would fall outside the Act because it would not meet either limb of the definition of personal information.

Examples in the above diagram are examples of how an individual can become more or less identifiable as the context in which information is held changes.

These examples are not intended as guidance of what will always be or will never be personal information.

4.3.2 Risk management of information

The location of information on the identifiability spectrum can be fluid over time and contexts. Information that in one context does not allow for identification of an individual may, in a different context, identify them. Information that has been quarantined from other information, or had linking identifiers removed to prevent identification, will only continue to prevent identification while those circumstances persist. If new, linkable information is introduced, the individual may once again be able to be identified.

The obligation to mitigate privacy risks in APP 1.2 therefore extends to mitigating the risks of identifiability when APP entities are collecting, using, disclosing and storing unidentified or de-identified information.

A number of submitters to the Review indicate they already focus on risk-based management of information and de-identified information.¹⁶⁷ Current OAIC guidance provides APP entities should err on the side of caution if there is uncertainty about whether or not information is personal information.¹⁶⁸

The actual steps to address risk will depend on the circumstances of the activities of each individual entity. For example (depending on the activities and risks posed by an entity's activities):

- an entity may need to apply a stricter de-identification standard to different disclosures depending on the activities of the recipient and the risks of re-identification in a new context
- an entity may need to use a higher level of encryption on information it keeps for fraud prevention purposes and ensure it is quarantined from de-identified information used for business planning, or
- an entity who wishes to use *only* unidentified information may need to store different datasets separate from one another and implement access controls due to the risk that the collections, when able to be linked, will identify an individual whom it can be foreseen would appear in both datasets.

Chapter 13 on Additional Protections discusses risk management of high risk practices which can include any information on the identifiability spectrum if the factors indicate it should.

4.3.3 Factors to consider when assessing whether a person is 'reasonably identifiable'

As identified by submitters, whether a person is reasonably identifiable will depend on the context in which the information exists,¹⁶⁹ the means reasonably likely to be used to identify someone,¹⁷⁰ from whose perspective the individual must be identifiable,¹⁷¹ and current data processing practices.¹⁷²

OAIC guidance contains factors to assisting identifiability: the nature and amount of information, who holds and has access to information, the other information available, the practicality of using that information to identify an individual, and the context into which information may be disclosed.¹⁷³

The Discussion Paper proposed including a *list of factors* in the Act to assist with the assessment of whether an individual is reasonably identifiable. The Discussion Paper suggested that the factors should include the context in which the information is held or disclosed, the costs and amount of time required for identification and available technology.¹⁷⁴

The OAIC considered that any list should remain in OAIC guidance rather than being in the Act; with the OAIC recommending that APP entities should be required to have regard to their guidance.¹⁷⁵ However, notwithstanding the existence of OAIC guidance, there was support to incorporate factors into the Act either in full or in-principle in

167 Submissions to the Discussion Paper: [Microsoft](#), 4; [Privacy 108](#), 5, 6; [Telstra](#), 9; [Woolworths](#), 5-6; [ADMA](#), 10-11; [IoT Alliance Australia](#), 9-10.

168 OAIC, [What is personal information?](#) (Web Page, 5 May 2017).

169 See for example Submissions to the Discussion Paper: [OAIC](#), 31; [ADMA](#), 12-13; [Experian](#), 8; [Insurance Council of Australia](#), 4.

170 Submissions to the Discussion Paper: [Castan Centre](#), 6; [ANZ](#), 8.

171 Submissions to the Discussion Paper: [ANZ](#), 8; [OAIC](#), 31.

172 Submission to the Discussion Paper: [Castan Centre](#), 6.

173 OAIC, [What is personal information?](#) (Web Page, 5 May 2017).

174 [Discussion Paper](#), 2.3. See GDPR, art 4.

175 Submission to the Discussion Paper: [OAIC](#), rec 4.

submissions from health researchers,¹⁷⁶ businesses,¹⁷⁷ academics,¹⁷⁸ civil society,¹⁷⁹ and the European Commission.¹⁸⁰ Some thought that listed factors would provide an opportunity to clarify the standard of identification risk required for an individual to be reasonably identifiable with suggested standards ranging from 'insignificant or hypothetical',¹⁸¹ to 'very low'.¹⁸² Those opposed generally objected to the suite of proposals 2.1-2.3, but some aired specific concerns that it would cause confusion, or that the reference to indirect identification would make the definition too broad.¹⁸³

De-identified information may be disclosed to a third party who holds information which enables the individual to be identified.¹⁸⁴ It needs to be clear that such a case involves the disclosure of personal information. On the other hand, disclosing information from an environment in which it is personal information into a new context where an individual is no longer identifiable, will not be a disclosure of personal information.¹⁸⁵

The circumstances to aid assessment of reasonable identifiability, could include:

- (a) the nature and volume of the information
- (a) who holds or has access to the information
- (a) how and why the information is collected, used, stored and disclosed
- (a) the other information that is available (or known) to the recipient, and the practicability of using that information to identify an individual, and
- (a) the context in which information is handled, including the context into which information will be disclosed.

Further defining when the reasonableness threshold would be met would not be useful. The range of circumstances in which entities deal with information is broad. Each entity will need to conduct the assessment in their own context and address the reasonableness of identification in that context.

4.4 'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.

4.3.4 Individuation

Several submitters considered that the definition of personal information should extend to the concept of 'individuation'.¹⁸⁶ The concept of individuation as defined by Anna Johnson, Principal of Salinger Privacy is: 'the ability to disambiguate or 'single out' a person in the crowd, such that they could, at an individual level, be tracked, profiled, targeted, contacted, or subject to a decision or action that impacts upon them - even if that individual's 'identity' is not known (or knowable)'.¹⁸⁷ Some submitters suggested including information within the definition of personal information if it can be used to influence, make predictions about, or otherwise facilitate interaction with an individual. The intention behind including this type of information was to address potential harms that flow from the use of this information, which submitters viewed as 'essential to the future effectiveness of data privacy laws'.¹⁸⁸

¹⁷⁶ Submissions to the Discussion Paper: [Australian Institute of Health and Welfare](#), 3; [Eckstein et al.](#), 2.

¹⁷⁷ Submissions to the Discussion Paper: [Meta](#), 18; [ANZ](#), 7-8; [Calabash Solutions](#), 3; [elevenM](#), 11; [Privacy 108](#), 5; [FinTech Australia](#), 5.

¹⁷⁸ Submissions to the Discussion Paper: [Castan Centre](#), 4-5; [Minderoo Tech & Policy Lab](#), [UWA Law School](#), 2.

¹⁷⁹ Submissions to the Discussion Paper: [Uniting Church in Australia](#), [Synod of Victoria and Tasmania](#), 2; [NSW Council for Civil Liberties](#), 7.

¹⁸⁰ Submission to the Discussion Paper: [European Commission](#), 1.

¹⁸¹ Submission to the Discussion Paper: [Castan Centre](#), 6.

¹⁸² Submission to the Discussion Paper: [ANZ](#), 8.

¹⁸³ See for example Submissions to the Discussion Paper: [ABC](#), 3; [Experian](#), 7; [CSIRO](#), 2.

¹⁸⁴ Submission to the Discussion Paper: [Dr Katharine Kemp, UNSW Sydney](#), 7-8.

¹⁸⁵ Submissions to the Discussion Paper: [ANZ](#), 8; [ADMA](#), 10-11.

¹⁸⁶ Submissions to the Discussion Paper: [Salinger Privacy](#), 8-9; [Kimberlee Weatherall, Tom Manousaridis, Melanie Trezise](#), 11; [Graham Greenleaf, UNSW Sydney](#), 3; [Electronic Frontiers Australia](#), 5-6; similar concepts were raised in submissions by [Dr Henry Fraser](#), 2; and [Dr Katharine Kemp, UNSW Sydney](#), 7-9.

¹⁸⁷ Anna Johnson, 'Individuation: Re-Imagining Data Privacy Law to Protect Against Digital Harms', *Brussels Privacy Hub Working Paper*, Vol. 6, No. 42, July 2020, Vrije Universiteit Brussel.

¹⁸⁸ Submissions to the Discussion Paper: [Graham Greenleaf, UNSW Sydney](#), 3. See also [Salinger Privacy](#), 8-9; [Dr Henry Fraser](#), 2.

The concept of individuation as understood by the Review is where information relating to an individual reveals their characteristics and can be used to impact them even though they are not reasonably distinguishable or distinguishable from all others. In the context of targeted content and advertising, information relating to an individual ‘individuates’ them from others and can be used to target them even though they are not reasonably identifiable.

Woolworths expressed concern about extending the definition of personal information to encompass any information that can ‘individuate’ an individual from others because it goes beyond what is reasonably required.¹⁸⁹ Extending the definition of personal information in this way could unjustifiably limit valuable uses of data in ways which do not harm or affect the individuated person. For example, a research subject will likely be individuated in datasets but applying all of the APPs to that information is not justified in terms of potential privacy harms flowing from use of that information in that context. There are also concerns about the ability to apply some privacy protections to that information, particularly the Rights of the Individual.

This information should remain outside the definition of personal information. However, the privacy harms posed by the act of targeting an individual using information relating to that individual including unidentified and de-identified information (or the act of individuating) is addressed in Chapter 20 on targeting.

4.4 De-identified, anonymised and pseudonymised information

The term ‘de-identified’ is currently defined by the Privacy Act to be a state of information where an individual’s personal information is treated in such a way such that the individual is no longer reasonably identifiable. De-identified information sits outside the protections of the Act.

The Review’s October 2020 Issues Paper asked whether additional protections are required for deidentified, anonymised or pseudonymised information as recommended by the DPI Report.¹⁹⁰ Proposal 2.5 of the Discussion Paper proposed to replace the definition of ‘de-identification’ with a definition of ‘anonymous information’. This proposal attracted both varying support¹⁹¹ and opposition¹⁹² from submitters.

Despite available technical guidance on de-identification,¹⁹³ APP entities struggle to apply de-identification in practice because they may fail to understand what standard of de-identification is required. The importance of robust deidentification standards is increasing in the digital economy due to the increasing amount of data in circulation and continuing advances in technology that make identification increasingly available.¹⁹⁴

Many submissions indicated that an irreversible standard of anonymisation would either be extremely difficult or impossible.¹⁹⁵ Some submitters pointed out that information like genetic or genomic information may, by its nature, never be able to be truly divorced from the individual to which it relates and therefore never be able to be truly anonymised.¹⁹⁶ ADMA and other submissions referred to the practical impossibility of achieving a state of complete and forever anonymisation.¹⁹⁷ Associate Professor Vanessa Teague submitted that de-identification for detailed individual records will almost always be re-identifiable. Associate Professor Teague suggested it was only aggregated data of sufficiently large groups that was capable of reliable anonymisation without risk of re-identification.¹⁹⁸ The OAIC noted the need for regulation to remain proportionate to risk and cautioned against an irreversible standard.¹⁹⁹

189 Submission to the Discussion Paper: [Woolworths](#), 3.

190 [Discussion Paper](#), 29-30. See also ACCC, [DPI Report](#), rec 17(f), 480.

191 Support to a varying degree was expressed in Submissions to the Discussion Paper: [Castan Centre](#), 6; [Dr Katharine Kemp, UNSW Sydney](#), 7; [Minderoo Tech & Policy Lab, UWA Law School](#), 2; [Professor David Lindsay](#), 15; [elevenM](#), 13-14; [Privacy 108](#), 6; [DIGI](#), 8; [FinTech Australia](#), 6-7; [Retail Drinks Australia](#), 11-12; [Access Now](#), 3; [Digital Law Association](#), 11; [Digital Rights Watch](#), 7-8; [NSW Council for Civil Liberties](#), 9-10; [ACCC](#), 3; [OAIC](#), rec 6; [Meta](#), 5.

192 Opposition to a varying degree was expressed in Submissions to the Discussion Paper: [Eckstein et al.](#), 2; [ANZ](#), 4; [Equifax](#), 2; [Google](#), 2; [Microsoft](#), 3-4; [Optus](#), 9; [Telstra](#), 10-11; [Australian Banking Association](#), 2; [ADMA](#), 10-13; [Australian Retail Credit Association](#), 5-6; [Business Council of Australia](#), 6; [IAB](#), 5; [IGEA](#), 9-10; [Tech Council of Australia](#), 5; [Avant Mutual](#), 3; [MIGA](#), 2; [AAMRI](#), 2-3; [Law Council of Australia](#), 7; [Australian Digital Health Agency](#), 2; [Services Australia](#), 4; [CSIRO](#), 2-3; [Free TV Australia](#), 27-28.

193 OAIC, [De-identification and the Privacy Act](#) (March 2018); Christine O’Keefe, Stephanie Otorepec, Mark Elliot, Elaine Mackey and Kieron O’Hara, [‘The De-Identification Decision-Making Framework’](#) (2017) (CSIRO Reports EP173122 and EP175702).

194 [Discussion Paper](#), 30.

195 Submissions to the Discussion Paper: [Eckstein et al.](#), 2-3; [Avant Mutual](#), 3; [Deloitte Australia](#), 8-9; [Equifax](#), 2; [Optus](#), 9; [ADMA](#), 10-13; [Ai Group](#), 7-8; [IoT Alliance Australia](#), 8-9; [Tech Council of Australia](#), 5; [Free TV Australia](#), 27-28; [Research Australia](#), 8.

196 Submissions to the Discussion Paper: [Garvan Institute of Medical Research and Garvan Research Foundation](#), 5; [Eckstein et al.](#), 2-3;

197 Submissions to the Discussion Paper: [ADMA](#), 11-12; [Ai Group](#), 7-8; [IoT Alliance Australia](#), 8-9.

198 Submission to the Issues Paper: [Vanessa Teague](#), 4.

199 Submission to the Discussion Paper: [OAIC](#), 38.

The Australian Privacy Foundation suggested an alternative approach that unless the information is deleted, the Act should apply.²⁰⁰ Some suggested a standard of 'functional anonymisation' be implemented whereby legal and access controls around re-identification should be considered,²⁰¹ or that a middle tier of 'pseudonymised information' be created subject to less strict obligations if anonymisation were to be implemented.²⁰²

Some believed that the standard of de-identification required was not in fact the issue, rather that APP entities should be properly using existing frameworks, like the De-Identification Decision Making Framework (DDF), and such frameworks should be promoted.²⁰³ However, mandating the use of the DDF was not supported by one of the co-authors of the framework, the CSIRO, who noted the framework was already becoming dated and the practical difficulties with continuously updating the framework.²⁰⁴ Mandating any specific standards may be unwise. Even what at one point may be considered best practice may be shown with time to have gaps or flaws.²⁰⁵

Stakeholders submitted that they are best equipped to assess the risk of identification in the context in which information is handled, held or released.²⁰⁶ They should be expected to employ available and relevant best practice.

4.4.1 De-identification is a contextual process

Given the impracticality of achieving irreversible anonymisation, a complete anonymisation standard is not warranted in the Privacy Act. However, de-identification should not be viewed as a static condition. The level of technical de-identification is determined by the context in which the information is held, used or disclosed, or, in other words, the risk of re-identification. De-identified information for the purposes of the principles-based Privacy Act should be defined to make it clear that de-identifying information is a process that involves treating it in such a way so as to not allow an individual to be reasonably identifiable while those circumstances persist.

The current definition in section 6 of the Act and in the APPs speaks of de-identification in the present tense, as a task that could be performed and 'de-identification' achieved. However, de-identification is subject to its circumstances. When those circumstances change (for example it is moved to a new environment or new linkable information is introduced), an APP entity cannot rely on the past de-identification and must conduct a proportional reassessment and possibly further de-identification.

The Act gives effect to the principle of data minimisation.²⁰⁷ APP entities should be encouraged to only collect and keep the personal information they need, and to use de-identified rather than raw personal information where the latter is not required. APP entities may be able to engage in 'functional de-identification' with strict organisational and technical controls so that identifying information is separated. This enables risk managed use, even though without the controls the information would be personal information. De-identification is different to true anonymisation which may only be achievable by aggregating individuals' data together.

Where further standards and guidance is required due to technically complex and evolving uses of personal information and de-identified information, the flexibility of the Privacy Act to develop codes discussed in Chapter 5 may be of assistance.

4.5 Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information that involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.

200 Submission to the Discussion Paper: [Australian Privacy Foundation](#), 5-6.

201 Submissions to the Discussion Paper: [ADMA](#), 10-13; [IoT Alliance Australia](#), 8-9.

202 Submissions to the Discussion Paper: [Business Council of Australia](#), 6; [Ai Group](#), 8; [NSW Council for Civil Liberties](#), 9; [ResMed](#), 2.

203 Submissions to the Discussion Paper: [Australian Institute of Health and Welfare](#), 3; [ANZ](#), 11; [Privacy 108](#), 6; [ADMA](#), 11-12. See also [The De-Identification Decision-Making Framework](#).

204 Submission to the Discussion Paper: [CSIRO](#), 14-15.

205 Chris Culnane, Benjamin Rubinstein and David Watts, 'Not fit for purpose: A critical analysis of the 'Five Safes'' (2020).

206 Submission to the Discussion Paper: [IGEA](#), 9.

207 See OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, [OECD/LEGAL/0188](#), pt 2, 'basic principles of national application', 10.

4.5 Protections for de-identified information

Given there is a risk that de-identified information can be re-identified, there is benefit in extending some of the protections of the Act to it.

Disclosure of de-identified information into an environment where it can be linked with other information may enable an individual to be identified or become reasonably identifiable. In recognition of this risk, privacy laws in other countries place restrictions on disclosure of de-identified or pseudonymised information.²⁰⁸

Canada's proposed new privacy reform Bill, the *Digital Charter Implementation Act 2022* would enact the *Consumer Privacy Protection Act* (CPPA) (Bill C-27), and recognise a concept of de-identified information which is considered to be personal information and must be treated as such with the exception of data subject rights.²⁰⁹ The GDPR also extends protections to information where contextually the risk of identification is present.²¹⁰

It would not be appropriate to apply all of the protections under the Act to de-identified information as there is insufficient justification to hinder activities that seek to maximise the utility and productivity of de-identified data. Encouraging use of de-identified data in a privacy risk-managed context was supported by many APP entity users of digital personal information.²¹¹ Encouraging de-identification reinforces the value to the economy and public at large of permitting APP entities to use risk-managed data to improve their services or conduct research. The Privacy Act should not discourage these practices, but should rather ensure that functional or incomplete de-identification is afforded the necessary protections to ensure that the public can have confidence that entities are appropriately managing the privacy risks associated with handling de-identified information.

The OAIC's APP Guidelines on deidentification 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).²¹² It is therefore likely that many APP entities already consider the risk of re-identification when disclosing de-identified information. However, given the risk, the information should be expressly subject to proportionate additional protections in the Act.

It is proposed that the protections under APP 11.1 should apply to de-identified information. The reasonable steps required to protect de-identified information will be those steps that reinforce the quality and continuation of the de-identification, including further reasonable steps to protect it from motivated third parties where the information is sensitive, voluminous, or valuable.²¹³

APP 8 should also apply to de-identified information. It would undermine the protections in APP 11.1 if APP entities could simply disclose de-identified information to a partner overseas where it may be re-identified without breaching the APPs. APP 8 should be amended to require that APP entities take reasonable steps when disclosing de-identified information overseas to ensure that the receiving entity does not re-identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification.

Finally, it is important to note that the NDB scheme in Part IIIC of the Act would also extend to de-identified information where the access or disclosure would be likely to result in serious harm because of the risk of re-identification together with the sensitivity of the information and other relevant harm factors.²¹⁴ This is further discussed in the Chapter 28.

208 *Act on the Protection of Personal Information* (2003) (Japan), art 35-2; CCPA § 1798.148.

209 [Bill C-27](#) ss 2(3), 21, 22, 39, 55, 56, 71, 116.

210 See Court of Justice of the European Union discussion at [39]–[44] in *Breyer v Deutschland* (C-582/14) EU:C:2016:779.

211 Productivity Commission, *Data Availability and Use* (Inquiry Report No. 82, 31 March 2017) 4; Submissions to the Discussion Paper: [Google](#), 3; [BSA | The Software Alliance](#), 8-9; [DIGI](#), 3.

212 OAIC, *Australian Privacy Principles Guidelines* (July 2019), [B.60]–[B.61], [11.42]–[11.44].

213 See Submissions to the Discussion Paper: [CSIRO](#), 3; [Castan Centre](#), 6; [Salinger Privacy](#), 5.

214 Submission to the Discussion Paper: [OAIC](#), 39.

4.6 Extend the following protections of the Privacy Act to de-identified information:

- **APP 11.1 – require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information: (a) from misuse, interference and loss; and (b) from unauthorised re-identification, access, modification or disclosure.**
- **APP 8 – require APP entities when disclosing de-identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information, including ensuring that the receiving entity does not re-identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification.**
- **Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice. (See further Chapter 20)**

4.5.1 Prohibition on re-identification

The Discussion Paper proposal 2.6 suggested re-introducing the lapsed Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments to address the concerns of the Senate Standing Committee on Legal and Constitutional Affairs.²¹⁵

ANZ submitted an offence provision together with strengthening de-identification practices could be a good alternative to requiring full anonymisation.²¹⁶ A statutory prohibition or fines for re-identification was considered helpful by some submitters to deter attempts to circumvent de-identification.²¹⁷ Other submitters were concerned that an offence would discourage research and public release of data itself,²¹⁸ or was not a substitute for addressing the problem of inadequate de-identification practices.²¹⁹ Further criticism of a criminal offence was that it would not likely discourage the most malicious actors or those based in foreign jurisdictions.²²⁰

The OAIC supported the re-introduction of the Bill with amendments, which could serve as a deterrent and improve compliance as part of accountability requirements to take steps to prevent re-identification. It noted that any offence should be subject to appropriate exceptions for research and information security analysis.²²¹ The Australian Computer Society supported an offence but emphasised the need for intent.²²²

A number of other countries have implemented re-identification offences. In Canada's proposed Bill C-27, s 75 prohibits organisations using de-identified information to identify an individual except to test de-identification or comply with laws. Section 128 creates an indictable offence for contravention of s 75 punishable by a fine calculated as a percentage of gross global revenue.²²³ The United Kingdom has an offence for knowing re-identification of

215 Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Privacy (Re-Identification) Offence Bill 2016* ([Report, February 2017](#)), *Dissenting Report of the Australian Labor Party and Australian Greens*, 1.3; Department of the Prime Minister and Cabinet, [Australian Government Public Data Policy Statement](#), 7 December 2015.

216 Submission to the Discussion Paper: [ANZ](#), 11.

217 Submissions to the Discussion Paper: [Civic Data](#), 5; [elevenM](#), 14; [OAIC](#), rec 11, 39.

218 Submissions to the Discussion Paper: [Castan Centre](#), 6-7; [Civic Data](#), 5; [Centre for AI and Digital Ethics](#), 3; [Dr Katharine Kemp, UNSW Sydney](#), 9; [Australian Privacy Foundation](#), 6; [Privacy 108](#), 6-7; [Internet Association of Australia](#), 4.

219 Submission to the Issues Paper: [Vanessa Teague](#), 4.

220 Submissions to the Discussion Paper: [Centre for AI and Digital Ethics](#), 3; [Privacy 108](#), 6; [NSW Council for Civil Liberties](#), 10-11.

221 Submission to the Discussion Paper: [OAIC](#), 39-40.

222 Submission to the Discussion Paper: [Australian Computer Society](#), 2.

223 Bill C-27, 'An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts', Parliament of Canada, [First Reading Speech](#), 16 June 2022.

de-identified information without the consent of the controller.²²⁴ Singapore has a criminal offence for re-identification of anonymised information without authorisation punishable by imprisonment.²²⁵ Japan likewise has a similar offence.²²⁶ These offence provisions apply to information released by both public agency and private organisations.

However, a re-identification offence would not address poor de-identification practices and disclosures. elevenM submitted that a re-identification offence would be an ineffective and unnecessarily punitive approach to the problem of government agencies publishing poorly de-identified information.²²⁷ Privacy 108 did not support Proposal 2.6 due to APP 3 and 6 applying to re-identification already and that the offence would still leave data at risk to foreign entities.²²⁸

Salinger Privacy strongly opposed the re-identification offence on the basis that it did not address poor de-identification practices and may affect public interest research and cybersecurity efforts. The statutory tort was considered a better way to regulate re-identification.²²⁹ Electronic Frontiers Australia agreed that a tort was a more appropriate way to regulate re-identification. However, a statutory tort would only capture serious infringements which would not cover all types of re-identification.²³⁰

It would not be appropriate to introduce criminal offences for re-identification of de-identified information released by government agencies as contemplated in the Privacy Amendment (Re-identification) Offence Bill 2016. Since that Bill, the *Data Availability and Transparency Act 2022* (Cth) (DAT Act) has passed the Parliament. The DAT Act provides a regime for the disclosure of government datasets containing personal information and de-identified information. The DAT Act contains criminal offences for breaches of the DAT Act regime. The DAT Act is the appropriate avenue for criminal penalties to apply to government data disclosed under that scheme.

However, a criminal offence for strictly malicious re-identification of de-identified information may be justified. This offence should not be limited to re-identification of government agency datasets, but all information de-identified by any APP entity. This offence would be aimed at individuals who seek to cause harm or obtain an illegitimate benefit through re-identification.²³¹ These individuals may be external to the APP entity or they may be employees acting maliciously.

To address submitters concerns, the offence should not apply to research involving cryptology, information security and data analysis, and in order to conduct testing of the effectiveness of security safeguards that have been put in place to protect the information.²³²

4.7 Consult on introducing a criminal offence for malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit, with appropriate exceptions.

4.5.2 Prohibition in the APPs

While an offence for malicious re-identification would be directed at deterring bad actors, the potential for privacy harms resulting from re-identification also applies where APP entities share de-identified information with third parties who engage in re-identification. A malicious re-identification offence should also not be an excuse for APP entities to not take necessary precautions to protect de-identified information from malicious re-identification.²³³

A prohibition in the Act on re-identification could operate to prevent APP entities from re-identifying de-identified information that they collected in a de-identified state. Breach of the prohibition would constitute an interference with privacy and would be enforceable by the OAIC.

²²⁴ *Data Protection Act 2018* (UK) ss 171, 196.

²²⁵ *Personal Data Protection Act 2012* (Singapore) s 48F.

²²⁶ *Act on the Protection of Personal Information* (Japan) art 38.

²²⁷ Submission to the Discussion Paper: [elevenM](#), 14.

²²⁸ Submission to the Discussion Paper: [Privacy 108](#), 6.

²²⁹ Submission to the Discussion Paper: [Salinger Privacy](#), 5.

²³⁰ Submission to the Discussion Paper: [Electronic Frontiers Australia](#), 7.

²³¹ Submission to the Discussion Paper: [Australian Computer Society](#), 2.

²³² See for example Submissions to the Discussion Paper: [Castan Centre](#), 6-7; [Civic Data](#), 5; [Centre for AI and Digital Ethics](#), 3.

²³³ Submissions to the Discussion Paper: [OAIC](#), 39-40; [Australian Computer Society](#), 2.

The prohibition would work in conjunction with the requirement on the APP entity disclosing the de-identified information to have regard to the factors relevant to whether a person can be reasonably identifiable (discussed earlier in this chapter). Where an APP entity disclosed de-identified information with the knowledge or expectation that the information would be re-identified, the de-identified information would effectively be disclosed as personal information due to the context of its disclosure.

It would not be appropriate for the prohibition to apply:

- If the entity that originally de-identified the information re-identifies it and complies with APPs 3 and 6 within the context of the original collection, and
- If the controller processor distinction is introduced (as discussed in Chapter 22), and the processor re-identifies the information with the authorisation of the controller.

However, if the entity that re-identifies the information is not covered by the Act (an individual or a small business if the exemption is not removed), the prohibition could not apply. In these circumstances, the APP entity who discloses the information should take reasonable steps consistent with its obligations under APP 11 to ensure that the receiving party does not re-identify the de-identified information.

Exceptions to the prohibition should also be similar to those for the proposed criminal offence such as research involving cryptology, information security and data analysis, and in order to conduct testing of the effectiveness of security safeguards that have been put in place to protect the information. This should enable the quality of de-identification to be safely assessed.

4.8 Prohibit an APP entity from re-identifying de-identified information obtained from a source other than the individual to whom the information relates, with appropriate exceptions.

In addition, the prohibition should not apply where:

- **the re-identified information was de-identified by the APP entity itself - in this case, the APP entity should simply comply with the APPs in the ordinary way**
- **the re-identification is conducted by a processor with the authority of an APP entity controller of the information.**

4.6 Information about deceased individuals

The Act applies to living, natural persons and only captures information about deceased individuals where the information is also about a living person.²³⁴ This approach is consistent with the international instruments upon which the Act is based,²³⁵ but inconsistent with some Australian states and territories.²³⁶ In 2008, the ALRC recommended the Act be extended to cover information about deceased persons.²³⁷

²³⁴ Privacy Act s 6 'individual means a natural person'. OAIC, ['What is personal information?: Information about deceased persons'](#), [Web Page, 5 May 2017].

²³⁵ See for example *International Covenant on Civil and Political Rights*, Opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976); OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, [OECD/LEGAL/0188](#).

²³⁶ See for example *Information Act 2002* (NT), s 4: '...includes a deceased individual within the first 5 years after death'; *Privacy and Personal Information Protections Act 1998* (NSW), s 4(3)(a): personal information does not include 'information about an individual who has been dead for more than 30 years'.

²³⁷ [ALRC Report 108](#), 377.

A small number of submitters addressed this issue in submissions to the Discussion Paper, including medical stakeholders and government bodies.²³⁸ These submissions noted that while the deceased generally are not afforded privacy rights,²³⁹ information does not necessarily lose its sensitivity merely because the individual has died.²⁴⁰

Since the Discussion Paper was released, the Standing Council of Attorneys-General agreed that an access scheme for digital records after death or loss of decision-making capacity would be one of the work priorities for 2022. In December 2022, the Standing Council of Attorneys-General agreed to provide drafting instructions to the Parliamentary Counsel's Committee for the development of uniform model legislation for a national access scheme for digital records after death or incapacity.²⁴¹ Any reforms to the Act consequent upon this work could be considered by the Intergovernmental Working Group discussed at Chapter 29.

4.7 Sensitive information

Designated categories of sensitive information are contained in the Act. Sensitive information is subject to additional protections. It may only be collected with consent unless an exception applies, and more stringent requirements apply to its use or disclosure.²⁴²

Sensitive information is defined as:²⁴³

- information or an opinion about an individual's:
 - racial or ethnic origin
 - political opinions
 - membership of a political association
 - religious beliefs or affiliations
 - philosophical beliefs
 - membership of a professional or trade association
 - membership of a trade union
 - sexual orientation or practices, or
 - criminal recordthat is also personal information.
- health information about an individual²⁴⁴
- genetic information (that is not otherwise health information)
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
- biometric templates.

The Discussion Paper did not make any proposals to amend the definition of sensitive information. Instead, it asked what the risks and benefits would be if the definition were amended, or expanded to include new categories of personal information.²⁴⁵

4.7.1 Updating existing categories of sensitive information

Biometric information

Biometric information is sensitive information if it is to be used for the purpose of automated biometric verification or biometric identification.²⁴⁶ Other biometric information that is not a template or used for automatic biometric identification would be personal information where it meets the definition. Biometric templates form a separate category of sensitive information and are covered regardless of whether they first meet the definition of personal information.

238 See for example Submissions to the Discussion Paper: [Social Services Portfolio](#), 16; [Privacy 108](#), 5-6; [Australian Federal Police \(AFP\)](#), 8; [Australian Department of Health](#), 18; [Australian Genomics](#), 3; [Australian Medical Association](#), 19; [Australian Computer Society](#), 2; [Australian Society of Archivists](#), 3-4.

239 Submission to the Discussion Paper: [Professor John V Swinson](#), 3.

240 Submissions to the Discussion Paper: [Social Services Portfolio](#), 16; [Australian Society of Archivists](#), 3-4.

241 Attorney-General's Department, [Standing Council of Attorneys-General communique](#) [9 December 2022] 4.

242 Privacy Act sch 1, APPs 3, 6.

243 Privacy Act s 6 'sensitive information'.

244 For the definition of *health information*, see Privacy Act s 6FA.

245 [Discussion Paper](#), 33-35.

246 Privacy Act s 6 'sensitive information'. Note that 'biometric information' itself is not defined.

The ALRC in Report 108 recommended that identifying biometric information should be ‘sensitive information’ under the Act because of the serious privacy concerns around being used to identify an individual without their knowledge or consent.²⁴⁷ The Office of the Privacy Commissioner submitted at the time to the ALRC that only such biometric information that can be used to identify an individual should be sensitive information, other biometric information would still be captured by the Act if it meets the definition of personal information.²⁴⁸ Biometric templates and biometric information used to verify identity are unique and inalienable to the individual such that they warrant particular protection. Professor Peter Holland and others explained that the sensitivity of biometric information arises because of its unchangeable nature and inability to recover or protect biometric information if compromised.²⁴⁹ The Australia Institute’s Centre for Responsible Technology pointed to deeper harms, such as biometric scanning normalising surveillance culture and the potential for one-to-many facial recognition to result in false positives or misidentification.²⁵⁰

Submissions highlighted that biometric information is increasingly collected for identity verification in new ways. For example, voiceprint technology can be used to improve customer identification and call handling in client-facing workplaces,²⁵¹ and facial detection can be employed to measure consumer sentiment in retail settings.²⁵² Virtual and augmented reality technologies can collect data about gaze and body movements which can be so unique that it can be impossible to effectively de-identify.²⁵³ The Foundation for Alcohol Research and Education outlined that even information about stress levels or sleep patterns can be collected and collated for marketing purposes.²⁵⁴ While many submitters outlined that such uses of biometric information can be beneficial, a number of submissions recommended that as a consequence of expanding use, a broader range of uses of biometric information should be considered sensitive.²⁵⁵

OAIC guidance and IC determinations indicate that biometrics information can include both physiological features (like fingerprints, iris, or face geometry) and behavioural attributes (like a person’s gait or keystroke pattern).²⁵⁶ However, there is little detail on what is considered to be biometric information in the APP Guidelines.²⁵⁷ For example, the Guidelines are silent on whether metrics such as heartbeat, ear, odour and vein recognition may fall within the definition.²⁵⁸

Submitters called for more examples of biometric information, automated biometric information or verification and biometric templates to be provided in OAIC guidance.²⁵⁹ Others wanted greater protections to apply to biometric information, such as designating its use as a restricted practice.²⁶⁰ UNSW Allens Hub, Deakin CSRI and IEEE SSIT called for entirely separate regulation of biometric information in light of legislation in other jurisdictions.²⁶¹ The AHRC in its 2021 *Human Rights and Technology Report* recommended that Australia’s federal, state and territory governments should introduce legislation to regulate the use of FRT and other biometric technology.²⁶² If biometric information does not and cannot be used to identify an individual, and is not used for the purpose of automated biometric verification or biometric identification, it is not regulated by the Privacy Act.²⁶³ However, that does not mean that it cannot carry risks of harm. As discussed in Chapter 13, there are potential uses of biometric information that may warrant targeted regulation in the future.

The definition of sensitive information in the Act can encompass a broad range of biometric information, including behavioural biometrics, where used for automated verification or identification or a template is created. However, the definition is also deliberately limited. This is to avoid capturing information that may pose negligible risk as sensitive information because of its use or nature (such as a photo not used for identification purposes). What is considered biometrics for the purposes of the definition of sensitive information in the Act should be developed in OAIC guidance and guidelines. This guidance will need to be updated by the OAIC as technology develops.

247 ALRC Report 108, 325.

248 Submission to ALRC Report 108: Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007.

249 Submissions to the Discussion Paper: Professor Peter Holland, 4; UNSW Allens Hub, Deakin CSRI and IEEE SSIT, 13-14.

250 Submission to the Discussion Paper: The Australia Institute – Centre for Responsible Technology, 8.

251 Submission to the Discussion Paper: Australian Collectors & Debt Buyers Association, 4.

252 Submissions to the Discussion Paper: Shopping Centre Council of Australia, 3-4; Centre for Media Transition, 7; 7-Eleven Determination.

253 Submission to the Discussion Paper: Dr Ben Egliston, Lucinda Nelson, and Dr Marcus Carter (Egliston et al.), 1-2.

254 Submission to the Discussion Paper: Foundation for Alcohol Research and Education, 6.

255 Submissions to the Discussion Paper: Privacy 108, 7; UNSW Allens Hub, Deakin CSRI and IEEE SSIT, 14.

256 OAIC, ‘Biometric scanning’ (Web Page); 7-Eleven Determination; Clearview Determination.

257 OAIC, APP Guidelines (July 2019) [B.30].

258 For a list of types of biometrics, see Biometrics Institute, ‘Types of Biometrics’ (Web Page, 2022).

259 Submissions to the Discussion Paper: Calabash Solutions, 4; ResMed, 3.

260 Submissions to the Discussion Paper: Salinger Privacy, 27; UNSW Allens Hub, Deakin CSRI and IEEE SSIT, 14; The Australia Institute – Centre for Responsible Technology, 13.

261 Submission to the Discussion Paper: UNSW Allens Hub, Deakin CSRI and IEEE SSIT, 14;

262 AHRC, *Human Rights and Technology* (Final Report, March 2021), rec 19, 116.

263 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 62.

Genetic and genomic information

Currently, genetic but not genomic information is included in the definition of sensitive information. Genetics is the study of how genes work and transmit information from parents to offspring. Genomics is the study and mapping of genomes, the full set of genetic instructions for an organism.

The Pharmaceutical Society of Australia noted that further clarity on the coverage of genomic information would be useful as the ability to develop personally-targeted medicines develops.²⁶⁴ Privacy 108 supported explicitly covering genomic information as a type of sensitive information.²⁶⁵

Australian Genomics and the Murdoch Children's Research Institute noted that they already treat genomic information of the deceased as covered by the Act.²⁶⁶ Some genetic and genomic information is also captured as health information.²⁶⁷ The Australian Government Social Services Portfolio noted that the scope of genetic information is already outlined by the APP Guidelines, but they would welcome further guidance on this topic.²⁶⁸

An amendment to add genomic information within the definition of sensitive information is recommended.

Consequential amendments

Salinger Privacy, the Australian Privacy Foundation and Digital Rights Watch highlighted that if changes to the definition of personal information are made to replace the word, 'about' with 'relates to', then this should be reflected in any updated definition of sensitive information.²⁶⁹ This change should also carry through in respect of the definition 'health information'.²⁷⁰

4.8 Potential new categories of sensitive information

The Discussion Paper also sought feedback on whether new types of information should be added to the current list of sensitive information. Some submitters suggested designating device fingerprints,²⁷¹ psychometric information,²⁷² or access credentials as sensitive information.²⁷³ However, these were not widely-held views and lack widespread international precedent.²⁷⁴ Others cautioned generally that any expansion of the definition may carry risk and should be done with care, including the OAIC.²⁷⁵

The Discussion Paper also queried whether financial information, particularly transaction data should be considered sensitive information given the potential for sensitive inferences to be drawn from such data. However, many submitters pointed out that financial information is already regulated and thought that further regulation through the Act may conflict with the needs of other sectors.²⁷⁶

4.8.1 Proxies for existing categories of sensitive information

Several submissions supported extending the definition of sensitive information to expressly include information that can act as a proxy for sensitive information. This was considered important because proxies can facilitate discrimination, particularly through the processes of data analytics and machine learning.²⁷⁷ Civic Data gave an example of how proxies have the potential to discriminate – citing an example where commercially-available data was used to determine that a priest had visited gay bars while using Grindr, a dating app.²⁷⁸

²⁶⁴ Submission to the Discussion Paper: [Pharmaceutical Society of Australia](#), 1-2.

²⁶⁵ Submission to the Discussion Paper: [Privacy 108](#), 7.

²⁶⁶ Submissions to the Discussion Paper: [Australian Genomics](#), 1-2; [Murdoch Children's Research Institute](#), 3.

²⁶⁷ See definition of 'health information' in s 6FA(d) of the Privacy Act: 'genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual'. See also Submission to the Discussion Paper: [Avant Mutual](#), 3.

²⁶⁸ Submission to the Discussion Paper: [Social Services Portfolio](#), 16. See OAIC, [APP Guidelines](#) (July 2019) [B.77], [D.26]–[D.29].

²⁶⁹ Submissions to the Discussion Paper: [Salinger Privacy](#), 16; [Digital Rights Watch](#), rec 8, 2; [Australian Privacy Foundation](#), 6.

²⁷⁰ Privacy Act s 6FA.

²⁷¹ Submission to the Discussion Paper: [Mark Nottingham](#), 3.

²⁷² Attorney-General's Department, *Academics, research centres and civil society roundtable*, 24 November 2021.

²⁷³ Submission to the Discussion Paper: [Privacy 108](#), 7.

²⁷⁴ However, see in relation to device fingerprinting in the EU and the interaction with the Cookie Directive: Article 29 Data Protection Working Party, *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting* ([14/EN WP 224](#), 25 November 2014).

²⁷⁵ Submissions to the Discussion Paper: [OAIC](#), 34; [Services Australia](#), 4; [Ramsay Health Care Australia](#), 4.

²⁷⁶ Submissions to the Discussion Paper: [ANZ](#), 12; [Equifax](#), 8-9; [National Australia Bank](#), 2; [Optus](#), 13; [Insurance Council of Australia](#), 5; [Information Technology Industry Council](#), 4-5; [Australian Retail Credit Association](#), 2, 7-8; [IGEA](#), 10.

²⁷⁷ Submissions to the Discussion Paper: [Centre for Media Transition](#), 6-7; [CPA Australia](#), 1-2; [Digital Rights Watch](#), 2; [Castan Centre](#), 7; [elevenM](#), 15-16.

²⁷⁸ Submissions to the Discussion Paper: [Civic Data](#), 4; [Castan Centre](#), 7.

The APP Guidelines state that information that clearly implies a category of sensitive information should be treated as sensitive information.²⁷⁹ Proposals 4.1 and 4.3 would make it clear that inferred information can be personal or sensitive information. Therefore, it is not considered necessary to include ‘proxies’ in the list of sensitive information. However, several submitters supported making it clearer that inferences about sensitive information are themselves sensitive information.²⁸⁰ The Office of the Victorian Information Commissioner considered that information used as proxies for sensitive information are currently being collected without knowledge or consent, contrary to community expectations.²⁸¹

Therefore, there would be benefit in clarifying that a category of sensitive information can be inferred where information that is not sensitive information is used as a proxy for the sensitive information. For example, if the information that a gay dating app has been downloaded to an individual’s phone is used to market on the basis of that individual’s sexual orientation, then the marketer has used the fact of the download as information about the individual’s sexual orientation and has therefore used sensitive information as defined in s 6 of the Act.

4.9 Sensitive Information

- (a) Amend the definition of sensitive information to include ‘genomic’ information.**
- (b) Amend the definition of sensitive information to replace the word ‘about’ with ‘relates to’ for consistency of terminology within the Act.**
- (c) Clarify that sensitive information can be inferred from information that is not sensitive information**

4.9 Recognising the sensitivity of location tracking data

In response to the discussion regarding the sensitivity of location data in the Discussion Paper, support emerged for specifying location data (particularly tracking precise geolocation) as a category of sensitive information.²⁸² Submissions used research, surveys and recent case law to illustrate public concern around the widespread collection of location data in Australia, highlighting how location data may risk revealing other sensitive information about individuals, or threaten personal safety.²⁸³ Reset Australia provided feedback to the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (‘OP Bill’) consultation on behalf of children and young people, which highlighted that children also share concerns about how their location data is handled.²⁸⁴

The ACCC DPI Report highlighted that 86 per cent of respondents to the ACCC’s consumer survey considered that monitoring of offline location and movement without consent was a misuse of personal information.²⁸⁵ Deloitte Australia in its submission noted the highly intrusive nature of location information and the significant privacy harms if misused.²⁸⁶ Following the US Supreme Court decision to overturn the 1973 *Roe v Wade* decision, privacy protection of location data in the US has received significant attention for its potential to expose individuals who have attended an abortion clinic to risks to their safety and wellbeing.²⁸⁷

²⁷⁹ OAIC, [APP Guidelines](#) (July 2019) [B.142]

²⁸⁰ Submissions to the Discussion Paper: [Deloitte Australia](#), 9-10; [CPA Australia](#), 1-2; [Optus](#), 13 – Optus argued that the inference itself, not the proxy, should be treated as ‘sensitive’.

²⁸¹ Submission to the Discussion Paper: [OVIC](#), 2.

²⁸² Submissions to the Discussion Paper: [QUT Digital Media Research Centre](#), 1-3; [elevenM](#), 15; [Privacy 108](#), 7; [Australian Privacy Foundation](#), 6; [Response 586092876](#); [Salinger Privacy](#), 15-16.

²⁸³ Submissions to the Discussion Paper: [QUT Digital Media Research Centre](#), citing: Michelle Riedlinger, Chantal Chapman and Peta Mitchell (2019) [Location Awareness and Geodata Sharing Practices of Australian Smartphone Users](#), QUT Digital Media Research Centre: ‘over half of the respondents reported negative feelings about the collection of their location data by smartphone apps’; [elevenM](#), 15 citing: OAIC, [Australian Community Attitudes to Privacy Survey 2020](#) 7: ‘half (48%) of Australians consider location information to be one of the biggest privacy risks today, and only a quarter (24%) feel that their location information is well protected by law and Regulations’.

²⁸⁴ Submission to the OP Bill Exposure Draft: [Children and Young People \[Compiled by Reset Australia\]](#) (2021), 7-12, 16, 18, 21-22, 31-33.

²⁸⁵ ACCC, [DPI Report](#) 374, 381, 384-386.

²⁸⁶ Submission to the Discussion Paper: [Deloitte Australia](#), 10.

²⁸⁷ R Chandran and D Baptista, [‘Analysis: After Roe v. Wade, healthcare data privacy fears grow worldwide’](#), *Reuters*, 13 July 2022; D Cox, [‘How overturning Roe v Wade has eroded privacy of personal data’](#), *BMJ* 2022, 378, 26 August 2022; N Grant, [‘Google Says It Will Delete Location Data When Users Visit Abortion Clinics’](#), *New York Times*, 1 July 2022. See also F Molloy, [‘Roe v Wade hits women’s digital health worldwide’](#), *Oncology Republic*, 19 October 2022.

Deloitte's Australian Privacy Index 2022 indicated that, of the individuals surveyed, more consumers than not are happy for their precise location information to be used to present distances to nearby services and similar services nearby. However, the vast majority of respondents were unhappy with sharing location data with other companies, creating a map of locations visited, linking location with other information about what apps were accessed where, learning about daily habits, and storing the data over time.²⁸⁸ Deloitte considered that, as such, there was merit in including location data in the list of sensitive information.²⁸⁹

There is merit in including precise geolocation tracking data as a special category of personal information requiring express consent for tracking and storage over time. A reform to designate precise geolocation tracking data as a new consent-dependent category of information would reflect community concerns and expectations. However, it would not be appropriate to include location data as a category of sensitive information where the basis for the risk arising from geolocation tracking data does not stem from the geolocation data per se but from what it reveals.²⁹⁰

Optus cautioned against coverage of location data or providing opt-out rights in relation to its use due to its core role in the supply of telecommunications services.²⁹¹ The Interactive Advertising Bureau (IAB) cited changing consumer sentiment to the use of location data, and noted how it can be used to provide consumers with more relevant search results.²⁹² The Interactive Games and Entertainment Association (IGEA) noted how the gaming industry uses of location information in a way that enables game functionality and poses limited risk (such as when location is used to place users on the nearest gaming server).²⁹³ Services Australia noted that coverage could increase regulatory requirements, such as information used for making payments to eligible recipients, including during emergency responses.²⁹⁴ It is not intended that these limited uses of location data would be affected by a proposal to require consent to precise geolocation tracking data.

Precise geolocation data should not normally include IP Address or address/post-code type information, but rather the technologically precise location an individual was located at (by reference to GPS or equivalent) at a particular time or when undertaking a particular activity. Limiting location data to precise geolocation tracking will limit the regulatory burden of incidental location data required for the delivery of services, for example an online cookie recording a person is in Australia where country specific services or website versions are provided.

The data should also be limited to tracking data, meaning data collected repeatedly over time to record movements or activity. This should avoid unintended regulation of a single instance of precise geolocation data collection relevant to the concurrent provision of a service for the duration required for that service. Geolocation tracking data would, however, likely include an app tracking movement throughout the day for the purposes of marketing. It would also include tracking movement for the purposes of rideshare services or health apps. Such apps would need to rely on valid, concurrent consent when using the app to authorise collection and could not store that information without consent.

While consumers are concerned about the collection of location data, it is not appropriate for this activity to be prohibited. Many individuals will appreciate the benefits of location data offering nearby services and indicating distances. The issue to address is transparency and ensuring that APP entities are not collecting a history or diary of an individual's activity without their valid, informed consent. As part of implementing this proposal, further consideration could be given to expanding location tracking data to other tracking metrics such as health data, heart rate and sleeping schedule.

4.10 Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice that requires consent.

Define 'geolocation tracking data' as personal information that shows an individual's precise geolocation, that is collected and stored by reference to the particular individual at particular places and times, and tracked over time.

²⁸⁸ Deloitte, [Deloitte Australian Privacy Index 2022](#), 17.

²⁸⁹ Submission to the Discussion Paper: [Deloitte Australia](#), 10.

²⁹⁰ Submissions to the Discussion Paper: [Helen Gregorczyk](#); [QUT Digital Media Research Centre](#), 1-2.

²⁹¹ Submission to the Discussion Paper: [Optus](#), 4-5.

²⁹² Submission to the Discussion Paper: [IAB](#), 17.

²⁹³ Submission to the Discussion Paper: [IGEA](#), 10.

²⁹⁴ Submission to the Discussion Paper: [Services Australia](#), 4.

5. Flexibility of the APPs

The Discussion Paper considered options for ensuring the Act is effective in providing enough flexibility to cater for a wide variety of entities, acts and practices, whilst being clear about the obligations under the Act. It noted there was general support for the flexibility which the existing framework provides and for the industry and technology neutral nature of the APPs. However, the Discussion Paper sought feedback on whether the APP code provisions and Emergency Declaration provisions could be improved.

5.1 Improve the ability to make APP codes

An APP code is a written code of practice about information privacy. It may apply to all personal information or to types of personal information, to certain industries or professions, or to specific activity, classes of activities or the use of certain technology. A code can provide additional specificity regarding how one or more of the APPs are to be complied with. It may also deal with other relevant matters and may impose additional requirements to those imposed by the APPs, so long as the additional requirements are not contrary to, or inconsistent with, the APPs.²⁹⁵ The provisions in the Act relating to APP codes set out steps and requirements to make and register a code. The benefit of codes is that they can provide greater clarity and specificity on particular issues when required, without increasing the overall prescriptiveness of the legislation.

Currently, the Act provides a process for making APP codes in which the IC is primarily responsible for identifying a code developer and registering codes developed by them.²⁹⁶ The term ‘APP code developer’ means an APP entity, a group of APP entities, or an association or body representing one or more APP entities.²⁹⁷ The IC is only permitted to make an APP code if a code developer has been requested to make a code by the IC and has not complied with the request or the IC has decided not to register the code which has been developed.²⁹⁸

The OAIC submitted that it is often challenging to identify a suitable APP entity or group of entities to develop an APP code.²⁹⁹ There are also circumstances where there is unlikely to be a suitable industry-based code developer – for example, where a code is required to cover an activity which covers a broad sector of the economy.³⁰⁰ Difficulties identifying a suitable APP code developer can hamper the efficient development of APP codes. The OAIC estimates that generally it would take 12-24 months to develop and register an APP code under the existing framework.³⁰¹

To facilitate the development of APP codes, it is proposed that the IC be provided with additional power to make an APP code on the direction or approval of the Attorney-General:

- where it is in the public interest for a code to be developed, and
- where there is unlikely to be an appropriate industry representative to develop the code.

Explanatory materials to the amending provisions should provide additional detail as to when the second limb would be likely to apply. In addition, through the legislative development process, further consideration could be given to whether it would be helpful to set out factors that may be relevant to the second limb. For example, the types of entities or range of activities proposed to be bound by a code and consideration of industry participants.

This proposal would enable an APP code to be made in the absence of a suitable industry code developer, and strengthen the efficacy of the code-making provisions.

Some submitters raised concerns that including a ‘public interest’ component in the new power could give the IC broad, subjective discretionary power to develop an APP Code.³⁰² However, the inclusion of the ‘public interest’ consideration is consistent with the current provisions in the Act which require consideration of the public interest by the IC when requesting a code developer to develop a code or when making an APP code after having made a request to industry.³⁰³ The relevant explanatory material for section 26G provides that in considering the public interest, the IC can consider the interests of stakeholders in an industry or activity, or the interests of certain segments of the public, as well as the public interest at large. The current proposal does not intend to modify this established approach to considering the public interest in the context of IC-developed codes. Furthermore, the IC would only be able to develop an APP code in these circumstances with approval of the Attorney-General.

²⁹⁵ Privacy Act s 26C. See also Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 3.

²⁹⁶ Privacy Act s 26E-26F

²⁹⁷ Privacy Act s 6.

²⁹⁸ Privacy Act s 26G(1).

²⁹⁹ Submission to the Discussion Paper: [OAIC](#), 44; Submission to the Issues Paper: [OAIC](#), 39.

³⁰⁰ Submission to the Discussion Paper: [OAIC](#), 44.

³⁰¹ Noting that each of the registered codes had different scopes and were developed in different circumstances.

³⁰² Submissions to the Discussion Paper: [Meta](#), 21; [IoT Alliance Australia](#), 6; [Google](#), 2.

³⁰³ Privacy Act ss 26E(2) and 26G(2).

5.1.2 Additional Safeguards

Some submitters raised concerns about the potential lack of industry involvement where an APP code was made by the IC.³⁰⁴ Some submitters proposed strengthened consultation requirements to enable industry to contribute to the development of codes by the IC.³⁰⁵

The proposed new code making power should retain and strengthen safeguards which are in the current code-making provisions. As with all APP codes, a code developed by the IC would be subject to disallowance by the Parliament. This would address concerns about the IC having excessive power to initiate and develop regulation as it would operate as a check on the IC's exercise of this power.³⁰⁶

In recognition of the importance of industry involvement and public consultation, a mandatory consultation period of at least 40 days could apply to IC-developed codes, along with powers to consult any person the IC considers appropriate. A 40-day consultation period would be longer than the consultation requirement in the existing code making provisions which require a draft code to be available to the public for at least 28 days.³⁰⁷ A longer consultation period would enable the IC to bring a draft code to the attention of specific stakeholders, as well as individuals, or representative or advocacy associations. It also reflects that industry may need more time to consider an IC-developed code than one prepared by an APP code developer.

Enabling the IC to consult others in developing the code replicates components of the existing provisions but would allow for consultation during, as opposed to only at the end of the code development process. This would allow industry to provide insights on technical or other industry-specific challenges in the development of a code. Consulting during code development may also result in time savings by enabling issues identified by stakeholders to be resolved prior to the period for consultation on a completed draft code.

Enhanced consultation provisions for IC-developed codes would allow meaningful consultation with industry, the community, individuals affected by the code and other relevant bodies – including other regulators where the matters to be regulated under a code are also regulated under other frameworks. These safeguards would help to ensure an IC-developed code is fit for purpose and capable of being implemented.

5.1 Amend the Act to give power to the Information Commissioner to make an APP code where the AttorneyGeneral has directed or approved that a code should be made:

- **where it is in the public interest for a code to be developed, and**
- **where there is unlikely to be an appropriate industry representative to develop the code.**

In developing an APP code, the Information Commissioner would:

- **be required to make the APP Code available for public consultation for at least 40 days,**
- **be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.**

304 Submissions to the Discussion Paper: [Optus](#), 13; [Meta](#), 21; [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 5; [IoT Alliance Australia](#), 6.

305 Submissions to the Discussion Paper: [Amazon Web Services](#), 2; [Electrical Trade Unions of Australia](#), 4.

306 Submissions to the Discussion Paper: [Meta](#), 21; [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 5.

307 Privacy Act s 26F(2).

5.2 Temporary APP codes

The existing process to develop a code can be lengthy. This includes finding a suitable code developer, developing the code within a minimum 120day period, making the draft code available for public consultation for a minimum 28day period, assessing and consulting about code registration, registering the code by tabling it as a legislative instrument in parliament and resolving any disallowance motions. The OAIC submitted that the current code making process does not allow for an APP code to be developed as a matter of urgency– such as, in the context of the COVID-19 pandemic, to instruct entities on how to comply with APPs while collecting contract-tracing information.³⁰⁸ The OAIC proposed that the IC be given a power to issue a temporary APP code, without following all the regular code-making procedures, including consultation, if it is urgently required and where it is in the public interest to do so.

Submitters were generally supportive of a temporary code-making power. However some proposed additional measures, such as time limits,³⁰⁹ industry consultation,³¹⁰ community participation³¹¹ and guidance on what constitutes ‘urgently required’³¹² as safeguards against government overreach.

An IC-developed code as per Proposal 5.1 may be able to be developed more quickly than an industry-developed code. However, the proposed increased mandatory consultation period of 40 days would reduce the capacity for IC-developed codes to be developed urgently.

The *Privacy Act 2020* (NZ) (NZ Privacy Act) allows the New Zealand Privacy Commissioner to issue a privacy ‘Code of practice’ without complying with consultation requirements of inviting and considering submissions on a publicly released draft code.³¹³ This power has been used once, to facilitate information sharing in the context of the Christchurch earthquake in 2011. Specifically, the *Christchurch Earthquake (Information Sharing) Code 2011 (Temporary)*, which remained in effect until 30 June 2011, relaxed legal restrictions on the collection, use and disclosure of personal information by expressly providing authority for certain additional permitted purposes so that those dealing with the emergency could share personal information to assist victims and their families.³¹⁴ The Code notes the operative clauses are based on sections 80H and 80P of Part VIA of the Australian Privacy Act – which provides for emergency declarations.

In March 2013, the New Zealand Privacy Commissioner issued the Civil Defence National Emergencies (Information Sharing) Code 2013³¹⁵ to facilitate information sharing during emergencies. The code was developed under the permanent code making power.³¹⁶ However, it operates on a temporary basis after a state of national emergency has been declared under the *Civil Defence Emergency Management Act 2002* (NZ), until 20 working days after the state of national emergency expires or is terminated.³¹⁷ It therefore appears to serve a similar purpose to the Christchurch Earthquake Information Sharing Code and is akin to a Privacy Emergency Declaration in the Australian context.

These examples demonstrate a distinction between the New Zealand Code of Practice and Australian APP Code frameworks. While the New Zealand framework allows for Codes to prescribe less stringent standards,³¹⁸ the Australian APP Codes are intended to set out how to apply or comply with APPs³¹⁹ and may impose additional requirements, but do not allow for entities to derogate from privacy obligations. Despite these differences, the New Zealand example provides useful guidance for a temporary APP code making power in the Australian context.

It is proposed that the IC should have power to develop a temporary urgent code to enable an APP code to be made more quickly to respond to an urgent situation such as during a pandemic. The Act or explanatory materials to the amendment could provide examples of the types of scenarios which may warrant exercise of the power. A temporary code could be developed in less time than the current 120 days,³²⁰ and without the need to make it available for public consultation for at least 28 days.³²¹ Such a code should be time limited, for a period no longer than 12 months, which would be consistent with a Temporary Public Interest Determination.³²²

308 Submission to the Discussion Paper: [OAIC](#), 44

309 Submission to the Discussion Paper: [NSW Council for Civil Liberties](#), 12.

310 Submission to the Discussion Paper: [Meta](#), 22.

311 Submission to the Discussion Paper: [Australian Communications Consumer Action Network](#), 7.

312 Submission to the Discussion Paper: [Calabash Solutions](#), 4.

313 *Privacy Act 2020* (NZ), ss 33-34.

314 Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) (NZ).

315 Repealed and replaced in October 2020 with the Civil Defence National Emergencies (Information Sharing) Code 2020 as part of a wider project to align Codes of Practice under the *Privacy Act 1993* (NZ) with the *NZ Privacy Act*.

316 *Privacy Act 2020* (NZ) s 32.

317 Civil Defence National Emergencies (Information Sharing) Code 2020 cl 3.

318 *Privacy Act 2020* (NZ) subparagraph 32(2)(a)(i).

319 Privacy Act s 26C.

320 Ibid s 26E(4).

321 Ibid s 26E(7).

322 Ibid s 80A(3).

The IC would be required to publish a temporary code and ensure that those affected by the code are aware of it. However, temporary codes would not be legislative instruments subject to disallowance, as it would not be feasible to complete all relevant parliamentary processes in truncated time periods.

If it was proposed to extend a temporary code beyond the maximum 12-month period, it should be subject to all the requirements of the non-temporary code-making provisions, including that it be tabled in the Parliament and subject to disallowance.

5.2 Amend the Act to enable the Information Commissioner to issue a temporary APP code for a maximum 12 month period 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.

5.3 Emergency Declarations

The Emergency Declaration (ED) provisions in Part VIA of the Act are intended to enhance information exchange between government agencies, private sector organisations, non-government organisations and others, in an emergency or disaster situation.³²³ Noting that only a few EDs have been made since the provisions were introduced, the Discussion Paper sought feedback on how the provisions could be made more effective.

Currently, the Prime Minister or Attorney-General may make an ED which allows for wide sharing of personal information provided it relates to the declared emergency or disaster.³²⁴ Once an ED is made, it applies to all organisations and agencies covered by the Act. Specifically, it enables an entity to share personal information about an individual if the entity believes the individual may be involved in the relevant emergency or disaster, the handling of personal information is for a permitted purpose and the disclosure is to a specified type of entity. An entity which handles personal information in accordance with the ED provisions will not be in breach of the APPs or most secrecy provisions in other legislation.³²⁵ While this enables entities to share personal information as required to help individuals, provide services and otherwise respond to an emergency or disaster, it raises concerns about potential privacy risks when an ED is in force.

When deciding whether or not to make an ED, the Prime Minister or Attorney-General must consider whether the need to effectively respond to the emergency outweighs the need for the privacy protections that would ordinarily apply. In its submission to the Issues Paper, the Department of Health noted Commonwealth agencies have expressed concern that the ED provisions do not allow EDs to selectively authorise specific information sharing acts or practices of particular types of entities³²⁶.

To enhance the capacity for EDs to assist in disaster and emergency situations, EDs should be able to be targeted by entity, personal information types or by specified acts and practices. This would allow for a narrower scope of information sharing under EDs where appropriate, enabling agencies and organisations to strike a better balance between sharing personal information in order to respond to an emergency, and protecting individuals' privacy. This would be similar to the Code of Practice provisions in the NZ Privacy Act which enable a code to be targeted to information, agencies, activities, industries, professions, callings, or classes thereof.³²⁷

The security and destruction obligations under the Act would continue to apply to entities in relation to information received under an ED. This includes requirements to destroy or de-identify information when it is no longer required, such as when the ED is no longer in effect. This would be consistent with recent amendments to the *Privacy and Personal Information Protection Act 1998* (NSW) which enable NSW government agencies to collect, use or disclose personal information and/or health information if it is reasonably necessary to assist in an emergency under the *State Emergency and Rescue Management Act 1989* (NSW). Those provisions stipulate that agencies may not hold the information for longer than 18 months unless extenuating circumstances exist.³²⁸

323 Explanatory Memorandum, Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006 (Cth) 1

324 Privacy Act ss 80J or 80K.

325 Ibid ss 80P(2) and (4).

326 Submission to the Issues Paper: [Australian Department of Health](#), 9.

327 Privacy Act 2020 (NZ) s 32(3).

328 Submission to the Discussion Paper: [Information and Privacy Commission NSW](#), 3

5.3 Amend the Act to enable 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.**

5.3.1 Ongoing emergency situations

The ED framework was inserted into the Act following the 2004 Indian Ocean tsunami. Accordingly, the provisions are framed in such a way as to contemplate relief efforts in the aftermath period of disasters with an immediate impact in the short-term such as natural disasters, rather than a longer-term emergency such as a pandemic. The Social Services Portfolio submission highlighted that the wording of the ED provisions, which include in the definition of 'permitted purpose' identifying individuals who 'are or may be injured, missing or dead as a result of the emergency or disaster', appear to limit the scope of EDs to sharing information relating to individuals already impacted by the disaster.³²⁹ A pandemic involves providing services to individuals at risk of being impacted, but may not be directly impacted yet. Given the importance of swift government assistance to individuals during events such as the COVID-19 pandemic, there is benefit in ensuring the ED framework is available in the circumstance of an ongoing emergency, such as declared pandemics.

5.4 Ensure the Emergency Declarations are able to be made in relation to ongoing emergencies.

5.3.2 Disclosure by organisations to state and territory authorities

An ED permits an agency to disclose personal information to a state or territory authority. However, an organisation may only disclose information to a Commonwealth agency. Submitters have noted that permitting organisations to also disclose information to state and territory authorities would better facilitate the response to an emergency or disaster,³³⁰ particularly where state and territory authorities are often responsible for providing or coordinating services for individuals.

For this reason, it is proposed that the Act be amended to permit organisations to disclose personal information to state and territory authorities when an ED is in force. As state and territory authorities are not subject to the Act, information disclosed to them by organisations would not be subject to protections of the Act. To address risks resulting from this, the provisions should only permit organisations to disclose information to authorities in states or territories with comparable privacy laws to the Commonwealth. An individual would be able to make a complaint to the relevant state or territory privacy commissioner in respect of privacy breaches under the relevant state or territory privacy law.

The state and territory authority receiving personal information under an ED would be bound by their obligations under state and territory privacy laws and the information received under an ED should not be used for any purpose other than a permitted purpose under the Act. This would clarify that state or territory authorities could not, for instance, use any personal information received under an ED for the purpose of prosecutions or law enforcement.

5.5 Amend the Act to permit organisations to disclose personal information to state and territory authorities under an Emergency Declaration, provided the state or territory has enacted comparable privacy laws to the Commonwealth.

³²⁹ Privacy Act s 80H(2)(a)(i)

³³⁰ Submissions to the Discussion Paper: [Department of Health \(Cth\)](#), 5; [Insurance Council of Australia](#), 7; [Department of Health Western Australia](#), 6.

6. Small business exemption

Subject to a number of exceptions, the Act does not apply to businesses with an annual turnover of \$3 million or less. 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. The Discussion Paper canvassed options to address this increased privacy risk, but did not put forward any specific proposals. There was a high level of interest in the exemption from submitters who generally took the view that advances in technology have shifted the way small businesses operate and increased the privacy risks they pose.³³¹ The majority of submitters that addressed the small business exemption recommended the exemption should be removed.³³² Some small business representatives acknowledged the importance of small businesses protecting individuals' privacy but were opposed to the exemption being removed.³³³

6.1 Businesses covered by the exemption

When the Act was extended to the private sector in 2000, the small business exemption was introduced in recognition of the potentially unreasonable compliance costs for small businesses, which were considered to pose little or no risk to the privacy of individuals.³³⁴ It was considered that compliance costs would be greater in relative terms for small businesses and that this cost was not justified in light of their low privacy risk.³³⁵ At the time, it was considered that some small businesses, or acts and practices of small businesses that posed a higher risk to privacy should be covered by the Act through an exception to the exemption.³³⁶

The Act prescribes a number of small businesses as being outside the scope of the exemption. A small business can also be brought into the scope of the Act if it is prescribed through regulation.³³⁷ The regulation-making power allows small businesses by name or type, or which engage in certain practices to be brought within the scope of the Act if the Attorney-General is satisfied that it is in the public interest to do so.³³⁸ Small businesses can also voluntarily opt-in to the Act.³³⁹

The exemption does not apply to a business that:³⁴⁰

- is a health service provider³⁴¹
- trades in personal information³⁴²
- provides services under a Commonwealth contract
- is a credit reporting body
- operates a residential tenancy database³⁴³

331 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; [Privacy 108](#), 4; [Queensland Council for Civil Liberties](#), 4; [Shogun Cybersecurity](#), 2.

332 Submissions to the Issues Paper: [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; [Privacy 108](#), 4; [Queensland Council for Civil Liberties](#), 4; [Shogun Cybersecurity](#), 2; [Professor Kimberlee Weatherill](#), 4; [Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia](#), 12; [Centre for Cyber Security Research and Innovation – Deakin University](#), 6; [Office of the Information Commissioner Queensland](#), 2; [Reset Australia](#), 4; [Shaun Chung and Rohan Shukla](#), 12; [Dr Kate Mathews Hunt](#), 5; [Karen Meohas](#), 8; [Electronic Frontiers Australia](#), 4. Submissions to the Discussion Paper: [Australian Data and Insights Association](#), 4; [OAIC](#), 49; [Calabash Solutions](#), 5; [Salinger Privacy](#), 17; [Electronic Frontiers Australia](#), 7; [Privacy 108](#), 9; [Consumer Policy Research Centre](#); [Australian Information Security Association](#), 5; [Australian Communications Consumer Action Network](#), 7; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 7; [Graham Greenleaf](#), 2; [NSW Council for Civil Liberties](#), 13; [Professor John V Swinson](#), 4; [IIS Partners and Ground Up Consulting](#), 7; [Professor David Lindsay](#), 16; [Shopping Centre Council of Australia](#), 6; [FinTech Australia](#), 8; [Emin Hasic](#); [Minderoo Tech & Policy Lab, UWA Law School](#), 8.

333 Attorney-General's Department, *Small Business Representatives Roundtable 1*, 30 March 2021; Attorney-General's Department, *Small Business Representatives Roundtable 2*, 4 February 2022.

334 Commonwealth, Parliamentary Debates, House of Representatives, 12 April 2000, 15749 (Daryl Williams, Attorney-General).

335 Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 36.

336 Ibid.

337 *Privacy Regulation 2013* (Cth) s 7.

338 The Regulation currently prescribes small businesses that operate a residential tenancy database and Aussie Farms Inc.

339 Privacy Act s 6EA; the OAIC maintains a [register](#) of small businesses that have opted-in to the Privacy Act. As at 2 November 2022, the register contained the names of 697 businesses.

340 Privacy Act ss 6D(b)-(f), 6E(1A)-(1D), 6D(9); *Privacy Regulation 2013* (Cth) s 7.

341 Health service is defined in s 6FB.

342 This is defined as a small business that discloses personal information about another individual to anyone else for a benefit, service or advantage.

343 OAIC [guidance](#) states that a residential tenancy database holds personal information about an individual's defaults or alleged defaults

- is a reporting entity for the purposes of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
- is an employee association registered or recognised under the *Fair Work (Registered Organisations) Act 2009*
- conducts protection action ballots
- is accredited under the Consumer Data Right system³⁴⁴
- is related to a business that is an APP entity.

As at June 2021, there were 2,288,441 Australian businesses with a turnover of \$3 million or less.³⁴⁵ It is estimated that less than 5 per cent of businesses actively trading in the Australian economy had an annual turnover of more than \$3 million.³⁴⁶

6.1.1 Businesses that trade in personal information

As noted above, small businesses that trade in personal information are prescribed as being outside the scope of the exemption. However, section 6D allows small businesses that trade in personal information to be exempt from the Act if they obtain the consent of individuals to collect or disclose their personal information.³⁴⁷ The view at the time the Act was extended to the private sector was that trading in personal information posed a high privacy risk, but that small businesses should not lose the benefit of the exemption if they acted with the consent of the individual concerned.³⁴⁸ Submissions that addressed this issue generally considered this consent provision should be removed.³⁴⁹ The OAIC noted that the effect of giving consent is to exempt the small business from all obligations under the Act, which unfairly places responsibility on an individual to understand the broad implications of their consent as giving up the protections of the Act in relation to their personal information, which could include sensitive information.³⁵⁰

6.2 Feedback on the small business exemption

The use of digital technology in conducting business has increased privacy risks posed by small, medium and large businesses. As noted in the Discussion Paper, increased risks posed by small businesses relating to personal information, even by those businesses not engaging in complex information handling, stem from the increasing prevalence of businesses receiving orders via the internet, having a web presence and using cloud computing services.³⁵¹ Submitters noted that the exemption does not reflect community expectations that Australians' privacy should be protected irrespective of the size of an entity.³⁵² Submissions also highlighted that annual turnover is not an accurate proxy for potential impact on privacy,³⁵³ or the seriousness of a potential breach.³⁵⁴ Submissions raised

on any tenancy agreements, including damage or failure to pay rent. A real estate agent may supply this information to a residential tenancy database operator, so another real estate agent can access the information when assessing a tenancy application.

- 344 In some circumstances, the APPs are replaced with privacy safeguards in the *Competition and Consumer Act 2010* (Cth) for entities that are accredited under the Consumer Data Right system. Unaccredited small business operators who may collect and handle personal information associated with the Consumer Data Right system (including unaccredited trusted advisers, outsourced service providers and CDR representatives) are covered by the small business exemption.
- 345 Estimate prepared for the OAIC using ABS counts of Australian Businesses, including entries and exits.
- 346 Estimate prepared for the OAIC using ABS counts of Australian Businesses, including entries and exits. Note this estimate does not reflect the number of businesses required to comply with the Act as it does not include exceptions to the small business exemption.
- 347 Privacy Act s 6D(7).
- 348 Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 4.
- 349 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](#), 14; [Australian Privacy Foundation](#), 15; [Legal Aid Queensland](#), 6; [Department of Health Western Australia](#), 3. Submissions to the Discussion Paper: [Australian Data and Insights Association](#), 5; [OAIC](#), 52-53; [Calabash Solutions](#), 6.
- 350 Submission to the Discussion Paper: [OAIC](#), 52.
- 351 ABS Characteristics of Australian Businesses, various years. Business use of information technology (small business < 19 employees). [Discussion Paper](#), 40-41.
- 352 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; [Privacy 108](#), 4; [Queensland Council for Civil Liberties](#), 4; [Shogun Cybersecurity](#), 2. Submissions to the Discussion Paper: [Calabash Solutions](#), 5; [Salinger Privacy](#), 17; [Rob Lake](#); [Electronic Frontiers Australia](#), 7.
- 353 Submissions to the Issues Paper: [Financial Rights Legal Centre](#), [Consumer Action Law Centre and Financial Counselling Australia](#), 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. Submissions to the Discussion Paper: [Privacy 108](#), 10; [Reset Australia](#), 3; [ACCI](#), 2;
- 354 [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. Submissions to the Discussion Paper: [Privacy 108](#), 9.

particular concerns about the cyber security risks posed by small businesses, the impact of the exemption on the Consumer Data Right system and the exemption negatively impacting Australia's international trade.

The Discussion Paper sought feedback on a range of possible approaches to address the privacy risks posed by small businesses, including removing the exemption, reducing the annual turnover threshold, replacing the annual turnover threshold with an employee number threshold, requiring small businesses to comply with some but not all of the APPs, prescribing further acts and practices and encouraging small businesses to uplift their privacy standards through non-regulatory measures. The Discussion Paper explored the benefits and limitations of each of these options.

Some submitters suggested the small business exemption should be retained as compliance with the Act would be beyond the resources of many smaller businesses.³⁵⁵ ACCI and Clubs Australia noted that small businesses are struggling to recover from the impact of COVID-19. Small business representatives considered that removing the exemption would impose unjustified regulatory burden on small businesses that do not pose a significant privacy risk.³⁵⁶ ACCI suggested that removing the exemption would make small businesses less competitive.³⁵⁷

Submitters did not support options to amend the threshold, or to require small businesses to comply with some but not all of the APPs.³⁵⁸ As noted in the Discussion Paper, a reduced annual turnover threshold was not put forward as a preferred option in any submissions. Submitters also considered that using an employee number threshold to determine whether an organisation was a small business would be problematic in the privacy law context and should be avoided.³⁵⁹ The Discussion Paper noted that 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 supported by a small number of submissions to the Issues Paper, with APPs 1, 3, 4, 5, 6, 7, 8, 10, 11, 12 and 13 put forward as the APPs small businesses should be required to comply with.³⁶⁰ Other submissions noted that the APPs are interlinked and do not operate on a standalone basis and did not support applying a limited number of APPs to small business.³⁶¹ This option was not supported by any submissions to the Discussion Paper. ACCI and elevenM submitted that such an approach would increase complexity.

6.2.1 Cyber security

A number of submissions suggested small businesses are often the 'weakest link' in supply chains.³⁶² Some submitters were of the view that requiring small businesses to comply with the Act (in particular the APP 11 security requirements and the NDB scheme) could 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.³⁶³ The impact to an individual can be long lasting or permanent. The Australian Computer Society submitted that small businesses are increasingly vulnerable to data related crime.³⁶⁴ A report by the Actuaries Institute found cybercrime in Australia increased 13 per cent in the last financial year, with evidence pointing to a shift in focus of cyber attackers towards smaller firms 'as easier targets'.³⁶⁵ In 2021/22 the average cost per cybercrime report was \$39,000 for small businesses.³⁶⁶

355 Submissions to the Discussion Paper: [ACCI](#), 2; [Australian Small Business and Family Enterprise Ombudsman](#), 1; [Clubs Australia](#), 1; [Internet Association of Australia](#), 2; [Communications Alliance](#), 14; [Australian Collectors and Debt Buyers Association](#), 4; [Housing Industry Association](#), 1.

356 Attorney-General's Department, *Small Business Representatives Roundtable 1*, 30 March 2021; Attorney-General's Department, *Small Business Representatives Roundtable 2*, 4 February 2022.

357 Submission to the Discussion Paper: [ACCI](#), 3.

358 Submissions to the Discussion Paper: [ACCI](#), 4; [Calabash Solutions](#), 5; [Consumer Policy Research Centre](#), 2-3.

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

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

361 Submission to the Issues Paper: [Queensland University of Technology Faculty of Law](#), 16. Submissions to the Discussion Paper: [ACCI](#), 4; [Calabash Solutions](#), 5; [elevenM](#), 19.

362 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. Submissions to the Discussion Paper: [Australian Information Security Association](#), 6.

363 Submissions to the Issues Paper: [Dr Kate Mathews Hunt](#), 6; [IDCARE](#), 3.

364 Submission to the Discussion Paper: [Australian Computer Society](#), 3.

365 Actuaries Institute, *Cyber Risks and the Role of Insurance* (Report, September 2022) 14.

366 Australian Cyber Security Centre, *Annual Cyber Threat Report July 2021 to June 2022* (Report, November 2022) 24. Note this figure is not limited to cyber incidents where personal information is exposed.

Recent high-profile data breaches have focused attention on the potential impacts of a cyber security incident, particularly when identity documents are accessed. Small businesses not covered by the Act do not have an obligation to keep personal information secure or to notify affected individuals if the business experiences a data breach that exposes personal information. IDCARE submitted that 'the risk of exploitation persisting and remaining untreated for impacted persons will be contingent on the person being notified of such risks'.³⁶⁷ Without such knowledge, an individual impacted by a data breach remains exposed.³⁶⁸

For example, real estate agents routinely collect identity documents, employment history and financial information from prospective tenants. Individuals are often required to provide multiple documents to verify their identity as part of rental applications. While this information is often collected through platforms that are covered by the Act, there is no obligation on small business real estate agencies that collect and hold this personal information to keep it secure or to notify individuals of a data breach. As noted above, there is an exception to the small business exemption for small businesses that operate a residential tenancy database. These databases hold personal information about individuals who have defaulted or are alleged to have defaulted on tenancy agreements. A real estate agent may supply this information to a residential tenancy database operator so that another real estate agent can access the information when assessing a tenancy application. Unless a real estate agent is the operator of a residential tenancy database, there is no obligation for real estate agents with an annual turnover of \$3 million or less to comply with the Act in relation to their broader personal information handling activities.

6.2.2 Consumer Data Right

Recent amendments to the CDR rules enable consumers to consent to the disclosure of their data to 'trusted advisers' who are not required to obtain CDR accreditation. Trusted advisers are classes of professionals who already receive personal information to conduct their services, including accountants, lawyers, registered tax agents, Business Activity Statement agents, financial advisers, financial counselling agencies and mortgage brokers.³⁶⁹ Although the rationale for permitting CDR data to be disclosed to small business 'trusted advisers' outside the Act's coverage was that these industries already receive personal information and are generally bound by professional standards³⁷⁰, submitters noted that trusted advisers that fall under the small business exemption may not be expected to meet the same standards as other entities that handle CDR data.³⁷¹ The lack of maturity or understanding of data handling practices by some unaccredited small businesses could increase the risk of a data breach occurring and this could undermine confidence in the CDR system.

Submitters noted that trusted advisers may not be subject to specific information security requirements and suggested that trusted advisers covered by the small business exemption could be the 'weakest link' in the chain of transfers of CDR data.³⁷² The Consumer Policy Research Centre suggested this presented an opportunity for bad actors to exploit this loophole and that the onus would be on consumers to understand the size of the business to understand what level of privacy protection would apply to their data.³⁷³ Submitters that addressed this issue suggested the small business exemption could undermine the success of the CDR scheme.³⁷⁴ Outside of initiatives such as the CDR scheme, individuals are able to directly provide their personal information to professionals that fall under the category of 'trusted advisers'.

367 Submission to the Issues Paper: [IDCARE](#), 3.

368 Ibid.

369 Trusted advisers must belong to one of the specified professions listed in CDR Rule 1.10C(2) and include:

- qualified accountants within the meaning of the *Corporations Act 2001*
- people admitted to the legal profession that hold a current practising certificate
- registered tax agents, Business Activity Statement agents and tax (financial) advisers within the meaning of the *Tax Agent Services Act 2009*
- financial counselling agencies within the meaning of the ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792
- financial advisers that are relevant providers under the *Corporations Act 2001*, other than provisional and limited-service time-share advisers
- mortgage brokers within the meaning of the *National Consumer Credit Protection Act 2009*

370 Exposure Draft Explanatory Materials, *Competition and Consumer (Consumer Data Right) Amendment (2021 Measures No. 1) Rules 2021* (Cth) 15.

371 Submissions to the Discussion Paper: [Consumer Policy Research Centre](#), 2-3; [Australian Communications Consumer Action Network](#), 8; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 6.

372 Submissions to the Discussion Paper: [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 6.

373 Submissions to the Discussion Paper: [Consumer Policy Research Centre](#), 2-3.

374 Submissions to the Discussion Paper: [Australian Communications Consumer Action Network](#), 8; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 6.

6.2.3 International trade

No comparable jurisdiction exempts small businesses from the general privacy law.³⁷⁵ A number of submitters expressed concern that the small business exemption is an international anomaly and could be inhibiting Australia's international trade.³⁷⁶ In particular, submitters expressed concern that the exemption is a barrier to a GDPR 'adequacy decision' (discussed further in Chapter 23) and that failure to remove the exemption could lead to a loss of trade and collaboration with the EU market.³⁷⁷ A GDPR adequacy decision is recognition by the EU that data protection laws in a non-EU country provide 'adequate' protection of personal information when compared with the protection provided under GDPR. Not having an adequacy decision means Australian businesses must rely on another transfer mechanism, such as contractual provisions that protect personal information received in the course of international trade to an 'adequate' level. GDPR adequacy would be beneficial for some small and medium sized businesses as it would remove the requirement for contractual clauses, which are likely to be a significant and costly administrative burden for smaller entities. Submitters also pointed out that an adequacy decision could facilitate international trade more broadly, including with other non-EU jurisdictions that have adequacy decisions.³⁷⁸

6.3 Removing the small business exemption

A large number of submitters suggested that all businesses, regardless of size should be covered by the Act.³⁷⁹ Submitters suggested it was important for privacy protections to keep in step with community expectations and other similar jurisdictions³⁸⁰ and that the exemption may no longer be acceptable to the community when considered in the context of technology proliferation and the increased use of personal information for online sales and marketing, background analytics and data-related partnerships.³⁸¹ The European Commission submitted that citizens expect a high level of data protection irrespective of whether data is processed by large corporations or small businesses.³⁸² Submitters also noted that the exemption is a barrier to introducing the concepts of controllers and processors (discussed in Chapter 22) into the Act.³⁸³

The ALRC recognised in Report 108 that while privacy protection must be balanced carefully against other competing rights, it generally should take precedence over a range of other countervailing interests, such as cost and convenience. It concluded that while the cost of compliance with the Act is an important consideration, this factor

- 375 Submissions to the Discussion Paper: [Calabash Solutions](#), 5; [Salinger Privacy](#), 17; [Australian Communications Consumer Action Network](#), 8; [Graham Greenleaf](#), 2.
- 376 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](#), 12; [Professor Kimberlee Weatherill](#), 4; [Palo Alto Networks](#), 3; [The Guardian Australia](#), 5. Submissions to the Discussion Paper: [Salinger Privacy](#), 17;
- 377 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](#), 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. Submissions to the Discussion Paper: [Privacy 108](#), 11; [Graham Greenleaf](#), 2; [Interactive Games and Entertainment Association](#), 4; [Professor David Lindsay](#), 16; [Australian Institute of Company Directors](#), 7; [Salinger Privacy](#), 17; [OAIC](#), 50.
- 378 Submissions to the Issues Paper: [Blanco](#), 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.
- 379 Submissions to the Issues Paper: [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; [Privacy 108](#), 4; [Queensland Council for Civil Liberties](#), 4; [Shogun Cybersecurity](#), 2; [Professor Kimberlee Weatherill](#), 4; [Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia](#), 12; [Centre for Cyber Security Research and Innovation – Deakin University](#), 6; [Office of the Information Commissioner Queensland](#), 2; [Reset Australia](#), 4; [Shaun Chung and Rohan Shukla](#), 12; [Dr Kate Mathews Hunt](#), 5; [Karen Meohas](#), 8; [Electronic Frontiers Australia](#), 4. Submissions to the Discussion Paper: [Australian Data and Insights Association](#), 4; [OAIC](#), 49; [Calabash Solutions](#), 5; [Salinger Privacy](#), 17; [Electronic Frontiers Australia](#), 7; [Privacy 108](#), 9; [Consumer Policy Research Centre](#), 2; [Australian Information Security Association](#), 5; [Australian Communications Consumer Action Network](#), 7; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#); [Graham Greenleaf](#), 7; [NSW Council for Civil Liberties](#), 13; [Professor John V Swinson](#), 4; [IIS Partners and Ground Up Consulting](#), 7; [Professor David Lindsay](#), 16; [Shopping Centre Council of Australia](#), 6; [FinTech Australia](#), 8; [Emin Hasic](#); [Minderoo Tech & Policy Lab, UWA Law School](#), 8;
- 380 Submissions to the Discussion Paper: [Information and Privacy Commission NSW](#), 4.
- 381 Submissions to the Discussion Paper: [OAIC](#), 48–49; [Calabash Solutions](#), 5; [Electronic Frontiers Australia](#), 7; [Australian Information Security Association](#), 5; [IIS Partners and Ground Up Consulting](#), 8.
- 382 Submission to the Discussion Paper: [European Commission](#), 2;
- 383 Submissions to the Discussion Paper: [Privacy 108](#); [Business Council of Australia](#), 12;

alone does not provide a sufficient policy basis to support the small business exemption.³⁸⁴ This is because Australia has recognised that no one shall be subject to unlawful or arbitrary interference with their privacy, which should apply irrespective of the size of the entity that is collecting and using their personal information. In this way, privacy protections are similar to protections from unlawful discrimination and consumer law protections.

6.3.1 Compliance costs

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.³⁸⁵ 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.³⁸⁶ 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. For example, a hairdresser would not have the same security obligations as a bank.³⁸⁷ As noted in Chapter 5, obligations under the Act are proportionate to the potential risk to privacy.

Other submitters suggested compliance costs should not be a determining factor when considering the protection of personal information³⁸⁸ and that removing the exemption would be on par with other regulations that aim to protect consumers from the risk of harm, such as product safety mandatory standards which do not exempt small businesses from the expectation to keep consumers safe.³⁸⁹ Some submitters were of the view that compliance with the Act is a reasonable cost of doing business in the digital age,³⁹⁰ with others suggesting compliance with the Act could lead to commercial benefits for small businesses.³⁹¹

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.³⁹² The OAIC's Privacy Regulatory Action Policy lists factors to be taken into account in deciding when to 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.³⁹³

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. 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 could be provided with additional support and free tools to assist them in complying with the Act.³⁹⁴ The OAIC stated it would be well placed to support small businesses to meet their compliance obligations.³⁹⁵ 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 proved unduly burdensome for certain small businesses as a class.³⁹⁶ The European Commission submitted that limited tailored exemptions from certain obligations based on the risk of the data processing activities at stake was more appropriate than exempting businesses based solely on size.³⁹⁷ For example, the GDPR provides a limited exemption from the requirement to maintain records of processing activities for organisations with less than

384 ALRC Report 108, 1356.

385 Submissions to the Issues Paper: [Shaun Chung and Rohan Shukla](#), 12; [Data Synergies](#), 28; [Law Council of Australia](#), 13.

386 Submissions to the Issues Paper: [Institute for Cyber Investigations and Forensics, University of the Sunshine Coast](#), 2; [OAIC](#), 61; [Privacy 108](#), 5; [AGL Energy Limited](#), 2; [Financial Services Council](#), 10. Submissions to the Discussion Paper: [Salinger Privacy](#), 18; [Rob Lake](#); [Electronic Frontiers Australia](#), 7; [Privacy 108](#), 9; [OAIC](#), 51.

387 Submissions to the Discussion Paper: [Salinger Privacy](#), 18; [Rob Lake](#).

388 Submissions to the Issues Paper: [Calabash Solutions](#), 5. Submissions to the Discussion Paper: [Calabash Solutions](#), 5.

389 Submissions to the Discussion Paper: [Electronic Frontiers Australia](#), 7; [Consumer Policy Research Centre](#), 2.

390 Submissions to the Issues Paper: [Consumer Policy Research Centre](#), 4; [Data Synergies](#), 28; [Law Council of Australia](#), 13.

391 Submissions to the Issues Paper: [Salinger Privacy](#), 11; [Calabash Solutions](#), 5; [Financial Rights Legal Centre](#), [Consumer Action Law Centre and Financial Counselling Australia](#), 13; [ID Exchange](#), 9.

392 Submissions to the Issues Paper: [Gadens](#), 3; [The Guardian Australia](#), 5.

393 OAIC, [Privacy regulatory action policy](#) (May 2018) 9.

394 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.

395 Submission to the Issues Paper: [OAIC](#), 61.

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

397 Submission to the Discussion Paper: [European Commission](#), 2.

250 employees.³⁹⁸ 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'.³⁹⁹ The exemption also does not apply to the processing of sensitive information or information relating to criminal convictions and offences.

The UK Government has proposed adopting more flexible organisational accountability measures in recognition of the disproportionate regulatory burden that more prescriptive requirements place on smaller entities.⁴⁰⁰ For example, organisations will no longer be required to undertake data protection impact assessments as prescribed in the UK GDPR, but they will be required to ensure there are risk assessment tools in place for the identification, assessment and mitigation of data protection risks across the organisation.⁴⁰¹

Submitters also suggested that an appropriate transition period should apply if the exemption was to be removed to ensure small businesses are able to comply.⁴⁰² The OAIC suggested a transition period would aid with awareness of, and preparation for compliance with the Act.⁴⁰³

6.4 Prescribing 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' annual turnover.⁴⁰⁴ ACCI and Clubs Australia submitted that where activities are identified as posing high privacy risks, they should be included in the list of exceptions to the exemption and that this approach would address sectors and types of businesses where privacy law compliance may be needed without broadly imposing a compliance burden on all small businesses.⁴⁰⁵ The Discussion Paper noted that 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.

6.4.1 Acts and practices that could be prescribed

The Discussion Paper referred to the UK ICO's list of data processing operations 'likely to result in high risk'⁴⁰⁶ which could be prescribed as being outside the scope of the exemption. These included 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.

Submitters to the Discussion Paper suggested further prescriptions for businesses that:

- are trusted advisers as defined by the CDR Rules⁴⁰⁷
- use or disclose personal information for any purpose other than the primary purpose for which it was collected⁴⁰⁸
- trade in personal information⁴⁰⁹
- handle sensitive information⁴¹⁰
- hold personal information of a large number of individuals⁴¹¹
- engage in restricted or prohibited practices (as per Chapter 11 of the Discussion Paper)⁴¹²

398 GDPR art 30(5). 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.

399 GDPR art 40(5).

400 UK Department for Digital Culture, Media & Sport, [Data: a new direction – government response to consultation](#) (June 2022).

401 Ibid.

402 Submissions to the Discussion Paper: OAIC, 51; Australian Information Security Association, 5; IIS Partners and Ground Up Consulting, 8; Australian Information Industry Association, 6.

403 Submission to the Discussion Paper: OAIC, 52.

404 Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 36.

405 Submissions to the Discussion Paper: ACCI, 5; Clubs Australia, 5.

406 UK ICO, [Examples of processing 'likely to result in high risk'](#) (Web Page, May 2018).

407 Submission to the Discussion Paper: UNSW Allens Hub, Deakin CSRI and IEEE SSIT, 7.

408 Submission to the Discussion Paper: Calabash Solutions, 5.

409 Ibid.

410 Submission to the Discussion Paper: OAIC, 51; Housing Industry Association, 1.

411 Submission to the Discussion Paper: OAIC, 51.

412 Ibid.

Submissions to the Issues Paper identified using or disclosing the personal information of children under 15,⁴¹³ supplying products or services to children under 15,⁴¹⁴ handling financial or sensitive information,⁴¹⁵ buy now, pay later businesses,⁴¹⁶ offering products and services that use the Internet of Things (IoT), AI and data analytics⁴¹⁷ and IT businesses which provide services to healthcare providers as posing a high risk.⁴¹⁸

ACCI recommended that a transition period of at least two years should apply to any further prescription of exceptions to the exemption to ensure businesses had an opportunity to adjust their practices to meet privacy standards,⁴¹⁹ which could require significant investment and alterations to existing commercial arrangements.⁴²⁰

6.4.2 Challenges in prescribing additional acts and practices

Some submitters did not support prescribing further high privacy risk acts and practices⁴²¹ and suggested that creating more exceptions to the exemption would create confusion.⁴²² The Discussion Paper noted that it would be important to ensure that any new exceptions were clearly defined and not too broad. ACCI suggested that any further prescription of exceptions that are implemented too widely or without proper consideration could lead to extensive non-compliance and illegality.⁴²³

The OAIC submitted that ‘privacy risks are constantly emerging and evolving’ and, as a result, prescriptions could quickly become out of date.⁴²⁴ It noted that it may also be difficult 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 whether a business was covered by a prescription, particularly since the small business exemption is not well understood by consumers.⁴²⁵

6.5 Providing small businesses with additional support

The Discussion Paper sought feedback on support that could be provided to small businesses to assist them to adopt the privacy standards in the Act and realise the benefits of improved privacy practices. As an example, the UK ICO provides a live chat service, helpline, webinars, step by step guides and interactive tools to support compliance.⁴²⁶ The UK ICO provides a guide on how to write a privacy policy, which was designed with the needs of small businesses in mind.⁴²⁷ Small businesses can download a free privacy policy template which includes detailed guidance on how to complete the document.

The New Zealand Privacy Commissioner provides free online privacy education, including a number of e-learning courses. Basic modules take 30 minutes to complete and more advanced modules, such as the Health Information Privacy Code training take 3-4 hours to complete, but do not have to be completed in a single session. Businesses of all sizes can create a privacy policy using the privacy statement generator, which allows businesses to select options from a menu and ‘takes five minutes’.⁴²⁸

413 Submission to the Issues Paper: [Australian Council on Children and the Media](#), 3.

414 Ibid.

415 Submissions to the Issues Paper: [Law Institute of Victoria](#), 6; [Anonymous 2](#), 3.

416 Submission to the Issues Paper: [Legal Aid Queensland](#), 6.

417 Submission to the Issues Paper: [Financial Services Council](#), 10.

418 Submission to the Issues Paper: [Australian Medical Association](#), 4.

419 Submission to the Discussion Paper: [ACCI](#), 7.

420 Ibid.

421 Submissions to the Discussion Paper: [Salinger Privacy](#), 17; [Rob Lake](#); [Graham Greenleaf](#), 2.

422 Submissions to the Discussion Paper: [Salinger Privacy](#), 17; [Rob Lake](#)

423 Submission to the Discussion Paper: [ACCI](#), 6.

424 Submission to the Issues Paper: [OAIC](#), 61.

425 Submission to the Issues Paper: [OAIC](#), 60.

426 UK ICO, [SME web hub – advice for all small organisations](#) (Web Page).

427 UK ICO, [Make your own privacy notice](#) (Web Page).

428 New Zealand Office of the Privacy Commissioner, [Privacy Statement Generator](#) (Web Page).

A large number of submitters considered that small businesses should be supported through the provision of tailored resources to encourage compliance,⁴²⁹ and that the OAIC should be resourced to provide this support and handle additional complaints.⁴³⁰ In particular, submitters suggested:

- template privacy policies⁴³¹
- tailored advice and targeted education by the OAIC⁴³²
- assistance in the event of experiencing a cybersecurity incident⁴³³
- a small business hotline⁴³⁴
- a live chat service⁴³⁵
- free webinars⁴³⁶
- step-by-step guides⁴³⁷
- tax offsets commensurate to the cost of compliance,⁴³⁸ and
- government grants.⁴³⁹

Submitters recommended that resources should be adapted to different types of small businesses (e.g. sole traders, micro businesses) and should be developed and delivered in collaboration with small business and other industry representatives.⁴⁴⁰ Calabash Solutions submitted that it was important to articulate and promote the many benefits of complying with the Act, such as increased consumer trust, improved consumer confidence, better privacy protection for individuals and a reduced risk of harm where there is a data breach.⁴⁴¹ Small business representatives stressed the importance of leveraging their expertise and networks when developing and providing support and assistance to small business.⁴⁴²

A dedicated small business hub could be developed by the OAIC and could include guidance, training, tools and resources designed to meet the needs, capacity, resourcing and other unique challenges faced by small businesses. An interactive e-learning tool could be designed to guide small businesses through the APPs. The OAIC currently provides an e-learning course for Australian Government agencies on their website.⁴⁴³ The small business e-learning tool could include practical strategies, guidelines, resources and tools tailored to specific business sectors which are able to be implemented with minimal costs. A self-assessment toolkit could be used to effectively tailor these resources to the unique circumstances of a business accessing the small business hub. For example, the UK ICO provides a self-assessment toolkit to help businesses assess their compliance with the Data Protection Act. Following completion of a checklist, a report is generated that suggests practical actions the business can take to improve its data protection practices.⁴⁴⁴

These resources could complement existing industry engagement mechanisms, including through the Australian Cyber Security Centre (ACSC) and the Department of Home Affairs Cyber and Infrastructure Security Outreach network. Strengthening cyber security across small businesses is a key focus of the Cyber Security Strategy.

⁴²⁹ 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. Submissions to the Discussion Paper: [Calabash Solutions](#), 5; [Privacy 108](#), 11; [ACCI](#), 7; [Internet Association of Australia](#), 2; [Housing Industry Association](#); [Consumer Policy Research Centre](#), 3; [Australian Computer Society](#), 3; [Professor John V Swinson](#), 4; [Professor David Lindsay](#), 16; [Minderoo Tech & Policy Lab, UWA Law School](#), 8; [Australian Institute of Company Directors](#), 7; [Information and Privacy Commission NSW](#), 4; [Business Council of Australia](#), 12; [Australian Information Industry Association](#), 6; [Australia-New Zealand Chapter, Association of Professional genealogists](#), 14; [Office of the Information Commissioner Queensland](#), 2-3.

⁴³⁰ Submissions to the Discussion Paper: [Privacy 108](#), 11; [Consumer Policy Research Centre](#), 3; [Australian Information Security Association](#), 5; [IIS Partners and Ground Up Consulting](#), 8; [Australian Institute of Company Directors](#), 7.

⁴³¹ Submissions to the Discussion Paper: [Calabash Solutions](#), 5; [ACCI](#), 3; [Minderoo Tech & Policy Lab, UWA Law School](#), 8; [Australian Information Industry Association](#), 6.

⁴³² Submissions to the Discussion Paper: [ACCI](#), 3; [Australian Institute of Company Directors](#), 7; [Australia-New Zealand Chapter, Association of Professional genealogists](#), 14.

⁴³³ Submission to the Discussion Paper: [Australian Institute of Company Directors](#), 7.

⁴³⁴ Submissions to the Discussion Paper: [Calabash Solutions](#), 5; [Internet Association of Australia](#), 2.

⁴³⁵ Submission to the Discussion Paper: [Internet Association of Australia](#), 2.

⁴³⁶ Submissions to the Discussion Paper: [Calabash Solutions](#), 5.

⁴³⁷ Submissions to the Discussion Paper: [Calabash Solutions](#), 5; [Internet Association of Australia](#), 2.

⁴³⁸ Ibid.

⁴³⁹ Submission to the Discussion Paper: [Internet Association of Australia](#), 2.

⁴⁴⁰ Submissions to the Discussion Paper: [ACCI](#), 3; [Australian Information Security Association](#), 5.

⁴⁴¹ Submission to the Discussion Paper: [Calabash Solutions](#), 5-6.

⁴⁴² Attorney-General's Department small business consultation roundtable (4 February 2022).

⁴⁴³ OAIC, [e-learning: Privacy in Practice](#) (April 2020).

⁴⁴⁴ UK ICO, [Data protection self-assessment](#) (Web Page).

The Department of Home Affairs will work with industry to develop policy options to support small businesses strengthen their cyber resilience. This will build on existing support, including the ACSC's Partnership Program, which allows Australian organisations, including small businesses, to access the technical expertise and educational resources of the ACSC. Businesses also have access to the ACSC's online 'Learn Hub' cyber security training program.

⁴⁴⁵ Outreach Officers located at Joint Cyber Security Centres located in Brisbane, Sydney, Melbourne, Adelaide and Perth can also provide advice and guidance to uplift the security and resilience of small and medium sized business, and provide access to free information and resources. Small businesses are also able to report cybercrime and cyber security incidents to the 24/7 Australian Cyber Security Hotline and the ReportCyber portal. ⁴⁴⁶

6.6 Proposal

In recognition of the increasing privacy risks posed by small businesses and the benefits of improved privacy protection for Australians and the economy, the small business exemption should be removed. This would require all Australian businesses to comply with the Act, regardless of annual turnover.

Given the unique challenges faced by small businesses and the potential regulatory burden associated with complying with the Act, it is proposed that the exemption be removed only after such steps have been implemented to facilitate small business compliance. To support small businesses to comply with the Act, there would need to be a comprehensive package of assistance developed and implemented. This could include the OAIC developing tailored resources for small businesses that address the needs of different industries and business sectors. These resources should be developed with input from small business representatives and industry associations. Simplified guidance on how to comply with the Act could also be developed into a small business code under the Act to provide small businesses with certainty about their obligations under the Act.

The small business exemption should not be removed until support and resources are developed and available to small businesses. These resources should be designed to minimise the cost of complying with the Act for small businesses. At this time, it is difficult to quantify the potential compliance costs for small business, given the diversity of industries captured by the exemption and the various proposals put forward in this Report that would alter an entity's obligations under the Act. In January 2008, the ALRC engaged an external consultant to provide an independent assessment of the likely costs of compliance that would result from the removal of the small business exemption as part of its Report 108.⁴⁴⁷ It was estimated that the removal of the small business exemption would result in affected businesses incurring a start-up cost of \$225 (\$292.87 in 2021⁴⁴⁸) and ongoing annual costs of \$301 (\$391.79 in 2021⁴⁴⁹). It was considered that small businesses would incur costs associated with familiarisation with the Act, conducting privacy audits, developing privacy plans, amending business documentation, training staff, purchasing filing cabinets and shredders, handling customer complaints, record keeping, making their privacy policy available and updating and reviewing their privacy policy.

Since the ALRC estimate was prepared 14 years ago, it cannot be relied upon as an accurate indicator of the costs that small businesses would incur when complying with the Act. Following implementation of other proposals put forward in this Report and development of a support package for small business, an impact analysis should be undertaken to estimate the compliance costs for different types of small businesses. An updated impact analysis will take into account technological developments and updated obligations under the Act which have changed since the ALRC estimate. The below case studies illustrate the different impact that compliance with the Act would have for different types of small businesses, depending on the risk profile of their information handling acts and practices.

However, depending on the timeframe for removing the small business exemption, steps should be taken to prescribe the collection of biometric information for use in facial recognition technology, given the privacy and other human rights risks identified with this practice (refer to Chapter 13).

In addition, given the privacy risks identified in relation to trading in personal information (discussed in Chapter 20), the exception for small businesses that obtain consent to trade in personal information should be removed from the Act. This would ensure that any business that trades in personal information would be required to comply with the Act, including the additional requirements outlined in Chapter 20. Given the expanded scope of the Act, the OAIC will require additional resources to support entities' compliance with the Act.

⁴⁴⁵ Available at www.cyber.gov.au/learn.

⁴⁴⁶ See www.cyber.gov.au/acsc/report.

⁴⁴⁷ ALRC Report 108, 1351

⁴⁴⁸ Estimate using the Reserve Bank of Australia's [Inflation Calculator](#). Note the results produced by the Inflation Calculator are intended as guides only.

⁴⁴⁹ Estimate using the Reserve Bank of Australia's [Inflation Calculator](#). Note the results produced by the Inflation Calculator are intended as guides only.

6.1 Remove the small business exemption, but only after:

- **an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act**
- **appropriate support is developed in consultation with small business**
- **in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and**
- **small businesses are in a position to comply with these obligations.**

6.2 In the short-term:

- **prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption, and**
- **remove the exemption from the Act for small businesses that obtain consent to trade in personal information.**

Case study 1 – low risk

Judith owns a café and employs a small number of staff. Patrons do not disclose their personal information when visiting the café. The café does not have a website or a social media presence. Judith and her employees accept reservations and take away orders over the phone which involves recording a customer's first name and contact number. This information is stored in a book which is kept behind the counter.

Judith's business poses a very low risk to the privacy of her patrons as personal information is only collected in limited circumstances and this information can only be accessed by Judith and her employees. Judith could meet her obligations under the Act by downloading a privacy policy template and completing the required fields and ensuring the book containing personal information is kept secure. Judith would also need to ensure she was able to handle a complaint from a customer about misuse of their personal information (for example, if one of Judith's employee's used information in the book to contact a customer and ask them on a date).

Case study 2 – medium risk

Adam owns a pizza shop and employs a number of staff to work in the shop and to deliver pizzas. The pizza shop has a website which allows customers to place online orders for pickup or delivery. When a customer places an online order for delivery, the website collects their name, address, phone number, email address, credit card details and technical information including IP address, timestamps of the visit, web browser and operating system used by the customer. The website is hosted by a third party web-hosting company that can also access this information. Adam uses third party software which allows customers to pay for their orders online. Adam also runs a Facebook page and Instagram account for the pizza shop and uses paid advertising to target social media users within a 10km radius of the pizza shop. Adam also uses Facebook Pixel to track customers that visit the pizza shop's website so they can be targeted with Facebook and Instagram advertisements for the pizza shop. Adam and his employees also take orders over the phone – a customer's name, phone number and address are recorded on sticky notes and disposed of at the end of the day.

Adam would have the same obligations as Judith. In addition, Adam would need to make the privacy policy available on the pizza shop's website and would need to include a privacy notice on the website which outlined the information that would be collected and how it would be used. Adam would also need to ensure he had appropriate software to ensure the security of personal information his business holds. If Adam outsources all or part of his personal information handling activities, he will also need to consider what steps he needs to take to ensure the third party provider has appropriate security arrangements in place.

Case study 3 – high risk

James and Jennifer develop an App after pitching the idea for a university assignment. The App allows users to take a series of personality quizzes and connect with other users with the same 'personality type'. The App collects a user's name, date of birth, sexual orientation, political affiliation, phone number and email address when they sign up and allows users to 'match' with each other based on their photo, personality quiz results and location. The App is available for free download. James and Jennifer have compiled a database of the information collected from users, including their answers to the personality quizzes.

The App poses a significant risk to the privacy of users. A data breach of James and Jennifer's database could cause significant harm to users of the App. In order to comply with the requirements of the Act, James and Jennifer would need to provide a notice to users at the point of collecting their personal information setting out relevant information on how their personal information may be used or disclosed. They would also need to obtain users' express consent in relation to the collection, use and disclosure of their sensitive information. James and Jennifer would need a tailored privacy policy and sophisticated security software. James and Jennifer would also likely need to inform themselves fully in relation to relevant obligations when collecting, using and disclosing personal information, including compliance with the fair and reasonable test and specific restrictions in relation to certain acts or practices.

7. Employee records exemption

An organisation that is or was an employer is currently 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.⁴⁵⁰ An employee record is a record of personal information relating to the employment of the employee.⁴⁵¹

The exemption applies to acts or practices of 'organisations', which broadly covers non-public sector entities in their capacity as employers or former employers and does not extend to 'agencies' under the Act.⁴⁵² Personal information in an employee record that is used or disclosed for a purpose not directly related to the employment relationship is subject to the Act.⁴⁵³

The exemption was originally included on the basis that the 'handling of employee records is a matter better dealt with under workplace relations legislation' which, at that time, was primarily governed by state and territory legislation. However, it was recognised that personal information about employees typically held on personnel files was regarded as 'deserving of privacy protection'.⁴⁵⁴ The exemption also extends to the NDB scheme; that is, any data breach involving personal information of employees in an employee record that is likely to result in serious harm is not subject to the scheme's reporting requirements.

The Discussion Paper considered whether the personal information of private sector employees is adequately protected in light of the employee records exemption. It canvassed three possible approaches to reform:

- **removing the exemption:** noting that this would not affect most employers unless the small business exemption was also removed
- **modifying the exemption:** to allow better protection of private sector employee records (such as by applying security and destruction requirements and accountability for disclosure of information overseas) while retaining the flexibility that employers need to administer the employment relationship, or
- **enhancing protections in workplace relations legislation:** which might impact a larger number of employees if they applied to small business employers, but would result in further fragmentation of privacy protections because (a) it could result in private sector employees being covered by different privacy standards to those which apply to Commonwealth public sector employees and (b) jurisdiction for private sector employee privacy matters would likely be conferred on the Fair Work Ombudsman and Commission rather than the OAIC.

The Discussion Paper sought further feedback, including in relation to employers' current information-handling practices and the appropriateness of requiring consent to collect information in the context of the employment relationship. It also sought views on how the employee records exemption could be modified to better protect those records while retaining sufficient flexibility for employers, and on the benefits and limitations of providing enhanced privacy protections for employees in workplace relations legislation.

7.1 Employers' current information-handling practices

The Discussion Paper requested feedback on whether employers are collecting personal information beyond what is reasonably necessary for their functions or activities and whether employers' use and disclosure of employees' information is meeting community expectations.

Submitters had differing views on whether the current collection of personal information by employers is reasonably necessary. Some submitters highlighted the need to collect a wide range of information to properly administer the workplace.⁴⁵⁵ Others pointed out that the personal information currently collected was arguably not necessary.⁴⁵⁶

450 Privacy Act s 7B(3).

451 Ibid s 6.

452 The employee records exemption does not extend to acts or practices of 'agencies' under the Act which includes Commonwealth Departments and other bodies established under Commonwealth statute. These agencies are bound by the Act; Privacy Act s 7B(3).

453 'QF' & Others and Spotless Group Limited (Privacy) [2019] AICmr 20.

454 Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 4-5; Commonwealth, Parliamentary Debates, House of Representatives, 12 April 2000, 15752 (Daryl Williams, Attorney-General).

455 Submissions to the Discussion Paper: [Woolworths](#), 7; [Clubs Australia](#), 1; [Financial Services Council](#), 8; [Ai Group](#), 20.

456 Submissions to the Discussion Paper: [Peter Holland](#), 11; [Electrical Trades Union of Australia](#), 2.

ACCI submitted that employers collect and maintain employment records to comply with the law, either (a) directly as prescribed, (b) as a defence to claims of underpayment, or (c) to have legal records for litigation such as unfair dismissal or allegations of sexual harassment.⁴⁵⁷ ACCI stated that ‘no serious issues of employer over-collection of personal information have been brought to ACCI’s attention’ and that widespread misuse of information by employers is rarely demonstrated by those who object to the employee records exemption.⁴⁵⁸

Submitters raised that employers are justifiably collecting sensitive information as part of reasonable administrative action, particularly in response to the COVID-19 pandemic⁴⁵⁹ and the need for employers to comply with workplace health and safety measures to protect employees.⁴⁶⁰ Certis Security Australia noted that biometric verification enables security providers to assure the identity and work attendance of staff and submitted that this is in line with community expectations.⁴⁶¹

Submitters in favour of narrowing or removing the exemption noted that employers collect large amounts of personal, and often sensitive information.⁴⁶² The European Commission pointed out that employee records typically contain information that is particularly sensitive including health information, criminal records, performance evaluation or financial information.⁴⁶³

Submitters highlighted that the COVID pandemic had increased the importance of this issue as employers are collecting ‘additional’ sensitive information such as vaccination status, health-related information, data surveillance and travel history.⁴⁶⁴ Deloitte commented that the collection and use of sensitive information within the employment context is becoming more common, and has been heightened through the introduction of hybrid working models and organisational oversight into employee vaccination.⁴⁶⁵ Submitters also held concerns regarding the blurring of personal/private boundaries as a result of work from home arrangements and social media.⁴⁶⁶

Minderoo Tech & Policy Lab, UWA Law School indicated that the current requirement that information needed to be ‘*directly related*’ to the employment relationship is being interpreted too broadly, stating that the ‘drafters of the exemption could not have anticipated’ the breadth of its application.⁴⁶⁷ The Electrical Trades Union of Australia (ETU) and Professor Peter Holland submitted that employers are collecting employees’ sensitive information to use in new technologies where it is not clear that it is reasonable or necessary to administer the employment relationship.⁴⁶⁸ The ETU provided an example of an employer that required employees to undertake medical screening which included a blood test for the purpose of identifying a risk profile for cardiac arrest. When requesting the samples, the company required employees to sign a broad consent so that their blood samples could be disclosed to its related bodies corporate located outside Australia. The consent form stipulated that overseas recipients were not required to comply with the Privacy Act.⁴⁶⁹

Professor Holland noted the rapid development of technology enabling the increased opportunity to collect and use biometric information in the workplace. He considered that the significance of collecting such data is not understood by management or employees where biometric information ‘has capabilities of revealing private details of an individual, particulars that even they may not have knowledge of’.⁴⁷⁰ In reference to the attempted collection of Mr Lee’s fingerprint in the Fair Work Commission (FWC) Full Bench decision of *Lee v Superior Wood*⁴⁷¹, Professor Holland highlighted that the lack of transparency about employers’ purposes for collecting and intended use of employees’ biometric information is problematic as it does not allow workers to make informed decisions about whether they want to continue working in that workplace.⁴⁷²

457 Submission to the Discussion Paper: [Australian Chamber of Commerce and Industry \(ACCI\)](#), 10.

458 Ibid 9.

459 Submissions to the Discussion Paper: [Clubs Australia](#), 1; [Financial Services Council](#), 8; [Ai Group](#), 20.

460 Submissions to the Discussion Paper: [Financial Services Council](#), 8; [Woolworths](#), 7.

461 Submission to the Discussion Paper: [Certis Security Australia](#), 4.

462 Submissions to the Discussion Paper: [Digital Rights Watch](#), 19; [Law Council of Australia](#), 10; [ACTU](#), 2.

463 Submission to the Discussion Paper: [European Commission](#), 2.

464 Submissions to the Discussion Paper: [OAI](#), 54; [Salinger Privacy](#), 18; [Deloitte](#), 12; [Castan Centre](#), 10; [Australian Privacy Foundation](#), 7; [Digital Rights Watch](#), 19.

465 Submission to the Discussion Paper: [Deloitte](#), 12.

466 Submissions to the Discussion Paper: [The Benevolent Society](#), 3; [Professor John Swinson](#), 5; [Digital Rights Watch](#), 19.

467 Submission to the Discussion paper: [Minderoo Tech & Policy Lab, UWA Law School](#), 8. See also, Submission to the Issues Paper: [Minderoo Tech and Policy Lab, University of Western Australia Law School](#), 27–8.

468 Submissions to the Discussion Paper: [Peter Holland](#), 3; [Electrical Trades Union of Australia](#), 3.

469 Submission to the Discussion Paper: [Electrical Trades Union of Australia](#), 2.

470 Submission to the Discussion Paper: [Peter Holland](#), 3.

471 *Lee v Superior Wood Pty Ltd* [2019] FWC 2946.

472 Submission to the Discussion Paper: [Peter Holland](#), 7.

7.2 Consent to collect information in the employment context

In the *Lee* decision, the Full Bench of the FWC held that an employer's direction to an employee to submit to the collection of his fingerprints where the employee's consent was not obtained as required by APP 3.3 was not a lawful direction, because the employee records exemption does not apply to the solicitation of sensitive information not yet contained in an employee record.⁴⁷³ Consequently, organisations have treated APP 3, including the requirement to obtain consent to collect sensitive information, as applying to them in their capacity as employers.

Ai Group said the decision in *Lee* 'exposed a significant shortcoming in the existing exemption'.⁴⁷⁴ Clubs Australia said the application of APP 3 and subsequently the requirement to obtain consent to collect sensitive information from employees interfered with an employer's ability to issue a lawful and reasonable direction requiring information, which 'employees have an implied duty to comply with'.⁴⁷⁵ ACCI stated that 'an employee should not need to consent to the collection of information clearly essential to the existence of a contract of employment'.⁴⁷⁶

Submitters provided examples of where the requirement to obtain employees' consent to collect sensitive information could hamper employers' ability to implement important workplace policies and processes. Ai Group noted that employers had been restricted from directing employees to provide information necessary to implement COVID-19 protections in the workplace.⁴⁷⁷ Woolworths noted that requiring consent could jeopardise its ability to achieve diversity and inclusion in the workplace as this involves collecting and using employees' sensitive information such as racial and ethnic origin and health information.⁴⁷⁸

Submitters also highlighted concerns about whether valid consent is possible in the employment context. In a similar vein to the Full Bench's comment in *Lee* that any consent an employee may supply would likely be 'vitiated by the threat of termination of employment', submitters questioned whether consent in the context of the employment relationship could be freely given.⁴⁷⁹ The Business Council of Australia stated that the ability of employees to provide voluntary consent to collection of their personal information in an employment relationship is 'arguably fraught'.⁴⁸⁰ CSIRO stated that *Lee* has caused uncertainty for public sector agencies when relying on consent to collect sensitive information as it was now unclear whether an employee providing consent in circumstances where they face termination of their employment would be considered genuine.⁴⁸¹

Since the Discussion Paper was issued, the Fair Work Commission has considered the *Lee* decision in *CFMMEU v BHP Coal*,⁴⁸² which was a case concerning a request by BHP Coal for evidence of employees' COVID-19 vaccination status. Deputy President Asbury was required to determine if a site requirement by BHP Coal that workers must be vaccinated and provide evidence of vaccination to access Qld sites meant that employees had not consented to the collection of their health information as required by APP 3.3. Or, if consent was given, whether it was vitiated by coercion where non-compliance would result in discipline or termination of employment.⁴⁸³ The Applicants submitted, citing *Lee* in support, that if employees had not consented, or their consent was vitiated, the site requirement was not a lawful direction.⁴⁸⁴

Asbury DP held that the site requirement did not force employees to provide the vaccination information and it was open to employees to refuse. She distinguished *Lee* on its facts, stating that the unlawfulness of the requirement that Mr Lee submit to collection of his fingerprints stemmed from the employer's failure to provide a collection notice and non-compliance with other requirements of the Act as opposed to its failure to obtain Mr Lee's consent.⁴⁸⁵ Asbury DP further held that while disciplinary action and termination is a threat to the economic and social position of employees who do not comply with the direction, such pressure is not coercion that vitiates the consent of employees to provide sensitive information to establish vaccination status.⁴⁸⁶ In her judgment, Asbury DP also noted that the Full Bench in *Lee* was not definitive in its comments about consent being vitiated once Mr Lee was told he faced discipline or dismissal as the Full Bench's statement was that consent would 'likely have been vitiated by the threat'.⁴⁸⁷

⁴⁷³ *Lee v Superior Wood Pty Ltd* [2019] FWC 2946.

⁴⁷⁴ Submission to the Discussion Paper: [Ai Group](#), 21.

⁴⁷⁵ Submission to the Discussion Paper: [Clubs Australia](#), 3.

⁴⁷⁶ Submission to the Issues Paper: [Australian Chamber of Commerce and Industry \(ACCI\)](#), 11.

⁴⁷⁷ Submission to the Discussion Paper: [Ai Group](#), 21.

⁴⁷⁸ Submission to the Discussion Paper: [Woolworths](#), 7.

⁴⁷⁹ Submissions to the Discussion Paper: [Calabash Solutions](#); [The Benevolent Society](#); [ACTU](#); [Electrical Trades Union of Australia](#); [Australian Financial Markets Association](#); See also UK ICO, *When is consent appropriate?* (Web Page, October 2022).

⁴⁸⁰ Submission to the Discussion Paper: [Business Council of Australia](#), 11.

⁴⁸¹ Submission to the Discussion Paper: [CSIRO](#), 4.

⁴⁸² *CFMMEU & Ors v BHP Coal* [2022] FWC 81.

⁴⁸³ [2022] FWC 81, [79] and [91].

⁴⁸⁴ *Ibid* [161].

⁴⁸⁵ *Ibid* [160]–[164].

⁴⁸⁶ *Ibid* [79] and [91].

⁴⁸⁷ *Ibid* [164].

7.3 Modifying the exemption while ensuring flexibility

The Discussion Paper sought feedback on how the exemption could be modified to better protect employee privacy while retaining the flexibility needed by employers to administer the employment relationship. In particular, feedback was sought on how the fair and reasonable test and rights of access and correction might work in the employment context as well as the benefits and costs of applying security, destruction and data breach reporting obligations.

Submitters in favour of removing or narrowing the exemption said that employers should be required to demonstrate their collection of employees' personal information is 'necessary and proportionate'⁴⁸⁸ but were open to exceptions for employers' reasonable administrative action. Overall, most agreed with the need for dedicated exceptions or carveouts to permit employers to collect, use or disclose employees' personal information without consent under APPs 3 and 6.⁴⁸⁹

Minderoo Tech & Policy Lab, UWA Law School submitted that the exemption should be narrowed to apply only to the 'collection of pre-defined material, for specified purposes' and to also limit the use of that information.⁴⁹⁰ It said this would allow employers to articulate what particular kinds of information they believe is necessary to exempt from the APPs and remove the difficulty of having to determine whether the exemption applies in each instance of handling.⁴⁹¹ Privacy 108 supported specific prohibitions on the use of employee information for marketing or secondary purposes.⁴⁹² Others in support of modification were generally in favour of exceptions so that employers' need for flexibility could be assured.⁴⁹³

The OAIC noted that if the exemption was removed or narrowed, the Act's existing exceptions would facilitate information-handling within the employment relationship, such as by allowing employers to collect sensitive information and use or disclose personal information without consent in relation to unlawful activity or serious misconduct.⁴⁹⁴

Submitters in favour of retaining the exemption, either in full or substantially, indicated that various APPs would create difficulties for employers in administering the employment relationship.⁴⁹⁵ Woolworths submitted that its ability to administer sensitive matters such as complaints, disciplinary action and performance management would be negatively impacted by the application of APPs 3, 6, 12 and 13 along with pro-privacy defaults, restricted and prohibited practices and any new rights to object and erasure.⁴⁹⁶ ACCI warned that enabling access requests and other parts of the Act 'risks creating workplace problems and disputation' not currently seen in workplaces.⁴⁹⁷

Clubs Australia considered that it would be impractical for employers to comply with APPs 6, 12 and 13 and stated that 'attempting to govern the employment relationship with a one-size-fits-all law will require several new rules and exceptions, and ultimately make the APPs prescriptive and complex'.⁴⁹⁸ Others considered that modifying the exemption might cause confusion and duplication for employers who had grown familiar with operating under the workplace relations framework.⁴⁹⁹ Ai Group said 'employers should not be subject to multiple layers of regulation pertaining to the same subject matter'.⁵⁰⁰ It further cautioned that 'any watering down' of the exemption might inadvertently put employers at risk of contravening the Act due to confusion about its interaction with workplace relations laws.⁵⁰¹

488 Submissions to the Discussion Paper: [The Benevolent Society](#), 3; [Privacy 108](#), 12.

489 Submissions to the Discussion Paper: [Deloitte](#); [Minderoo Tech & Policy Lab, UWA Law School](#); [Salinger Privacy](#); [Calabash Solutions](#); [Privacy 108](#).

490 Submission to the Discussion Paper: [Minderoo Tech & Policy Lab, UWA Law School](#), 8.

491 Ibid 9. Other submitters made similar comments on the benefits of removing the exemption including providing a clearer framework for employers, who could adopt a single set of practices for handling employee record information and other personal information: [Avant Mutual](#); [OAIC](#); [Deloitte](#); [Law Council of Australia](#); [Privacy 108](#); [Minderoo Tech & Policy Lab, UWA Law School](#).

492 Submission to the Discussion Paper: [Privacy 108](#).

493 Submissions to the Discussion Paper: [Australian Banking Association](#), 12; [Australian Data and Insights Association \(ADIA\)](#), 6; [Financial Services Council](#), 8.

494 Submission to the Discussion Paper: [OAIC](#), 56.

495 Submissions to the Discussion Paper: [Ramsay Health Care Australia](#); [Optus](#); [BSA | The Software Alliance](#); [Australian Collectors & Debt Buyers Association](#); [Business Council of Australia](#); [Australian Chamber of Commerce and Industry \(ACCI\)](#).

496 Submission to the Discussion Paper: [Woolworths](#), 7.

497 Submission to the Discussion Paper: [Australian Chamber of Commerce and Industry \(ACCI\)](#), 10.

498 Submission to the Discussion Paper: [Clubs Australia](#), 1.

499 See for example Submissions to the Discussion Paper: [Australian Chamber of Commerce and Industry \(ACCI\)](#), 15; [Ai Group](#), 20; [Communications Alliance](#), 21; [Business Council of Australia](#), 11.

500 Submission to the Discussion Paper: [Ai Group](#), 20.

501 Ibid 20.

A number of submitters supported modifying the exemption to cover solicitation of information.⁵⁰² The AI Group submitted that the exemption should be extended to host employers in their engagement of labour hire workers.⁵⁰³

7.3.1 Fair and reasonable collection, use and disclosure

Some submitters supported the application of the test as a suitable safeguard in the workplace context.⁵⁰⁴ Deloitte said the test could act as the minimum standard for employers' handling of personal information, regardless of whether consent was obtained.⁵⁰⁵ The OAIC considered a requirement for collection, use and disclosure to be fair and reasonable would provide 'additional checks and balances on employers' handling of personal information in a context where individuals are likely to have limited control over information handling practices', including by addressing concerns about excessive workplace surveillance.⁵⁰⁶ Certis Security Australia considered that the test could provide employees with additional protection in light of concern about employees being vulnerable to excessive, unreasonable or coercive collection of their personal or sensitive information.⁵⁰⁷

However, ACCI considered that the concept of fairness 'would prove extremely problematic in the employment sphere' due to the 'uncertainty and developing nature of its meaning'.⁵⁰⁸ It noted that certain actions, such as collecting information to address poor performance may be at odds with an individual employee's interests.⁵⁰⁹

7.3.2 Security and NDB reporting

Many submitters thought that the Act's security requirements in APP 11 and obligations under the NDB scheme should apply to the workplace context to ensure employees are made aware of data breaches and provided adequate remedies and enforcement.⁵¹⁰ Submitters considered that the sensitivity, volume and variety of information about employees held by employers put them at significant risk of harm if the information were used or disclosed inappropriately⁵¹¹ making it 'crucial' that security measures be put in place and employees informed of data breaches.⁵¹² Calabash Solutions said it would improve employee trust and confidence in employers' handling of employee information, reduce risk of harms to employees associated with data breaches and result in better interoperability with other legislation.⁵¹³

Relevant costs would include compliance costs to employers and costs associated with enforcement by the IC.⁵¹⁴ The WA Department of Health considered that costs to employers would be minimal given that employee information is typically held in digital form, and noted that employers would benefit from reduced risk of reputational harm as a result of high-profile data breaches.⁵¹⁵

The OAIC said that employees would benefit from being able to protect themselves from harms associated with data breaches and noted that private sector employers are already required to report data breaches involving employees' personal information in some circumstances, such as for breaches involving tax file number information.⁵¹⁶ The OAIC also referred to a recent survey that revealed businesses are concerned about the potential for a cyber-attack on sensitive information they hold, including employee information.⁵¹⁷

502 Submissions to the Discussion Paper: [Woolworths](#), 7, [Clubs Australia](#), 3, [Australian Chamber of Commerce and Industry \(ACCI\)](#), 12, [Ai Group](#), 21

503 Submission to the Discussion Paper: [AI Group](#), 20-21.

504 Submission to the Discussion Paper: [Calabash Solutions](#), 7.

505 Submission to the Discussion Paper: [Deloitte](#), 12.

506 Submission to the Discussion Paper: [OAIC](#), 56.

507 Submission to the Discussion Paper: [Certis Security Australia](#), 6.

508 Submission to the Discussion Paper: [Australian Chamber of Commerce and Industry \(ACCI\)](#), 12.

509 Ibid 13.

510 Submissions to the Discussion Paper: [Calabash Solutions](#); [Digital Rights Watch](#); [Office of the Victorian Information Commissioner](#), [Australian Data and Insights Association \(ADIA\)](#); [European Commission](#) [re sensitive information]; [Law Council of Australia](#) [re sensitive information]; [elevenM](#); [Peter Holland](#); [Electrical Trades Union of Australia](#); [Deloitte](#).

511 Submission to the Discussion Paper: [Office of the Victorian Information Commissioner](#).

512 Submission to the Discussion Paper: [European Commission](#), 2.

513 Submission to the Discussion Paper: [Calabash Solutions](#), 8.

514 Submission to the Discussion Paper: Ibid.

515 Submission to the Discussion Paper: [Department of Health - Western Australia](#), 4.

516 Submission to the Discussion Paper: [OAIC](#), 55. See also [Privcore](#), 5.

517 Submission to the Discussion Paper: [OAIC](#), 55 citing Varonis, [Australian cybersecurity risk report: understanding Australian business and their approach and attitudes towards cybersecurity](#) (Report, October 2021) 10.

Some submitters in favour of retaining the exemption argued that employers already have measures in place to protect and secure employees' personal information.⁵¹⁸ ACCI said there was no evidence to suggest data breaches were a widespread issue, but, in any case, any application of security obligations and data breach notification should occur within the context of workplace relations laws.

7.3.3 Access and correction of personal information

Submitters in favour of retaining the exemption were particularly concerned about difficulties employers would face in administering the employment relationship if they were required to respond to requests for access or correction under APPs 12 and 13.⁵¹⁹ Some submitters thought such rights could discourage referees from giving a full and frank reference,⁵²⁰ and employers from conducting investigations or managing employee performance.⁵²¹

Several submitters in favour of removing or narrowing the exemption supported exceptions from APPs 12 and 13 to address concerns about employers maintaining confidentiality in regard to references and to safeguard employers' ability to conduct disciplinary, performance management and fitness for duty processes.⁵²² NAB qualified its support for the removal of the exemption on the basis that the application of APP 12 would likely cause the biggest impact on employers and should therefore be given further consideration. It suggested either amendments to the existing exceptions or 'the introduction of targeted grounds for validly and fairly denying' employees' access requests, including the 'ability for employers to deny ambit, unreasonably broad or otherwise bad faith access requests' (unless appropriately refined).⁵²³

Other submitters disagreed with the need to introduce employer-specific exceptions.⁵²⁴ Calabash Solutions said employees' ability to seek access to and correction of their personal information should not be sacrificed in exchange for matters already excepted from APPs 12 and 13.⁵²⁵ Some submitters said there was no justification to introduce exceptions to APP 12 if the intention was to limit an employee's ability to verify the accuracy of information held about them⁵²⁶ and noted that individuals should be able to be provided access to their records and correct any personal data that is inaccurate.⁵²⁷

7.4 Improving privacy protection in workplace relations legislation

In response to a question about the benefits and limitations of providing enhanced protections for employees' privacy in workplace relations legislation, a number of submitters opposed to removing the exemption maintained that existing workplace relations laws effectively protect employee records.⁵²⁸ However, ACCI and Ai Group submitted that if any changes were made to private sector employees' privacy protections, it should take place through workplace relations laws as 'any productive debate concerning the privacy obligations in place to protect employee records need to take place within the confines of workplace relations legislation which comprehensively deals with this area'⁵²⁹ and it is in the workplace relations 'sphere that expert trade unions and employers representatives engage with government to inform the best possible policy'.⁵³⁰

The OAIC considered the Privacy Act was a more appropriate regulatory framework for addressing employee privacy because 'the primary concern of workplace relations laws in setting record keeping obligations is to ensure that employees receive the correct wages and entitlements [which is] a different policy focus and objective to the Privacy Act'.⁵³¹ The Discussion Paper outlined the current obligations contained in workplace relations laws on employers to keep basic employee records for 7 years including on matters such as leave, income and hours of work.⁵³²

518 Submission to the Discussion Paper: [Clubs Australia](#), 2.

519 Submissions to the Discussion Paper: [Clubs Australia](#); [Australian Chamber of Commerce and Industry \(ACCI\)](#).

520 Although it is noted that references for candidates who do not become employees are not covered by the exemption currently.

521 Submission to the Discussion Paper: [Ramsay Health Care Australia](#), 4 – 5.

522 Submissions to the Discussion Paper: [Privacy 108](#); [Salinger Privacy](#); [OAIC](#); [Deloitte](#); [elevenM](#); [Castan Centre](#); [Law Council of Australia](#); [Australian Banking Association](#).

523 Submission to the Discussion Paper: [National Australia Bank](#), 2.

524 Submissions to the Discussion Paper: [ACTU](#); [Electrical Trades Union of Australia](#); [Professor John Swinson](#); [Professor David Lindsay](#).

525 Submission to the Discussion Paper: [Calabash Solutions](#), 7. See also, [Professor John Swinson](#), 4-5 and [Professor David Lindsay](#), 16-17.

526 Attorney-General's Department, *Employee Representatives Roundtable*, 9 February 2022.

527 Submission to the Discussion Paper: [European Commission](#), 2.

528 Submission to the Discussion Paper: [Business Council of Australia](#), 11; [Australian Chamber of Commerce and Industry \(ACCI\)](#), 9; [Ai Group](#), 20-21; [Optus](#), 14; [Communications Alliance](#), 21; [Clubs Australia](#), 2; [Australian Collectors & Debt Buyers Association](#), 5.

529 Submission to the Discussion Paper: [Ai Group](#), 21.

530 Submission to the Discussion Paper: [Australian Chamber of Commerce and Industry \(ACCI\)](#), 15.

531 Submission to the Discussion Paper: [OAIC](#), 55.

532 [Discussion Paper](#), 52-53.

Enhancing privacy protections through the *Fair Work Act 2009* (Cth) (Fair Work Act) would potentially benefit a larger number of private sector employees due to its greater coverage of private sector employers than the Privacy Act (depending on the removal of the small business exemption). It is also accessible to employers and employees and their representatives as a no costs jurisdiction with a focus on informal dispute resolution. The general protections provisions in the Fair Work Act also protect employees and employment candidates from adverse action in relation to their workplace rights, which would be relevant in the event of employees querying the collection of their personal information under privacy obligations included in a 'workplace law'⁵³³.

The Castan Centre supported enhancing privacy protections for employees under the Privacy Act because although some employers may follow best practice guidelines – including FWO guidance that employers should follow the principles in the Privacy Act regardless of its application – 'without the support of the legislation, employees are deprived of the legal protection and rights they have under the Privacy Act and to make complaints to the Privacy Commissioner'.⁵³⁴ The Office of the Victorian Information Commissioner also considered that providing privacy protections under the Act would ensure employees have 'appropriate avenues to make privacy complaints where necessary'.⁵³⁵

While the ACTU's submission highlighted 'a clear regulatory gap' in the treatment of employee records under workplace relations laws which 'do not regulate the storage, handling and use or potential disclosure of personal information within employee records',⁵³⁶ it supported regulating employee privacy through negotiated collective agreements.⁵³⁷ The ETU also favoured a regulatory approach involving the participation of industrial stakeholders, recommending that the Privacy Act be amended 'to require privacy codes to be developed in consultation with industry representatives similar to the manner in which safety Codes of Practice are developed', to specify what health information may be collected and used.⁵³⁸

7.5 Proposal

Stakeholders are divided on whether private sector employees' privacy is adequately protected and whether the employee records exemption requires reform. Submissions from employers and their representatives express a strong desire to retain the exemption or strengthen it. Submissions from employee representatives and other stakeholders consider that reform is needed, but there are different views on how it should be achieved.

However, it is evident from submissions and case law that there are legitimate concerns regarding:

- the amount and highly sensitive nature of employees' personal and sensitive information being collected, used and disclosed in the context of the employment relationship
- limited transparency about what employees' personal and sensitive information is being used and disclosed for and whether it is in fact reasonably necessary to administer the employment relationship
- the difficulties which requiring employees' consent to collect their sensitive information poses for employers and employees, including whether consent can be considered to be freely given in the employment and pre-employment context, and
- the fact that employee records containing often highly sensitive information are not subject to security and destruction or data breach reporting requirements.

It is less clear from submissions about the best way to enhance protections for private sector employees in legislation. Extending enhanced protections under the Act would guard against fragmenting privacy regulation:

- for individuals in their private capacity and as employees,
- for APP entities as regards employees' information and other information they hold, and
- enforcement by virtue of the OAIC being the specialised privacy regulator responsible for complaint resolution, enforcement and code development.

However, there are also benefits in using some of the existing architecture within the Fair Work Act. Further consideration is required as to how the privacy and workplace relations laws should interact.

533 *Fair Work Act 2009* (Cth) s 341.

534 Submission to the Discussion Paper: [Castan Centre](#), 9, citing Fair Work Ombudsman, [Workplace privacy: Best Practice Guides](#), 5.

535 Submission to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 3.

536 Submission to the Discussion Paper: [ACTU](#), citing [Legal Aid Queensland](#), 3.

537 Submission to the Discussion Paper: [ACTU](#), 4. Note, a recent ACTU resolution on [Workers Privacy and Data](#) 'aimed at addressing the significant shortfalls in regulation and safeguards regarding the use and protection of employee data by employers' endorsed principles for use of workers' data and their implementation through collective bargaining.

538 Submission to the Discussion Paper: [Electrical Trades Union of Australia](#), 4.

- 7.1 Enhanced privacy protections should be extended to private sector employees, with the aim of:**
- (a) A providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for**
 - (b) ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information**
 - (c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and**
 - (d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm.**

Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.

8. Political exemption

Registered political parties are exempted entirely from the Act.⁵³⁹ A more limited exemption, in section 7C of the Act, applies to political representatives (MPs and local government councillors), and their affiliates⁵⁴⁰ and the affiliates of registered political parties⁵⁴¹ (collectively, with political parties, 'political entities'). This exemption covers acts and practices done for any purpose in connection with an election, a referendum, or participation in another aspect of the political process.⁵⁴² The political exemption was introduced to encourage freedom of political communication and enhance the operation of the electoral and political process in Australia.⁵⁴³

Advances in technology which have increased the volume of information about voters that can be collected and harnessed for political influence have raised concerns about privacy risks and concerns that the exemption is not achieving its objective.⁵⁴⁴ The Issues Paper sought feedback on whether political acts and practices should continue to be exempted from the operation of some or all of the APPs. The Discussion Paper considered whether the exemption is achieving its objective and canvassed the approach to regulating political parties under data protection laws in the UK, Canada and New Zealand.⁵⁴⁵ Further feedback was sought on the impact on freedom of political communication of bringing political parties within the scope of the Act and costs and benefits of applying specific APPs to political parties and their affiliates.⁵⁴⁶

8.1 The implied freedom of political communication

Exempting political entities from requirements under the Act was intended to encourage freedom of political speech, and operate in a manner consistent with the implied freedom of political communication under the Australian Constitution. The implied freedom of political communication has been held by the High Court to be a limit on Commonwealth legislative and executive power which infringes political communication, implied from sections 7 and 24 and related sections of the Constitution, to ensure that the people of the Commonwealth may 'exercise a free and informed choice as electors'.⁵⁴⁷

The freedom of political communication can be limited only by laws which are reasonably appropriate and adapted to serving a legitimate end or overriding public purpose. The rights to freedom of expression and freedom of political communication are fundamental human rights that are enjoyed by all Australians, and all people who are in Australia. However, these rights are subject to limitations that are reasonable, necessary and proportionate to a legitimate objective in a free and democratic society to achieve an appropriate balance between freedom of expression and the protection of groups and individuals.

The ALRC in its Report 108 considered that the need to recognise the special status of political acts and practices under the Constitution was the most compelling reason for exempting political acts and practices of political entities from the Act.⁵⁴⁸ However, it concluded that registered political parties should be brought within the scope of the act and the exemption for political entities should be removed to promote public confidence in the political process and remove the advantage which the exemption confers on incumbent political entities.⁵⁴⁹

539 Privacy Act s 6C.

540 Contractors and subcontractors.

541 Contractors, subcontractors and volunteers.

542 Privacy Act s 7C. Acts and practices of affiliates that facilitate exempt acts or practices of political entities are also exempt.

543 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15752 (Daryl Williams, Attorney-General).

544 Moira Paterson and Normann Witzleb, 'Voter privacy in an era of big data: time to abolish the political exemption in the Australian Privacy Act', in Moira Paterson, Normann Witzleb and Janice Richardson (eds), *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-targeting* (Routledge, 2020) 164-185; Tegan Cohen, 'The Political Exemption: A Justifiable Invasion of Privacy in the Political Sphere?' (2021) 44(2) *University of New South Wales Law Journal* 584.

545 [Discussion Paper](#), 60-61.

546 *Ibid*, 61.

547 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 560.

548 [ALRC Report 108](#), [41.55]. The other constitutional doctrine referred to by the ALRC in relation to the political exemption is parliamentary privilege, [41.63]-[41.64], Recommendation 41-2.

549 [ALRC Report 108](#), Recommendation 41-1, 1433; [41.57]. The ALRC considered that including a 'savings clause' to the effect that the Act would not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication or parliamentary privilege would address any risk of infringing the implied freedom in repealing the exemptions: Recommendation 41-2, 1433; [41.63].

8.2 Feedback on the political exemption

Almost all submitters that commented on the exemption considered that it was not justifiable and should be narrowed or removed.⁵⁵⁰ Submitters highlighted that if the exemption were removed, political entities would still be able to collect personal information from the electorate, and communicate with voters in a variety of ways, within the framework of the Act.⁵⁵¹ Citing the example of the UK, the OAIC submitted that there was little evidence that data protection laws operating in other countries have had any considerable impact on political parties' ability to perform their basic democratic roles, including political communication.⁵⁵² The New South Wales Council for Civil Liberties submitted that a severe lack of privacy is incompatible with political freedom.⁵⁵³

Submitters considered that, rather than enhancing the operation of the electoral and political process in Australia by protecting freedom of political speech, the political exemption is serving to undermine the integrity of the democratic electoral process.⁵⁵⁴ Particular concerns included:

- lack of accountability and transparency in the handling of voters' information
- the potential for voters' information to be used unfairly in ways which undermine Australia's democratic system, particularly with regards to targeted political messaging and advertising
- the lack of control that individuals have over the use of their information to direct market and target them with political messages and advertisements, and
- the absence of security obligations for voters' information held by political entities.

Submitters also indicated that removing the exemption would more closely align the treatment of political entities under data protections laws in comparable international jurisdictions.⁵⁵⁵

Two submitters supported retaining the exemption. Nine stated that it 'enhances free and open communication and improves participation in and engagement with our political processes'.⁵⁵⁶ The Cyber Security Cooperative Research Centre proposed retaining the exemption from the Act but removing relevant exemptions from the *Do Not Call Register Act 2006* (Cth) (DNCR Act) and spam rules.⁵⁵⁷

8.2.1 Accountability and transparency

Accountability of registered political parties

Submitters considered that the political exemption contributes to a lack of accountability and transparency in the way political entities handle personal information,⁵⁵⁸ which has the potential to reduce public confidence in the political process.⁵⁵⁹

550 Submissions to the Discussion Paper: [OAIC](#), 60; [NSW Council for Civil Liberties](#), 14; [Office of the Victorian Information Commissioner](#), 4; [Salinger Privacy](#), 19; [Rob Lake](#); [ADIA](#), 6; [Calabash Solutions](#), 8; [Privacy 108](#), 13; [Access Now](#), 11; [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 4; [Electronic Frontiers Australia](#), 8; [Australian Privacy Foundation](#), 7; [Castan Centre](#), 12; [Digital Rights Watch](#), 18; [Professor David Lindsay](#), 16-17; [Graham Greenleaf, UNSW Sydney](#), 2; [Australian Communications Consumer Action Network](#), 8; [Law Council of Australia](#), 11; [elevenM](#), 22; [IIS Partners & Group Up Consulting](#), 7; [Australian Information Security Association](#), 5; [Paul Salanitri](#), 2; [Response 929507191](#); [Response 745270819](#); [Internet Association of Australia](#), 3; [Information and Privacy Commission NSW](#), 4; [Office of the Information Commissioner Queensland](#), 3. See also Submissions to the Discussion Paper: [Michael Douglas, UWA Law School](#), 2; [DIGI](#), 2; [Reset Australia](#), 3; [Data Synergies](#), 32. All but two submissions to the Issues Paper proposed removing the exemption or narrowing the scope, [Discussion Paper](#), 58.

551 Submissions to the Discussion Paper: [OAIC](#), 59; [Privacy 108](#), 13; [Office of the Victorian Information Commissioner](#), 4; [Castan Centre](#), 14 quoting Paterson and Witzleb 'Voter privacy' 183; [Law Council of Australia](#), 11. See also Submission to the Issues Paper: [Queensland University of Technology, Faculty of Law](#), 18.

552 Submission to the Discussion Paper: [OAIC](#), 58.

553 Submission to the Issues Paper: [NSW Council for Civil Liberties](#), 6. See also Submission to the Issues Paper: [Castan Centre for Human Rights Law – Monash University](#), 28.

554 Submissions to the Discussion Paper: [Michael Douglas, UWA Law School](#), 2; [Office of the Victorian Information Commissioner](#), 3; [elevenM](#), 22; [Digital Rights Watch](#), 18; [Professor David Lindsay](#), 17. See also Submissions to the Discussion Paper: [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 2-4; [OAIC](#), 58; Submission to the Issues Paper: [OAIC](#), 65.

555 Submissions to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 4; [Australian Communications Consumer Action Network](#), 8. See also Submission to the Discussion Paper: [Samantha Gavel, Information and Privacy Commission NSW](#), 4. The approach in other jurisdictions is set out in the [Discussion Paper](#), 60-61.

556 Submission to the Issues Paper: [Nine](#), 9.

557 Submission to the Issues Paper: [Cyber Security Cooperative Research Centre](#), 7.

558 Submission to the Discussion Paper: [Office of the Information Commissioner Queensland](#), 3.

559 Submissions to the Discussion Paper: [Castan Centre](#), 13; [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 2-3. See also Submissions to the Discussion Paper: [Electronic Frontiers Australia](#), 8; [OAIC](#), 58; [Privacy 108](#), 13; [Calabash Solutions](#), 8; [Office of the Victorian Information Commissioner](#), 4; [Access Now](#), 10-11; [Internet Association of Australia](#), 3; Submission to the Issues Paper: [Office of the Victorian Information Commissioner](#), 6.

A number of submitters echoed the ALRC Report 108 finding that public confidence in the political process would be promoted by ensuring that political entities adhered to the same privacy principles required of the wider community.⁵⁶⁰ elevenM submitted that 'a critical aspect of trust in public institutions is the willingness to submit to the same levels of accountability as everyone else.'⁵⁶¹

Currently, registered political parties are entirely outside of the Act under section 6C. This means that if a registered political party collects, uses or discloses personal information for a purpose unconnected with the political process, it is not required to comply with the Act. However, other political entities are only exempt from the Act's requirements to the extent that they are handling information for purposes connected to the political process under section 7C.

While it is questionable whether a registered political party would have an interest in handling personal information other than for a purpose connected to the political process, their exclusion from the definition of 'organisation' for the purposes of the Act renders them unaccountable for their handling of personal information for non-political purposes. Where the rationale for the exemption was to encourage freedom of political communication, excluding registered political parties from the Act entirely, and thereby from accountability for non-political handling of personal information, goes significantly further than the exemption's stated rationale.

Proposal – registered political parties within the scope of the Act

It is proposed that the definition of 'organisation' should be amended to include registered political parties, and that they be included within the scope of the exemption in section 7C of the Act. This would make registered political parties subject to the Act, and be required to comply with the APPs in the handling of personal information, to the same extent as political representatives (and political affiliates) unless exempted by the operation of the exemption in section 7C.

8.1 Amend the definition of 'organisation' under the Act so that it includes a 'registered political party' and include registered political parties within the scope of the exemption in section 7C.

Transparent handling of voters' information

Submitters raised concerns about transparency in relation to the handling of voters' information.⁵⁶² The Office of the Victorian Information Commissioner submitted that 'political parties collect personal information about voters from a variety of sources such as media and data brokerage services. When combined with personal information contained in electoral rolls, political parties can build large databases with detailed information about voters without their knowledge or consent.'⁵⁶³ Because of the exemption, they are not required to inform voters of the ways in which their personal information is collected, or specify how it will be used or disclosed.⁵⁶⁴

⁵⁶⁰ ALRC Report 108, [41.54]. Submissions to the Issues Paper: [Office of the Information Commissioner Queensland](#), 3; [Centre for Cyber Security Research and Innovation](#), 8; [Australian Information Security Association](#), 13; [Calabash Solutions](#), 5. See also Submission to the Discussion Paper: [IIS Partners & Ground Up Consulting](#), quoting former Federal Privacy Commissioner Malcolm Crompton, 7.

⁵⁶¹ Submission to the Discussion Paper: [elevenM](#), 22, citing former Victorian Privacy Commissioner, Paul Chadwick, quoted in [ALRC Report 108](#), [41.33].

⁵⁶² Submissions to the Discussion Paper: [Internet Association of Australia](#), 3; [Office of the Information Commissioner Queensland](#), 3; [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 2; [Castan Centre](#), 13; [Office of the Victorian Information Commissioner](#), 3; Submissions to the Issues Paper: [Office of the Victorian Information Commissioner](#), 6. See also Submissions to the Discussion Paper: [Data Synergies](#), 5; [Salinger Privacy](#), 12.

⁵⁶³ Submission to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 3; Submission to the Issues Paper: [Office of the Victorian Information Commissioner](#), 5-6. See also Submissions to the Discussion Paper [Australian Data and Insights Association](#), 6; [Australian Privacy Foundation](#) (which referred to 'large-scale data mining of voter characteristics'), 7 and Submission to the Issues Paper: [Office of the Information Commissioner Queensland](#), 3.

⁵⁶⁴ Submission to the Issues Paper: [Office of the Victorian Information Commissioner](#), 5-6.

The UK ICO has highlighted that the ‘often invisible’ nature of campaigning techniques using digital technologies can affect people’s trust and confidence in how their information is being used.⁵⁶⁵ The Internet Association of Australia submitted ‘[g]iven the gravity of the issue of voter manipulation, placing greater restrictions on political parties to ensure transparency is important and likely to result in greater public confidence.’⁵⁶⁶

Greater transparency in relation to political communication may, depending on the context, not only be consistent with and support the constitutionally-prescribed system of government but serve to protect it. In *LibertyWorks Inc v Commonwealth*⁵⁶⁷ the High Court determined that the purpose of the *Foreign Influence Transparency Act 2018*,⁵⁶⁸ which was intended to make transparent the involvement of foreign interests in political communication, was not merely consistent with the freedom of political communication, but ‘reinforces the freedom despite doing so by burdening some political communication.’⁵⁶⁹

Proposal – greater transparency through privacy policies

In light of concerns about the potential for lack of transparency in relation to political entities handling of voters’ information to undermine confidence in the political process, it is proposed that the Act be amended to require political entities to be more transparent about how they handle personal information. This could be achieved by requiring entities that are covered by the political exemption in section 7C to have a privacy policy in accordance with APP 1. A privacy policy would provide greater transparency about how they handle personal information for acts or practices covered by the exemption.

The Discussion Paper noted that a number of political parties have published privacy policies online.⁵⁷⁰ The requirement for entities covered by the exemption to have a privacy policy would enshrine this practice in legislation. It would also ensure the privacy policies include relevant matters listed under APP 1, including how they handle the personal information for the purposes covered by the exemption, whether the information is likely to be disclosed overseas, and detail on how an individual may access personal information held about them, or make a complaint.

8.2 Political entities should be required to publish a privacy policy which provides transparency in relation to acts or practices covered by the exemption.

8.2.2 Fair and reasonable handling of voters’ information

The advent of ‘Big Data’⁵⁷¹ and new techniques for understanding and utilising it (data analytics) has transformed political campaigning in recent years, in Australia and overseas.⁵⁷² Submitters expressed concern that the political exemption enables political parties to use voter information in targeting systems to deliver political messaging and advertisements in ways which may negatively impact democracy.⁵⁷³

565 UK ICO, ‘[Guidance for the use of personal data in political campaigning](#)’ (Web Page, October 2022).

566 Submission to the Discussion Paper: [Internet Association of Australia](#), 3.

567 *LibertyWorks Inc v Commonwealth* [2021] HCA 18.

568 *Foreign Influence Transparency Act 2018* [Cth].

569 *LibertyWorks Inc v Commonwealth* [2021] HCA 18. [208] [Edelman JJ]; [61] [Kiefel CJ, Keane and Gleeson JJ].

570 [Discussion Paper](#) 61. For example, 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).

571 Big Data may be defined as ‘large amounts of structured and unstructured data that exceeds the ability of commonly used software tools to capture, manage and process’, see Australian Cyber Security Centre, ‘[Big data](#)’ (Web Page); It is often described by reference to massive data sets, real-time data, and different sources of data, UK ICO, *Big data, artificial intelligence, machine learning and data protection* [Paper, 2016].

572 See Submission to the Issues Paper: [OAIC](#), 65 [4.31]–[4.32]; UK ICO, *Democracy disrupted? Personal information and political influence* (11 July 2018).

573 Submissions to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 3-4; [Access Now](#), 11; [elevenM](#), 22-23; [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 2-4; [Castan Centre](#), 12-13; [Digital Rights Watch](#), 18; [Professor David Lindsay](#), 17; Submissions to the Issues Paper: [Office of the Victorian Information Commissioner](#), 6; [Salinger Privacy](#), 12; [Office of the Information Commissioner, Queensland](#), 3; [Digital Rights Watch](#), 5. See also Submission to the Discussion Paper: [Reset Australia](#), 3,

Online political ‘micro-targeting’ involves collecting data about individuals, using that data to identify groups of people that are likely to be susceptible to a certain message, and tailoring online content to those groups.⁵⁷⁴ As set out in Chapter 20, targeting often relies on ‘profiling’ which is the analysis of information about an individual to evaluate certain aspects about them, and which classifies individuals into different groups or sectors, using algorithms or machine learning.⁵⁷⁵ Profiling⁵⁷⁶ and targeted advertising and content uses information which individuals may intentionally provide, as well as information obtained in ‘far less consensual (new) ways and then repurposed for unanticipated objectives.’⁵⁷⁷

Many submitters referenced the Cambridge Analytica matter,⁵⁷⁸ in which data was accessed from Facebook and used to target individuals with political messages, and some expressed concern about whether the political exemption may allow such an incident in Australia.⁵⁷⁹ In 2018, the UK ICO determined that the processing of Facebook users’ data by Cambridge Analytica for political purposes, including purposes connected with the United States 2016 presidential campaigns, was unfair under the UK Data Protection Act.⁵⁸⁰ According to the European Council, the Cambridge Analytica case demonstrated that data protection has become a key issue for the functioning of democracies.⁵⁸¹ The Office of the Information Commissioner, Queensland submitted that ‘the Cambridge Analytica example is illustrative of the significant risks posed to the integrity of the electoral process when personal information is misused for political ends.’⁵⁸²

It was submitted that targeting of political messaging and advertisement can impact democracy by inhibiting informed political debate and restricting voters’ ability to make freely informed decisions.⁵⁸³ The Castan Centre submitted:

Micro-targeting may be of concern for example, where it includes getting voters ‘to hold opinions that they would not hold if aware of the best available information and analysis’ and where ‘it is used to mislead voters or keep them ignorant about matters relevant to their vote’.⁵⁸⁴

It was also suggested that, in delivering political information directly to an individual, targeting reduces public scrutiny and collective deliberation.⁵⁸⁵ This can make it easier for voters to be misled and for fake news to be disseminated.⁵⁸⁶

574 Tom Dobber, Ronan Fathaigh and Frederik Zuiderveen Borgesius, ‘The regulation of online political micro-targeting in Europe’ (2019) 8(4) *Internet Policy Review* 2.

575 Chapter 20 provides an explanation of how targeting works. See also: UK ICO, ‘[Profiling](#)’ (Web Page, September 2020) and UK ICO, ‘[Profiling in political campaigning](#)’ (Web Page, October 2022).

576 Profiling is defined and discussed in Chapter 20.

577 Normann Witzleb and Moira Paterson ‘Micro-targeting in Political Campaigns: Political Promise and Democratic Risk’, in Uta Kohl and Jacob Eisler (eds) *Data-Driven Personalisation in Markets, Politics and Law* (Cambridge University Press, 2021) 223-239, 225. The UK ICO’s audits raised concerns about ‘invisible’ profiling activities by political parties: see UK ICO, [Audits of data protection compliance by UK political parties](#) (Summary report, November 2020) 17.

578 Submissions to the Discussion Paper: Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green, 3; [Digital Rights Watch](#), 18; [Professor David Lindsay](#) 17; [Castan Centre](#), 13; [elevenM](#), 22; Submissions to the Issues Paper: [NSW Council for Civil Liberties](#), 6; [Office of the Information Commissioner Queensland](#), 3; [Centre for Media Transition, University of Technology Sydney](#), 11; [Reset Australia](#), 5; [Kimberlee Weatherall](#), 4; [OAIC](#), 65; [Australian Communications Consumer Action Network](#), 10; [Australian Privacy Foundation](#), 16.

579 Submissions to the Issues Paper: [Centre for Media Transition, University of Technology Sydney](#) submitted that, in Australia, no action could be taken against political entities if they engage in Cambridge-Analytica style activities, 11; [New South Wales Council for Civil Liberties](#) submitted that, if contracted to an Australian political party, the activities of Cambridge Analytica would be likely be exempt, 6.

580 UK ICO, *Investigation into the use of data analytics in political campaigns* (Report to Parliament, 6 November 2018) 35.

581 Submission to the Issues Paper: [OAIC](#), 65 citing European Commission, *Free and Fair elections: Guidance Document: Commission guidance on the application of Union data protection law in the electoral context; A contribution from the European Commission to the Leaders’ meeting in Salzburg on 19-20 September 2018*, Brussels, 12.9.2018 COM (2018) 638 final.

582 Submission to the Issues Paper: [Office of the Australian Information Commissioner, Queensland](#), 3.

583 Submissions to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 3; [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 3. [Digital Rights Watch](#), 18. Submission to the Issues Paper: [Queensland University of Technology, Faculty of Law](#), 18.

584 Submission to the Discussion Paper: [Castan Centre](#), 12, quoting Lawrence R Jacobs and Robert Y Shapiro, *Politicians Don’t Pander: Political Manipulation and the Loss of Democratic Responsiveness*, University of Chicago Press, 2000, xv, as quoted in Murray Goot, ‘Politicians, public policy and poll following: Conceptual difficulties and empirical realities’ (2005) 40 *Australian Journal of Political Science* 189, 189; also quoting Paterson and Witzleb ‘Voter Privacy’, 172-173.

585 Submission to the Issues Paper: [Queensland University of Technology, Faculty of Law](#), 18.

586 Normann Witzleb and Moira Paterson ‘Micro-targeting in Political Campaigns: Political Promise and Democratic Risk’, in Uta Kohl and Jacob Eisler (eds) *Data-Driven Personalisation in Markets, Politics and Law* (Cambridge University Press, 2021) 227; Moira Paterson and Normann Witzleb, ‘Voter privacy in an era of big data: time to abolish the political exemption in the Australian Privacy Act’, in Moira Paterson, Normann Witzleb and Janice Richardson (eds), *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-targeting* (Routledge, 2020) 172-173; Submissions to Issues Paper: [Digital Rights Watch](#), 5, and [Salinger Privacy](#), 12 submitted that individual-targeted content online can more easily facilitate misinformation than offline political advertising could achieve. See also, ACMA, [A report to government on the adequacy of digital platforms’ disinformation and news quality measures](#) (June 2021) 56.

The OAIC submitted that targeting has been linked to political polarisation.⁵⁸⁷ Stakeholders said that targeting practices can be manipulative⁵⁸⁸ and exploit individual beliefs and fears.⁵⁸⁹ The ACCC found that it can be used to inflame societal tensions.⁵⁹⁰

According to a report by the Australian Communications and Media Authority (ACMA), there is increasing concern within the community over online disinformation and misinformation.⁵⁹¹ Micro-targeted advertising is an area of concern that the ACMA is continuing to monitor.⁵⁹²

As set out in the Discussion Paper, UK political parties are subject to data protection laws. The first data protection principle, that data be processed 'lawfully, fairly and in a transparent manner' has been described as 'the cornerstone' of data protection law.⁵⁹³ According to UK ICO guidance:

- fairness requires personal data to be handled only in ways that people reasonably expect, and not used in ways that have unjustified adverse effects on them
- it is unlikely to be fair if a person is deceived or misled when the personal data is obtained, and
- before engaging with voters using methods such as data analytics, micro-targeting and automated calling, a campaigner must assess whether the proposed methods are fair.⁵⁹⁴

The Castan Centre submitted that:

The example of the GDPR suggests that subjecting political parties to the general requirements of fair, transparent and lawful processing would go some way towards 'moderating' political micro-targeting in terms of creating a more rigorous and transparent process with regulatory oversight.⁵⁹⁵

In Chapter 3, it is proposed that the Act recognise the public interest in privacy protection. In recent times, Australians have observed privacy breaches and the apparent misuse of personal information in the political life of other democracies, with potential ramifications which are much broader than privacy harms affecting single individuals.⁵⁹⁶ The public interest in protecting the privacy of all Australians is particularly apparent in the political sphere.⁵⁹⁷

Submitters indicated that the political exemption is out of step with the expectations of the Australian community.⁵⁹⁸ Queensland University of Technology Faculty of Law highlighted that:

Big data, data analytics, and ubiquitous digital platforms such as Facebook and Google, have provided campaigners with new and enhanced methods for voter profiling and message personalisation which could not have been anticipated when the exemptions were originally crafted.⁵⁹⁹

587 Submission to the Issues Paper: [OAIC](#), 25 [1.20] citing Steven L. Johnson, Brent Kitchens and Peter Gray, 'Facebook serves as an echo chamber: especially for conservatives. Blames its algorithm', *The Washington Post* (Online, 26 October 2020). See also, Normann Witzleb and Moira Paterson 'Micro-targeting in Political Campaigns: Political Promise and Democratic Risk', in Uta Kohl and Jacob Eisler (eds) *Data-Driven Personalisation in Markets, Politics and Law* (Cambridge University Press, 2021) 224, 227-228.

588 Submissions to the Discussion Paper: [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 3; [Castan Centre](#), 15; [Digital Rights Watch](#), 18; [Professor David Lindsay](#), 17. Submissions to the Issues Paper: [Centre for Media Transition, University of Technology Sydney](#), 11; [Reset Australia](#), 5; [Australian Privacy Foundation](#), 16; [Castan Centre for Human Rights Law – Monash University](#), 28. [Dr Kate Mathews Hunt, Bond University](#), 8. See also, Submission to the Discussion Paper: [Reset Australia](#), 3.

589 Submission to the Discussion Paper: [elevenM](#), 23.

590 ACCC [DPI Report](#) 446.

591 ACMA, [A report to government on the adequacy of digital platforms' disinformation and news quality measures](#) (June 2021) 1.

592 Ibid 83.

593 UK GDPR art 5(1)(a) provides that personal data shall be 'processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'. See UK ICO, '[Lawful, fair and transparent processing](#)' (Web Page, October 2022); UK ICO, '[Democracy disrupted? Personal information and political influence](#)' (11 July 2018).

594 UK ICO, '[Lawful, fair and transparent processing](#)' (Web Page, October 2022). The guidance is for all 'controllers' who process personal data for political campaigning purposes.

595 Submission to the Discussion Paper: [Castan Centre](#), 13, quoting Normann Witzleb and Moira Paterson 'Micro-targeting in Political Campaigns: Political Promise and Democratic Risk', in Uta Kohl and Jacob Eisler (eds) *Data-Driven Personalisation in Markets, Politics and Law* (Cambridge University Press, 2021) 233.

596 See Submission to the Discussion Paper: [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 3 citing Nicholas Confessore, '[Cambridge Analytica and Facebook: The Scandal and the Fallout So Far](#)' *The New York Times* (online, 4 April 2018); see also United States Department of Justice [Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election](#) (Press Release 18 - 923, 13 July 2018).

597 Normann Witzleb and Moira Paterson note the 'collective interests engaged in politics and strongly affected by micro-targeting', Normann Witzleb and Moira Paterson 'Micro-targeting in Political Campaigns: Political Promise and Democratic Risk', in Uta Kohl and Jacob Eisler (eds) *Data-Driven Personalisation in Markets, Politics and Law* (Cambridge University Press, 2021) 225. See also, Submission to the Issues Paper: [OAIC](#), 25 [1.20]; [Salinger Privacy](#), 12.

598 Several submissions referred to the 2020 OAIC, *Australian Community Attitudes to Privacy Survey* (2020) finding that 74 per cent of respondents supported making political parties subject to the Privacy Act, and the Resolve Strategic (2021) survey for the Sydney Morning Herald and the Age, in which 80 per cent of respondents supported the same proposition: Submissions to the Discussion Paper: [Digital Rights Watch](#), 19; [Salinger Privacy](#), 19. Submission to the Issues Paper: [OAIC](#), 65. See also, Submission to the Discussion Paper: [Electronic Frontiers Australia](#), 8; [Australian Privacy Foundation](#), 7; Submission to the Issues Paper: [NSW Council for Civil Liberties](#), 6; [Kimberlee Weatherall](#), 4.

599 Submission to the Issues Paper: [Queensland University of Technology Faculty of Law](#), 17.

Proposal – require political acts and practices to be ‘fair and reasonable’

It is proposed that the ‘fair and reasonable’ test put forward in Chapter 12 apply to political acts and practices. The objective test would require that the collection, use and disclosure of personal information in political acts and practices be fair and reasonable in the circumstances. It is also proposed that the application of the fair and reasonable test to targeting as set out in Chapter 20, should apply to targeting undertaken by political entities. Targeting, as proposed in Chapter 20, involves the collection, use or disclosure of information which relates to an individual, including personal information, deidentified information, and unidentified information, for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class).

The fair and reasonable test would be guided by seven legislated factors:

1. Whether an individual would reasonably expect the collection, use or disclosure.
2. The kinds, sensitivity and amount of personal information.
3. Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the organisation.
4. The risk of unjustified adverse impact or harm.
5. Whether the impact on privacy is proportionate to the benefits.
6. If the personal information relates to a child, whether the collection, use or disclosure is in the best interests of the child.
7. The objects of the Act.

Requiring political acts and practices to be fair and reasonable would provide stronger protection for privacy. The High Court has found a connection between privacy and personal autonomy⁶⁰⁰ and between privacy and dignity.⁶⁰¹ In *Club v Edwards* it held: ‘the protection of the dignity of the people of the Commonwealth, whose political sovereignty is the basis of the implied freedom, is a purpose readily seen to be compatible with the maintenance of the constitutionally prescribed system of representative and responsible government.’⁶⁰²

Applying the fair and reasonable requirement to political acts and practices and targeting by political entities would also protect the integrity of the democratic electoral process. It would not prevent voters’ information being used to communicate with them but would require additional steps in the handling of that information, including being more transparent and only collecting, using or disclosing it where it is reasonably necessary for the political purpose and not in ways a reasonable individual would not expect. The additional burden would generally be procedural rather than determining the content of any political communication.

In proposing the complete removal of the exemption, the Castan Centre submitted that any adverse impact on the freedom of political communication would be ‘limited, justified and proportionate’.⁶⁰³ It stated:

The Privacy Act does not provide absolute protection for privacy but rather provides for a set of fair information-handling principles which are designed to protect privacy while still enabling the entities which are required to comply with it to carry out their functions and activities. This balance protects the personal autonomy which is necessary for the operation of a democratic system without unreasonably undermining the ability of political parties to communicate with voters.⁶⁰⁴

Applying the fair and reasonable test to political acts or practices may have the practical effect of reducing the circumstances in which the personal attributes of individuals could be used by political entities to profile or target them, but would protect privacy together with the integrity of the Australian democratic electoral process.

⁶⁰⁰ *Farm Transparency* [2022] HCA 23, [31] (Kiefel CJ and Keane JJ).

⁶⁰¹ *Clubb v Edwards* (2019) 267 CLR 171 [49] (Kiefel CJ, Bell and Keane JJ).

⁶⁰² *Ibid* [51].

⁶⁰³ Submission to the Discussion Paper: [Castan Centre](#), 14.

⁶⁰⁴ *Ibid*.

Proposal – prohibit targeting based on sensitive information and traits

It is also proposed that the prohibition on targeting based on certain types of sensitive information and traits (Chapter 20) be extended to targeting undertaken by political entities. Targeting on the basis of sensitive information can be used to marginalise or discriminate against minority groups.⁶⁰⁵ According to the OAIC's submission, political parties may use micro-targeting to 'redline', or avoid communication of certain policies to select demographics based on sensitive information like religious beliefs or ethnicity.⁶⁰⁶

In the UK political parties are prohibited from using special category data (which is similar to sensitive information) to target individuals with political messaging unless they have the explicit consent of the individual, or meet the following narrowly defined condition:

- the processing is of personal data revealing *political opinions*
- the processing is *necessary* for the purposes of the party's political activities
- the processing is *not likely to cause substantial damage or substantial distress* to a person, and
- the individual subject to the processing has not given written notice to the party requiring them not to process their personal data.⁶⁰⁷

There is a separate condition that provides for the processing of special category data of members and regular supporters of political parties in certain circumstances.⁶⁰⁸

In the Australian context, prohibiting political entities from targeting based on some categories of sensitive information (such as racial origin, religious beliefs, sexual orientation, or health) may reduce or prevent discrimination against minority groups, and provide stronger privacy protection for individuals. However, as discussed in Chapter 20, the prohibition should not extend to targeting based on political opinions, membership of a political association or membership of a trade union. This is because communications about such matters are inherently political, or a necessary ingredient of political communication. To guard against any risk of infringing any of the implied freedoms of political communication, several submitters (who proposed that the exemption be repealed entirely) indicated that a 'savings clause' could be included, as recommended by the ALRC, to allow a court to read down the application of the Act to ensure constitutional validity.⁶⁰⁹ Such a clause could be included in the political exemption to safeguard the validity of the requirements on political entities.

8.3 The political exemption should be subject to the following requirements:

(a) Political acts and practices covered by the exemption must be fair and reasonable.

(b) Political entities must not engage in targeting based on sensitive information or traits which relates to an individual, with an exception for political opinions, membership of a political association, or membership of a trade union.

The political exemption should include a savings clause as per Recommendation 41-2 of ALRC Report 108.

⁶⁰⁵ Tegan Cohen, 'The Political Exemption: A Justifiable Invasion in the Political Sphere?' [2021] 44(2) *University of New South Wales law Journal* 604.

⁶⁰⁶ Submission to the Discussion Paper: [OAIC](#), 59. See also, Submission to the Discussion Paper: [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 2-3.

⁶⁰⁷ UK ICO, 'Special category data' (Web Page, October 2022). The condition can only be relied upon by registered political parties, and an 'appropriate policy document' must also be in place.

⁶⁰⁸ *Ibid.*

⁶⁰⁹ [ALRC Report 108](#), Recommendation 41-2. Submissions to the Discussion Paper: [OAIC](#), 60; [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 4; [Castan Centre](#), 14, who submitted it was not strictly necessary. Submissions to the Issues Paper: [NSW Council for Civil Liberties](#), 7; [Australian Privacy Foundation](#), 16.

8.2.3 Greater control over political direct marketing and targeting

Submitters highlighted that the political exemption operates to prevent individuals from exercising control in relation to the use of their information by political entities. Submitters considered it unacceptable that political parties are able to use personal information to make unsolicited calls and texts,⁶¹⁰ and were concerned about individuals' inability to opt out of such communications.⁶¹¹

Stakeholders considered that a large majority of the electorate do not believe that political parties should be able to send out automated text messages, make 'robo-calls'⁶¹² or contact an individual whose number is on the Do Not Call Register.⁶¹³ Some submitters sought amendments to the *Spam Act 2003* (Cth) (Spam Act) and the DNCR Act.⁶¹⁴ The Cyber Security Cooperative Research Centre submitted that the 'explicit desire for privacy' of people listed on the Do Not Call Register should be respected.⁶¹⁵

The political exemption operates to remove the right for individuals under APP 7 to opt out of direct marketing from political entities.

The Spam Act and the DNCR Act contain specific provisions regarding direct marketing.⁶¹⁶ The DNCR Act prohibits the making of unsolicited telemarketing calls (and the sending of unsolicited marketing faxes) to a number on the Do Not Call Register. 'Telemarketing calls' have a commercial purpose and thus would not include any political calls which only provide information.⁶¹⁷ A specific exemption exists for certain 'designated telemarketing calls' (and faxes) by registered political parties, independent members of parliament and electoral candidates. This includes calls (and faxes) to conduct fund-raising for political or electoral purposes.⁶¹⁸ The Spam Act also regulates *commercial* electronic messages – those that offer, advertise or promote goods or services. There is a specific exemption for 'designated commercial electronic messages' authorised by a registered political party.⁶¹⁹

As noted above, targeting has been linked to misinformation.⁶²⁰ The voluntary Australian Code of Practice on Disinformation and Misinformation requires signatories to provide users with greater transparency about the sources of political advertising on digital platforms. Measures may include enabling users to understand whether a political advertisement has been targeted to them.⁶²¹

Proposal – right to opt out of direct marketing and targeting by political entities

Chapter 20 proposes that individuals should be able to opt out of receiving targeted advertising and have an unqualified right to opt out of their personal information being used or disclosed for direct marketing. The proposed right to opt out of direct marketing would extend the current right to opt out of *receiving* direct marketing to enable opting out of use or disclosure of personal information for direct marketing. Chapter 20 proposes that direct marketing be defined in the Act as involving the collection, use or disclosure of personal information to communicate directly with

610 Submissions to the Discussion Paper: [ADIA](#), 6; Response: [745270819](#). Submission to the Issues Paper: [Anonymous Submission](#) 4. See also, Submission to the Issues Paper: [NSW Council for Civil Liberties](#), 6.

611 Submissions to the Discussion Paper: [Calabash Solutions](#), 8; Response [745270819](#). See also, Submission to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 4.

612 An automated telephone call that delivers a pre-recorded message.

613 Resolve Strategic, [Political Campaigning Exemptions](#), survey report to the Sydney Morning Herald, 2, reported by David Crowe, 'Voters want to ban politicians from spamming them with texts and calls' *Sydney Morning Herald* (online, 26 September 2021) cited in Submission to the Discussion Paper: [OAIC](#), 58.

614 Submissions to the Discussion Paper: [elevenM](#), 23; Response: [745270819](#). See also, Submission to the Issues Paper: [Cyber Security Cooperative Research Centre](#), 7.

615 Submission to the Issues Paper: [Cyber Security Cooperative Research Centre](#), 7.

616 OAIC, [APP Guidelines](#) (July 2019) [7.48]

617 ACMA, 'Political calls you might receive' (Web Page, 29 January 2018). 'Telemarketing call' is defined in s 5(1) of the *Do Not Call Register Act 2006* (Cth).

618 ACMA, 'Political calls you might receive' (Web Page, 29 January 2018); *Do Not Call Register Act 2006* (Cth) sch 1, cl3.

619 *Spam Act 2003* (Cth), sch1, cl 3.

620 Submissions to Issues Paper: [Digital Rights Watch](#), 5; [Salinger Privacy](#), 12; Moira Paterson and Normann Witzleb, 'Voter privacy in an era of big data: time to abolish the political exemption in the Australian Privacy Act', in Moira Paterson, Normann Witzleb and Janice Richardson (eds), *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-targeting* (Routledge, 2020) 172-173; Normann Witzleb and Moira Paterson 'Micro-targeting in Political Campaigns: Political Promise and Democratic Risk', in Uta Kohl and Jacob Eisler (eds) *Data-Driven Personalisation in Markets, Politics and Law* (Cambridge University Press, 2021) 227.

621 DIGI, [Australian Code of Practice on Disinformation and Misinformation](#) (October 11 2021) Objective 5, 14. Subject to sections 5.21-5.23, political advertising or content authorised by a registered political party is excluded from the operation of the Code, except where specific instances clearly fall within the scope of disinformation, 7 [4.4]; ACMA, [A report to government on the adequacy of digital platforms: disinformation and news quality measures](#) (June 2021) 56.

an individual to promote advertising or marketing material. The proposed definition of direct marketing would not be limited to promotion of goods or services, and would include promoting the aims and ideals of any organisation, including political campaigning. In light of the concern that individuals should have more control over their receipt of political communication, the proposed opt out rights should apply to direct marketing and targeting by political entities for purposes covered by the exemption.

The High Court has found that ‘privacy and dignity are closely linked’,⁶²² and that, ‘generally speaking, to force upon another person a political message is inconsistent with the human dignity of that person.’⁶²³ It held:

[W]hen in *Lange*⁶²⁴ the Court declared that ‘each member of the Australian community has an interest in disseminating and receiving information, opinions and arguments concerning government and political matters that affect the people of Australia’, there was no suggestion that any member of the Australian community may be *obliged* to receive such information, opinions and arguments.⁶²⁵

In the UK, political parties are prohibited from direct marketing individuals electronically (including campaigning through emails, texts, voicemails or direct messages) unless they have obtained the recipient’s prior consent. They must also provide a simple way for the individual to opt out of the communications.⁶²⁶ Political campaigners may only make telephone calls without consent if the telephone number is not listed on the UK’s equivalent of the Do Not Call Register⁶²⁷ and the individual has not already said that they do not want to be called.⁶²⁸ Political parties must obtain specific consent in order to make automated calls.⁶²⁹

As noted, there are multiple laws which govern political communication in Australia. The ACMA regulates spam and telemarketing. It received 9,886 complaints about political SMS and email messages in 2021–22, equating to nearly half of all the spam complaints it received during this period.⁶³⁰ According to the OAIC’s submission, the large number of complaints to the ACMA about unsolicited political texts indicates that there is strong community concern in relation to these practices, and a misalignment between the privacy regulations and the expectations of the public.⁶³¹

If the proposed amendments are made, there may be an inconsistency between those provisions and the Act. In relation to the DNCR Act, a potential inconsistency could arise where a registered political party, independent member of parliament or electoral candidate authorises the making of a designated telemarketing call, or the sending of designated marketing fax. Where a registered political party sends a ‘designated commercial electronic message’ for a purpose connected to the political exemption there may be an inconsistency between the proposed amendments and the Spam Act. Further consideration of the provisions of the DNCR Act and Spam Act that provide exemptions for designated communications would be required if this proposal is adopted, to ensure there is a consistent policy in relation to communications from political entities.

8.4 The political exemption should be subject to a requirement that individuals must be provided with the means to:

- (a) opt-out of their personal information being used or disclosed for direct marketing by a political entity, and**
- (b) opt-out of receiving targeted advertising from a political entity.**

⁶²² *Clubb v Edwards* (2019) 267 CLR 171, [49] (Kiefel CJ, Bell and Keane JJ).

⁶²³ *Ibid* [51].

⁶²⁴ *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520 at 571.

⁶²⁵ *Clubb v Edwards* (2019) 267 CLR 171, [51].

⁶²⁶ They must comply with the UK *Privacy and Electronic Communications (EC Directive) Regulations 2003* (PECR) as well as the UK GDPR right to object if carrying out direct marketing by electronic means, UK ICO, ‘[Political campaigning – opinion research and direct marketing](#)’ (Web Page, October 2022).

⁶²⁷ The Telephone Preference Service (TPS).

⁶²⁸ UK ICO, ‘[Political campaigning – opinion research and direct marketing](#)’ (Web Page, October 2022).

⁶²⁹ *Ibid*.

⁶³⁰ ACMA, [Submission 325](#) to the Joint Standing Committee on Electoral Matters, *Inquiry into the 2022 Federal Election* (6 October 2022) 3.

⁶³¹ Submission to the Discussion Paper: [OAIC](#), 58–59.

8.2.4 Security

Submitters were also concerned about the security of personal information held by political parties, and supported applying security obligations to them.⁶³² It was submitted that there is no clear reason why parties should not be accountable for keeping personal information secure, and that this has been noted by the ALRC.⁶³³ The Internet Association of Australia supported the imposition of certain APPs to political parties, including the application of data security obligations.⁶³⁴

The OAIC submitted that the amount of personal information held by political parties makes them an attractive target for malicious actors.⁶³⁵ According to OVIC's submission, the fact that political parties are not currently required to implement robust information security measures to protect their information gives rise to the possibility of cyber-attacks or foreign interference in elections.⁶³⁶ 'Malicious actors, both state and non-state, ... are exploiting these weaknesses to interfere in our democratic processes', according to the submission of Reset Australia, which considers that they 'represent a fundamental risk to our existence as a liberal democracy.'⁶³⁷

A number of submitters referred to the reported cyber-attack on the Australian Parliament in the lead up to a federal election in 2019, believed to be perpetrated by a foreign government, which gained access to information held by major political parties.⁶³⁸ Following that attack, a former Privacy Commissioner was reported as saying that it was a 'staggering anachronism' that political parties had weaker oversight on data protection than other organisations, in light of the Mueller Report, which detailed Russian interference in United States politics.⁶³⁹ It was also pointed out following that incident that as 'small organisations with only a few full-time staff' who 'collect, store and use large amounts of information about voters and communities', political parties may be particularly vulnerable to attacks.⁶⁴⁰

Proposal – apply security and destruction obligations

It is proposed that all political entities be required to take reasonable steps to protect personal information and to destroy it when it is no longer required for any purpose in connection with an election, a referendum or participation in another aspect of the political process, in line with the requirements in APP 11. As an important corollary to security obligations, political entities should also be required to comply with the reporting requirements under the NDB scheme. This would enable affected individuals to take steps to protect themselves from harm.

Requiring that reasonable steps be taken to protect personal information, that voters' information be destroyed when it is no longer required, and that individuals be notified when they are affected by an eligible data breach, would not restrict the ability of political parties or representatives to communicate with the electorate. However, it would protect individuals and the community from the impact of loss or interference with the personal information of Australian voters.

632 Submissions to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 4; [OAIC](#), 59; [Internet Association of Australia](#), 3; [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 3-4. Submissions to the Issues Paper: [Queensland Law Society](#), 4; [Centre for Media Transition, University of Technology Sydney](#), 11; [Reset Australia](#), 5.

633 Submission to Discussion Paper: [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 3, citing [ALRC Report 108](#) [41.56], the submission made the same point in relation to 'efficacy' of data. See also, Submission to the Issues Paper: [Australian Privacy Foundation](#), 16.

634 Submission to the Discussion Paper: [Internet Association of Australia](#), 3. See also, Submissions to the Issues Paper: [Data Republic](#), 6; [New South Wales Council for Civil Liberties](#), 7.

635 Submission to the Discussion Paper: [OAIC](#), 59.

636 Submission to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 4; Submission to the Issues Paper: [Office of the Victorian Information Commissioner](#), 6, citing David Crowe, 'Democracy at stake': Parties warned Australia at risk of US-style cyber manipulation, [Sydney Morning Herald](#) (online, 25 April 2019).

637 Submission to the Issues Paper: [Reset Australia](#), 5, citing the cyber-attack on political parties in February 2019.

638 David Crowe, 'Democracy at stake': Parties warned Australia at risk of US style cyber manipulation, [Sydney Morning Herald](#) (online, 25 April 2019) cited in Submissions to Issues Paper: [Centre for Media Transition, University of Technology Sydney](#), 11; [Queensland Law Society](#), 4; Brett Worthington, 'Scott Morrison reveals foreign government hackers targeted Liberal, Labor and National parties in attack on Parliament's servers', [ABC News](#) (online, 18 February 2019) cited in Submission to the Issues Paper: [Reset Australia](#), 5.

639 David Crowe, 'Democracy at stake': Parties warned Australia at risk of US style cyber manipulation, [Sydney Morning Herald](#) (online, 25 April 2019) quoting former privacy commissioner Malcolm Crompton.

640 Michelle Grattan, 'State actor makes cyber attack on Australian political parties', [The Conversation](#) (online, 18 February 2019).

8.5 The political exemption should be subject to a requirement that political entities must:

- (a) take reasonable steps to protect personal information held for the purpose of the exemption from misuse, interference and loss, as well as unauthorised access, modification or disclosure**
- (b) take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for a purpose covered by the political exemption, and**
- (c) comply with the NDB scheme in relation to an eligible data breach involving personal information held for a purpose covered by the political exemption.**

8.2.5 OAIC to provide guidance

Political entities may need to put new frameworks in place to comply with the new obligations that have been proposed. Stakeholders said that there may be some costs,⁶⁴¹ but that it would not pose an unreasonable administrative burden for political parties given the available resources.⁶⁴² However to provide political entities with further assistance on how to comply with the new obligations which would apply, guidance should be developed for political entities.⁶⁴³

8.6 The OAIC should develop further guidance materials to assist political entities to understand and meet their obligations.

⁶⁴¹ Submission to the Discussion Paper: [Calabash Solutions](#), 9.

⁶⁴² Submission to the Discussion Paper: [Law Council of Australia](#), 11.

⁶⁴³ Submissions to the Discussion Paper: [Law Council of Australia](#), 11; [Privacy 108](#), 13. The ALRC also recommended that OPC publish guidance for political entities: [ALRC Report 108](#), Recommendation 41-4, 1437.

9. Journalism exemption

The journalism exemption in the Act recognises the important and beneficial role of journalistic output in Australian society: it provides a forum for the exchange of ideas and opinions and supports a healthy democracy and economy. Journalism fulfils public interest functions, such as holding the powerful to account, in a unique and significant way.⁶⁴⁴ The purpose of the journalism exemption is to balance 'the public interest in providing adequate safeguards for the handling of personal information and the public interest in allowing a free flow of information to the public through the media.'⁶⁴⁵

The Issues Paper sought feedback on whether the journalism exemption appropriately balances the competing interests of privacy and freedom of expression and information. The Discussion Paper considered the current scope of activities covered by the exemption, sought any further evidence of acts or practices of media organisations that pose risks to individuals' privacy and canvassed possible approaches to increasing individuals' privacy protection in relation to acts or practices of media organisations in the course of journalism.⁶⁴⁶

In the two decades since the exemption was introduced a significant shift has occurred in the way media (including news media) is produced and consumed. Traditional media organisations have been challenged by digital platforms and media 'convergence'.⁶⁴⁷ Various inquiries have called for media regulation reform, citing gaps and inconsistencies in its current regulation,⁶⁴⁸ including the ACCC DPI Report which recommended a process to implement a harmonised media regulatory framework.⁶⁴⁹ Any reforms to the journalism exemption under the Act should be considered in the context of the wider framework of media regulation in Australia.

The proposal to introduce a statutory tort for serious invasions of privacy in Chapter 27 would be part of the wider framework of regulation which applies to media organisations, and would operate separately to the exemption for journalism in the Act.

9.1 Journalism exemption and the wider media regulation framework

Acts or practices engaged in by 'media organisations' in the course of journalism are exempt from the operation of the Act, provided the organisation is publicly committed to observe standards that deal with privacy and have been published in writing.⁶⁵⁰ A media organisation may publish such standards itself, or be a member of an industry body which has a published code of conduct containing privacy standards.

In Australia, media regulation is sector specific.⁶⁵¹ Broadcast media primarily operates under a co-regulatory framework: broadcasters develop codes of practice which are registered by the ACMA if it is satisfied that the code provides appropriate community safeguards.⁶⁵² These codes address privacy, although obligations differ between them.⁶⁵³ The national broadcasters – ABC and SBS – develop their own codes of practice, under enabling legislation, which are notified to the ACMA. Each contain privacy standards.⁶⁵⁴ All broadcasting codes of practice provide that complaints can be made under the respective codes. The ACMA has the power to investigate potential breaches of registered codes and take a range of enforcement actions.⁶⁵⁵ The ACMA has more limited enforcement options for national broadcasters.

⁶⁴⁴ ACCC, [DPI Report](#) 283-284.

⁶⁴⁵ [Explanatory Memorandum](#), Privacy Amendment (Private Sector) Bill 2000 (Cth) 81.

⁶⁴⁶ [Discussion Paper](#), 62-66.

⁶⁴⁷ ACCC, [DPI Report](#) 1; Glen Boreham, Department of Broadband, Communications and the Digital Economy, [Convergence review: final report](#) (the Convergence Review) (1 May 2012), which defined 'convergence' as '[t]he coming together of the major communications platforms (broadcasting, telecommunications and online) so that their once separate functions now overlap', 174.

⁶⁴⁸ See for example Ray Finkelstein and Matthew Ricketson, Department of Broadband, Communications and the Digital Economy, [Report of the independent inquiry into the media and media regulation](#) (the Finkelstein Report) (28 February 2012); the Convergence Review, *ibid*; and more recently: Senate Environment and Communications References Committee, Parliament of Australia, [Media diversity in Australia \(Report, December 2021\)](#). See also ACMA, [What audiences want – Audience expectations for content safeguards](#) (Position Paper, June 2022) and [ALRC Report 108](#) [42.125]–[42.129].

⁶⁴⁹ ACCC, [DPI Report](#) Recommendation 6, 31.

⁶⁵⁰ *Privacy Act* s 7B(4).

⁶⁵¹ See overview in ACCC, [DPI Report](#) 4.3, 174-188.

⁶⁵² ACMA, [What audiences want – Audience expectations for content safeguards](#) (June 2022) 1-2. See also, Submission to the Discussion Paper: [Commercial Radio Australia](#), 3.

⁶⁵³ ACMA, [What audiences want – Audience expectations for content safeguards \(June 2022\)](#) 33.

⁶⁵⁴ Submission to the Discussion Paper: SBS, 2, 7; ABC [2021-22 ABC Annual Report](#), Appendix 4, 197, 201.

⁶⁵⁵ *Broadcasting Services Act 1992* (Cth) ss 149, 151, 170. ACMA, [What audiences want – Audience expectations for content safeguards](#) (June 2022) 44. Enforcement action can include imposing additional licence conditions: Submission to the Discussion Paper: Free TV Australia, 12.

The print media are self-regulated.⁶⁵⁶ Many media organisations are members of the Australian Press Council (APC) and are thereby subject to the APC's Standards of Practice, which include privacy standards. The APC has a system for receiving, handling and adjudicating complaints regarding these standards.⁶⁵⁷ Membership is optional and can be withdrawn.⁶⁵⁸ The Independent Media Council (IMC) also handles complaints against funding bodies. It publishes privacy standards to be observed by the print and print online publications which are subject to its oversight.⁶⁵⁹

'Digital Native' media services, including online-only news publishers and internet streaming services, are not captured by current media regulation in Australia.⁶⁶⁰ Live streaming services (including television and radio) are specifically excluded from the definition of a 'broadcasting service'⁶⁶¹ and the ACMA does not have authority to investigate journalism or privacy related complaints about them.⁶⁶²

A number of prominent online publishers are not members of an oversight body, but may have their own standards and complaints procedure. For example, Guardian Australia is subject to its own News and Media Editorial Code, which includes privacy obligations and is overseen by its own internal ombudsman.⁶⁶³

The Act does not contain a definition of 'journalist' or 'journalism' and journalists do not require professional accreditation or registration in order to work.⁶⁶⁴ Journalists who choose to become members of the MEAA⁶⁶⁵ are bound by its Code of Ethics (which includes certain privacy standards) and can be the subject of a complaint to the union.⁶⁶⁶

According to a recent position paper issued by the ACMA, there is now a complex system of direct regulation, co-regulation and self-regulation which 'can result in gaps and discrepancies when it comes to content safeguards, with content providers often subject to different rules for the same piece of content when distributed on- and offline.'⁶⁶⁷ The ACCC found that, despite the active participation of digital platforms in the online news ecosystem, virtually no media regulation applies to them, noting 'digitalisation and the increase in online sources of news and media content have highlighted the inconsistencies in the sector-specific approach to media regulation.'⁶⁶⁸

9.2 Risks to individuals' privacy

Submissions from media organisations said that there were very few privacy complaints or examples of privacy breaches by media organisations and that there was no evidence that a change to the exemption was warranted.⁶⁶⁹ SBS submitted that, in the last three annual reporting periods, it received only one Code complaint that related to privacy.⁶⁷⁰ According to the ABC's submission, the ACMA upheld only six privacy complaints across all investigations into Australian television and radio broadcasters in the five years from 2017-2021. Of the 94 APC complaints referred to in the Issues Paper,⁶⁷¹ only five were upheld, it submitted.⁶⁷² It was submitted that there were good public policy reasons for either maintaining the status quo, or expanding the exemption.⁶⁷³

⁶⁵⁶ ACCC, [DPI Report](#) 177, although it is subject to the general laws of the land, including copyright and defamation laws.

⁶⁵⁷ Ibid; Australian Press Council, [The complaints system: an overview](#) (Web Page, November 2019).

⁶⁵⁸ ACCC, [DPI Report](#) 177-178

⁶⁵⁹ Seven West Media, ['Privacy Policies'](#) (Web Page).

⁶⁶⁰ Senate Environment and Communications References Committee, Parliament of Australia, [Media diversity in Australia](#) (Report, December 2021) 43 [3.64], citing the submission from the Department of Infrastructure, Transport, Regional Development and Communications.

⁶⁶¹ Pursuant to Minister for Communications (Cth), [Broadcasting Services \("Broadcasting Service" Definition – Exclusion\) Determination 2022](#) (13 September 2022) (the Determination). See also ACCC, [DPI Report](#) 180.

⁶⁶² ACMA, [What audiences want – Audience expectations for content safeguards](#) (June 2022) 2; ACMA, ['Complain about a program on TV or radio'](#) (Web Page, 11 November 2022).

⁶⁶³ Submission to the Discussion Paper: [Guardian Australia](#), 18; Senate Environment and Communications References Committee, Parliament of Australia, [Media diversity in Australia](#) (Report, December 2021) 41-42 [3.58]; ACCC, [DPI report](#) 181.

⁶⁶⁴ [ALRC Report 108](#) [42.23].

⁶⁶⁵ Media Entertainment and Arts Alliance.

⁶⁶⁶ ACCC, [DPI Report](#) 178; [ALRC Report 108](#), [42.76]–[42.77].

⁶⁶⁷ ACMA, [What audiences want – Audience expectations for content safeguards](#) (June 2022) 5.

⁶⁶⁸ ACCC, [DPI Report](#) 166.

⁶⁶⁹ Submissions to the Discussion Paper: [ABC](#), 5; [SBS](#), 8; [Commercial Radio Australia](#), 2; [Guardian Australia](#), 20; [Free TV Australia](#), 10.

⁶⁷⁰ Submission to the Discussion Paper: [SBS](#), 8.

⁶⁷¹ [Issues Paper](#), 36, which referred to the APC Annual Report 2017-18.

⁶⁷² Submission to the Discussion Paper: [ABC](#), 5, citing the APC *Annual Report 2017-18*.

⁶⁷³ Submissions to the Discussion Paper: [ABC](#), 4; [SBS](#), 10-11; [Guardian Australia](#), 20; [ARTK](#), 1; [Free TV Australia](#), 8; [Nine](#), 7; [Commercial Radio Australia](#), 1.

In contrast, submissions by privacy advocates provided examples of what they said were unreasonable invasions of privacy by media organisations (and which were said to serve no public interest), such as the shaming of easily denigrated or disadvantaged groups in society, including those breaching pandemic regulations.⁶⁷⁴ Michael Douglas submitted that it is difficult to provide examples of Australian court cases because causes of action to protect privacy are lacking. Instead he pointed to examples of cases involving privacy breaches by the media in the UK, submitting that 'the UK sees more relevant cases because the law there is better for plaintiffs, not because Australian journalists are more ethical.'⁶⁷⁵

According to the submission of the Law Council of Australia, 'the retention of the journalism exemption provides a necessary pre-requisite for the provision of public interest journalism', and if evidence were to emerge that the exemption does not operate effectively in its current form, it 'would need to be considered in detail, together with the question of whether that evidence warranted a change to the journalism exemption.'⁶⁷⁶

The Discussion Paper canvassed feedback on a number of options to reform the journalism exemption, including:

- requiring journalism to be in the public interest to gain the benefit of the exemption
- improving the self-regulation model on which the exemption relies, and
- applying security obligations to media organisations in the course of journalism.

9.3 Public interest requirement

Submissions from media organisations were strongly opposed to introducing a public interest requirement to attract the benefit of the journalism exemption.⁶⁷⁷ The NSW Council for Civil Liberties also considered that it would be inappropriate for the Act to introduce a requirement for journalism to be in the 'public interest' to be protected and that the Act should refrain from defining the types of journalism that is in the public interest. It considered that a preferable approach is to define the public interest as one of *freedom of expression*.⁶⁷⁸

The majority of other submissions supported it, with some proposing a narrower exemption that would cover only investigative and public interest journalism.⁶⁷⁹ It was submitted that the existing exemption does not strike the right balance between privacy and freedom of expression and information and provides insufficient privacy protection.⁶⁸⁰ The OAIC submitted that the journalism exemption should be amended 'to confine it to journalism that is, on balance, in the public interest, as recognised in existing journalism privacy standards.'⁶⁸¹

The OAIC's submission, and some submissions from media organisations, noted that public interest considerations are already taken into account in many privacy standards to which organisations have publicly committed.⁶⁸² The OAIC considered that utilising the public interest standard from these sources would 'promote consistent protection of public interest journalism and limit the regulatory burden on media organisations'.⁶⁸³ Others submitted that the introduction of an additional public interest test as a threshold question – to determine whether the exemption applied – would create uncertainty,⁶⁸⁴ and imply that the existing privacy standards are insufficient.⁶⁸⁵ Important considerations were said to be the potential for an overlap of complaint handling under the Act and other privacy standards, and the interaction with the proposal to create a direct right of action.⁶⁸⁶

⁶⁷⁴ Submissions to the Discussion Paper: [Digital Rights Watch](#), 20; [Australian Privacy Foundation](#), 8; [Salinger Privacy](#), 19. See also, Submission to the Discussion Paper: [Calabash Solutions](#), 10.

⁶⁷⁵ Submission to the Discussion Paper: [Michael Douglas, UWA Law School](#), 2.

⁶⁷⁶ Submission to the Discussion Paper: [Law Council of Australia](#), 10-11.

⁶⁷⁷ Submissions to the Discussion Paper: [SBS](#), 11; [Guardian Australia](#), 20; [Free TV Australia](#), 11; [Commercial Radio Australia](#), 2; [ABC](#), 4-5; [Nine](#), 6. See also Submission to the Discussion Paper: [ARTK](#).

⁶⁷⁸ It proposed a more restrictive definition of 'journalism', limiting the scope of the exemption to acts and practices that are associated with a clear public interest in the freedom of expression, Submission to the Discussion Paper: [NSW Council for Civil Liberties](#), 14.

⁶⁷⁹ Submissions to the Discussion Paper: [OAIC](#), 61; [Calabash Solutions](#), 10; [Michael Douglas, UWA Law School](#), 2; [Digital Rights Watch](#), 20; [Social Services Portfolio](#), 4, 18; [elevenM](#), 23; a narrower exemption was proposed by Submissions to the Discussion Paper: [Australian Privacy Foundation](#), 7; [Privacy 108](#), 14; (applying only to APPs 3, 5 and 6): [Salinger Privacy](#), 19; [Electronic Frontiers Australia](#), 8; [Australian Communications Consumer Action Network](#), 8. See also, Submissions to the Discussion Paper: [Graham Greenleaf, UNSW Sydney](#), 2; [Professor John V Swinson](#), 5-6.

⁶⁸⁰ Submission to the Discussion Paper: [Professor John V Swinson](#), 6; [elevenM](#), 23; [Social Services Portfolio](#), 18.

⁶⁸¹ Submission to the Discussion Paper: [OAIC](#), 62.

⁶⁸² Submissions to the Discussion Paper: [OAIC](#), 61; [Free TV Australia](#), 11; [SBS](#), 11. See also, Submission to the Discussion Paper: [Nine](#), 5.

⁶⁸³ Submission to the Discussion Paper: [OAIC](#), 61-62.

⁶⁸⁴ Submissions to the Discussion Paper: [SBS](#), 11; [Nine](#), 6.

⁶⁸⁵ Submission to the Discussion Paper: [ABC](#), 5.

⁶⁸⁶ Submission to the Discussion Paper: [OAIC](#), 62, noting the ACMA has a complaint handling function.

Submitters highlighted that the line between what is and is not public interest journalism is not clear, and the significance of a particular story is not always known at the time information is collected or published, but may become apparent later on.⁶⁸⁷ Nine noted the impact of #MeToo as an illustration of the potential of 'kiss and tell' stories to shine a light on an important issue.⁶⁸⁸ The ABC submitted that the introduction of a public interest test would have a chilling effect on fair and reasonable reporting.⁶⁸⁹

Media organisations submitted that it would be inappropriate for the IC to be the arbiter of what is, and is not 'public interest journalism', asserting that the IC does not have the necessary expertise,⁶⁹⁰ or familiarity with relevant media-specific considerations.⁶⁹¹ It was submitted that the media industry's privacy standards are uniquely adapted to the context in which they operate.⁶⁹²

The Centre for Media Transition submitted that the journalism exemption 'does not appropriately balance the freedom of the media to report on matters of public interest with individuals' interests in protecting their privacy because its replacement of the APPs with industry guidelines is not rigorous enough in its implementation.'⁶⁹³ It submitted that 'the requirement for a media organisation to subject itself to alternative privacy protections, suitable for newsgathering, should be strengthened and there should be a requirement for independent complaint-handling and decision-making.'⁶⁹⁴

9.4 Strengthening self-regulation

Some stakeholders submitted that the current exemption, which relies, in part, on privacy standards being enforced by media self-regulatory bodies, has not adequately protected the rights of Australians⁶⁹⁵ and that it could be improved by the development of an industry code of practice under the Act, with independent complaint⁶⁹⁶ and appeal rights.⁶⁹⁷ Salinger Privacy submitted that the existing member-based media-industry complaints-handling bodies could be recognised under section 35A of the Act, provided effective appeal rights are also established.⁶⁹⁸ Others considered that self-regulation could not work.⁶⁹⁹

Several broadcasters submitted that the current co-regulatory approach, in which they are overseen by the ACMA, is effective and deals with complaints adequately.⁷⁰⁰ Nine submitted that the exemption has resulted in media organisations committing to standards which have been crafted for the particular context in which they operate, and which are subject to appropriate oversight.⁷⁰¹

Some stakeholders raised concerns about the lack of minimum standards or accountability, submitting that, for some organisations, the requirement to 'publicly commit to privacy standards' could be met by a statement on a website⁷⁰² without any condition of review or approval by a third party.⁷⁰³

The Centre for Media Transition considered that 'amending the journalism exemption without requiring something more than "publicly committing" to unspecified privacy standards would render meaningless any reform of this aspect of privacy regulation.'⁷⁰⁴ Instead, it proposed that 'access to the journalism exemption could be made contingent on participation within an industry-based scheme that is not operated by government, provided it meets criteria such as operating a complaints-handling scheme that is independent of any specific publisher.'⁷⁰⁵

687 Submission to the Discussion Paper: [Nine](#), 6; [Free TV Australia](#), 11.

688 Submission to the Discussion Paper: [Nine](#), 6.

689 Submission to the Discussion Paper: [ABC](#), 5. See also Submission to the Discussion Paper: [SBS](#), 10.

690 Submission to the Discussion Paper: [Guardian Australia](#), 20.

691 Submissions to the Discussion Paper: [Nine](#), 6.

692 Submission to the Discussion Paper: [Nine](#), 5; [Free TV Australia](#), 11.

693 Submission to the Issues Paper: [Centre for Media Transition, University of Technology Sydney](#), 12.

694 Ibid. It also proposed narrowing the definition of 'media organisation' and the introduction of a cross-media standards scheme.

695 Submission to the Discussion Paper: [Privacy 108](#), 14. See also submission to the Discussion Paper: [elevenM](#), 24; [Salinger Privacy](#), 19.

696 Submission to the Discussion Paper: [Privacy 108](#), 14. Complaints would be to the OAIC.

697 Submission to the Discussion Paper: [Electronic Frontiers Australia](#), 8, who submitted that such a Code should be approved and regulated by the Privacy Commissioner.

698 Submission to the Discussion Paper: [Salinger Privacy](#), 19.

699 Submission to the Discussion Paper: [Australian Privacy Foundation](#), 7; [Michael Douglas, UWA Law School](#), 2.

700 Submission to the Discussion Paper: [SBS](#), 9; [Commercial Radio Australia](#), 2-3; [Free TV Australia](#), 12.

701 Submission to the Discussion Paper: [Nine](#), 5.

702 Submission to the Issues Paper: [Centre for Media Transition, University of Technology Sydney](#), 13.

703 Submission to the Issues Paper: [Law Council of Australia](#), 17.

704 Submission to the Discussion Paper: [Centre for Media Transition](#), 8.

705 Ibid. It submitted that the scheme should set its own standards, 9.

9.4.1 Proposal – improve accountability

As noted by the ACCC, the sector-specific approach to media regulation has not adapted well to digitalisation and the shift to the online provision of media services.⁷⁰⁶ In particular, online content – which is increasing in availability and popularity – is not subject to the same level of regulation.⁷⁰⁷ The exemption removes certain journalistic acts and practices from the oversight of the OAIC – with the intent that industry-specific processes undertake the balancing of competing public interests. However, unless an individual has concerns in relation to acts or practices of an organisation that fall within the regulatory remit of the ACMA, access to a remedy is contingent on the publisher of the relevant content having voluntarily subjected itself to a complaints process.

In light of the feedback, rather than applying a public interest test to the exemption, the self-regulation model which underpins the exemption should be strengthened to improve entities' accountability within the existing framework. This would protect personal information while not unduly constraining the independence of the press or the free flow of information to the public.

To enhance the degree of accountability of media organisations under the self-regulation model, it is proposed that the Act be amended to require media organisations to be subject to:

- privacy standards overseen by a recognised oversight body (the ACMA, APC, or IMC); or
- standards that adequately deal with privacy.

The idea that media organisations should be subject to some oversight to access a benefit is not novel; there are examples of other such provisions. For example, to benefit from the provisions of the News Media Bargaining Code,⁷⁰⁸ organisations must be assessed by the ACMA as eligible news businesses. One requirement is the 'professional standards test': the organisation must demonstrate it is subject to one of the listed standards, or analogous internal editorial standards, including a mechanism for complaints.⁷⁰⁹

Guardian Australia submitted that a modified version of the professional standards test could be included in the Act, contending that such a test is objective and 'sets an appropriate rigorous standard for an entity to obtain the benefit of the exemption and is consistent with the public policy rationale for the inclusion of the exemption.'⁷¹⁰

In Victoria, journalists have certain privileges protecting them from being compelled to give evidence that would disclose the identity of their informants.⁷¹¹ The legislation sets out factors to be considered in determining if a person is engaged in journalism (and thus protected),⁷¹² which include a requirement that the person or publisher of the material 'is accountable to comply (through a complaints process) with recognised journalistic or media professional standards or codes of practice.'⁷¹³

In New Zealand, news entities are exempt from the provisions of the NZ Privacy Act to the extent they are carrying out news activities,⁷¹⁴ and are subject to the oversight of:

- the Broadcasting Standards Authority; or
- the New Zealand Media Council; or
- an overseas regulator providing an independent procedure for considering and adjudicating privacy complaints that is accessible to complainants, including complainants in New Zealand; or
- any other body prescribed as a regulatory body by regulation⁷¹⁵ – where to be prescribed the body must:
 - o act independently in performing its functions and duties; and
 - o encourage news entities to develop and observe principles, standards, or codes of conduct appropriate to the type of news activity undertaken by the entities; and
 - o have a proper procedure for receiving and dealing with complaints about news activities.⁷¹⁶

Under the proposed enhanced self-regulatory model, if an organisation is subject to the oversight of a recognised regulatory body any complaint regarding interference with privacy would be made through the relevant complaints process of each body. As noted above, the ACMA, APC, and IMC are oversight bodies that have procedures for receiving and dealing with privacy complaints.

⁷⁰⁶ ACCC, [DPI Report](#) 196.

⁷⁰⁷ Ibid 197.

⁷⁰⁸ Introduced by the [Treasury Laws Amendment \(News Media and Digital Platforms Mandatory Bargaining Code\) Act 2021](#) (Cth).

⁷⁰⁹ ACMA, [News media bargaining code: Eligibility guidelines](#) (July 2022) 7.

⁷¹⁰ Submission to the Discussion Paper: [Guardian Australia](#), 20.

⁷¹¹ [Evidence Act 2008 \(Victoria\)](#), s 126K.

⁷¹² Ibid s 126J.

⁷¹³ Ibid s 126J(2)(d).

⁷¹⁴ [Privacy Act 2020](#) (NZ), s 8(b)(x).

⁷¹⁵ Ibid s 7. A news entity's business must, in whole or part, consist of news activity.

⁷¹⁶ Ibid s 215(2)(b).

A media organisation would not be required to be subject to the oversight of one of those bodies to attract the exemption. A media organisation could develop and publish its own privacy standards. However, the requirement for such standards to be 'adequate' would mean that minimum criteria for what is considered to be adequate privacy standards would be needed.

It is proposed that the OAIC, in consultation with the ACMA, media representative bodies and media organisations, develop and publish criteria for adequate media privacy standards as well as a template privacy standard.⁷¹⁷ These could be developed on an industry basis and may be informed by the ACMA's Privacy Guidelines.⁷¹⁸

These resources may assist media organisations (particularly smaller organisations) with the costs associated with ensuring their privacy standards are adequate. A media organisation could choose to adopt the template privacy standard – but this would not be mandatory; it could choose to draft its own 'adequate' standard.

This proposal bears similarities to one element of the ALRC's recommendation in its Report 108 that the exemption for journalistic acts and practices was important and should be retained, but that media organisations should be committed to 'adequate privacy standards'.⁷¹⁹

In assessing whether a media organisation's privacy standards are adequate, the OAIC would consider, amongst other matters, its process for receiving and dealing with complaints.⁷²⁰ Where an organisation is not covered by the exemption, the OAIC would have jurisdiction to deal with privacy complaints as it does presently.⁷²¹

9.1 To benefit from the journalism exemption a media organisation must be subject to:

- **privacy standards overseen by a recognised oversight body (the ACMA, APC or IMC) or**
- **standards that adequately deal with privacy.**

9.2 In consultation with industry, and the ACMA, the OAIC should develop and publish criteria for adequate media privacy standards and a template privacy standard that a media organisation may choose to adopt.

9.5 Not proposed – change the scope of the exemption

Some submitters proposed limiting the scope of the exemption. As a 'media organisation' may include anyone who maintains a website or a blog, and disseminates information,⁷²² it was submitted that the exemption should focus on protecting professional journalists rather than 'bloggers' or 'citizen journalists',⁷²³ or that the definition of media organisation should include only those organisations whose activities 'predominantly consist of journalism'.⁷²⁴ The NSW Council for Civil Liberties countered in its submission that 'there is no principled reason for drawing a distinction between citizen journalists and those employed by media organisations'.⁷²⁵

717 This was Recommendation 42-4 of [ALRC Report 108](#), 1471.

718 ACMA, [Privacy guidelines for broadcasters](#) (September 2016).

719 [ALRC Report 108](#), [42.21]–[42.22], Recommendation 42-3, 1471. The ALRC also recommended that a definition for journalism be introduced.

720 In [ALRC Report 108](#), the ALRC considered enforcement powers and sanctions to be an important consideration in determining whether a media privacy standard is 'adequate' for the purposes of the journalism exemption, 172 [42.123].

721 This was the process envisaged by the ALRC: [ALRC Report 108](#), [42.83]; Discussion Paper 72, '[Review of Australian Privacy Law](#)' (12 September 2007), [38.89].

722 Submission to the Discussion Paper: [Calabash Solutions](#), 9; [elevenM](#), 23.

723 Submission to the Issues Paper: [Centre for Media Transition, University of Technology Sydney](#), 12-13. See also Submission to Issues Paper: [Cyber Security Cooperative Research Centre](#), 7; Submission to the Discussion Paper: [Calabash Solutions](#), 9.

724 Submission to the Issues Paper: [Michael Douglas, UWA Law School](#), 2. See also Submission to the Discussion Paper: [elevenM](#), 23-24.

725 Submission to the Discussion Paper: [NSW Council for Civil Liberties](#), 14.

The ALRC considered that the capacity for the exemption to apply to organisations outside the mainstream media was an important component of freedom of expression. It concluded that the journalism exemption should not be limited to established media businesses or professional journalists.⁷²⁶

Some submissions called for the definition to be *extended* to include artistic, academic or literary material⁷²⁷ whereas others said that the range of activities covered by the exemption should be more restricted.⁷²⁸

Submitters said that a free and robust media is essential to our democracy.⁷²⁹ However, there were different perspectives on what the exemption should cover. Recognising that journalistic material of public interest may be produced by a range of individuals, and the policy objective of allowing a free flow of information to the public, it is considered preferable to retain the existing definitions. However, a free media must also be responsible – adequate standards must be in place, and recourse available for individuals whose privacy is not sufficiently protected.

9.6 Proposal – review operation of exemption

In addition to submitter concerns about the broad scope of the exemption, submitters were concerned about the adequacy of the existing standards and complaints processes. Calabash Solutions supported oversight measures similar and commensurate to those contained in the UK Data Protection Act, submitting that the self-regulation model could be improved by ensuring it is reviewed frequently (every three years), and by inviting public debate and submissions on the model as part of the review.⁷³⁰ Similarly, the Centre for Media Transition – which proposed an independent industry-based standards scheme – submitted that ‘the standards should be reviewed periodically and this should involve public participation rather than just consultation.’⁷³¹

The UK Data Protection Act contains an exemption for the processing of data for the purposes of journalism. That legislation provides for two reviews of the operation of the exemption: a five-yearly review of the extent to which the processing of personal data for the purposes of journalism complies with data protection law and good practice;⁷³² and a three-yearly review of the use and effectiveness of the media’s dispute resolution processes.⁷³³

It is proposed that a review of the operation of the journalism exemption be conducted by an independent reviewer, appointed by the Attorney-General, commencing in three years. The IC could be directed to undertake this review if Proposal 25.4 (Chapter 25) is enacted.

It is anticipated that such a review could encompass an audit of complaints of alleged privacy breaches arising from acts and practices covered by the exemption, together with an assessment of the effectiveness of the complaint handling processes. It is also proposed that the review consider the extent to which minimum privacy standards have been met by media organisations in the course of journalism, as measured against the criteria for ‘adequate’ standards. A review would provide all stakeholders, including media organisations, an opportunity to provide feedback on the amended exemption. The outcome of the review would inform consideration of any further reforms. Depending on the precise scope and nature of this review, it could be done separate to, or as part of, the statutory review put forward in Proposal 30.1.

Proposal 9.3 An independent audit and review of the operation of the journalism exemption should be commenced three years after any amendments to the journalism exemption come into force.

726 [ALRC Report 108](#), [42.47]–[4.48]. The ALRC considered that adequate limitations were provided through the other requirements it recommended, which included defining journalism and requiring media organisations to publicly commit to privacy standards.

727 Submission to the Discussion Paper: [Nine](#), 3,7; [Commercial Radio Australia](#), 1; [Free TV Australia](#), 8. Content with entertainment value was also proposed.

728 Submission to the Discussion Paper: [NSW Council for Civil Liberties](#), 14. Submission to the Issues Paper: [Centre for Media Transition](#), [University of Technology Sydney](#), 12–13. See also, Submissions to the Discussion Paper: [Calabash Solutions](#), 9; [Privacy 108](#), 14 and Submissions cited above [at footnote 679] which proposed a limited exemption only for activities necessary to the conduct of investigative and public interest journalism.

729 Submission to the Discussion Paper: [Internet Association of Australia](#), 3; [Law Council of Australia](#), 10; [Nine](#): 1–3, 15–17.

730 Submission to the Discussion Paper: [Calabash Solutions](#), 10.

731 Submission to the Discussion Paper: [Centre for Media Transition](#), 9.

732 *Data Protection Act 2018* (UK) s 178.

733 *Ibid* s 179.

9.7 Security and destruction obligations

Many submitters supported applying the security and destruction obligations in APP 11 to acts or practices by media organisations in the course of journalism,⁷³⁴ although media organisations were opposed the idea.⁷³⁵

Submissions said there was no public interest served by the media failing to take reasonable steps to ensure the security of personal information⁷³⁶ and that extending the application of APP 11 to media organisations would not prevent them from undertaking journalism activities, but would reflect the genuine need to instil good digital security practices,⁷³⁷ and reduce the risk of harm to individuals.⁷³⁸

Privacy 108 considered it important that media organisations be held to the same level of responsibility to secure personal information as other entities, submitting that 'the recent ransomware attack impacting Channel 9 makes it clear that even the largest media organisations may not have robust security measures in place to protect the personal and sensitive information they hold'.⁷³⁹

In contrast, stakeholders from the media said there is no basis for applying APP 11 to media organisations engaging in journalism, submitting that there is no evidence of privacy harms that would justify its application.⁷⁴⁰ SBS submitted that it would be unduly burdensome and create practical difficulties.⁷⁴¹ Nine and Free TV submitted that security obligations do not sit well with the role of journalists to disclose facts to the public.⁷⁴² It was submitted that, as certain activities (such as advertising sales) fall outside the journalism exemption, sound security arrangements are already in place for the operations of media organisations as a whole.⁷⁴³

SBS submitted that the obligation to destroy or de-identify personal information pursuant to APP 11.2 would not be in the public interest as information collected by journalists in relation to a story is often of continuing importance to future reporting. 'Stories can develop over many years', it submitted, and 'research collected by a journalist could inform subsequent publications or content on the same issue'.⁷⁴⁴

According to the OAIC, the principles-based nature of APP 11.2 provides sufficient flexibility to accommodate the various needs of a media organisation to retain personal information.⁷⁴⁵ For example, the OAIC submitted that: 'the use of news articles as historical records means that media organisations may justify retention for an extended period of time. This could be explained in OAIC guidance.'⁷⁴⁶ Digital Rights Watch also considered that it was reasonable that media organisations dispose of personal information that they are no longer using, submitting that it was an important measure to decrease the risk of a data breach or other privacy harms to individuals in the future.⁷⁴⁷

Some media organisations are already required to comply with certain security obligations through the privacy standards to which they subscribe, such as the APC's Statement of Privacy Principles which require a media organisation to 'take reasonable steps to ensure that the personal information it holds is protected from misuse, loss, or unauthorised access'.⁷⁴⁸

9.7.1 Proposal – apply security and destruction obligations

It is proposed that APP 11 apply to all media organisations, including for acts and practices in the course of journalism. This would ensure uniform security obligations apply to media organisations and bring them into line with other APP entities, affording greater protection to the public. OAIC guidance should clarify that the destruction requirement should apply where information is no longer needed for the purposes of journalism.

⁷³⁴ For example, Submissions to the Discussion Paper: [Internet Association of Australia](#), 3; [Social Services Portfolio](#), 18; [OAIC](#), 63; [Privacy 108](#), 14; [Digital Rights Watch](#), 20; [elevenM](#), 23; [Salinger Privacy](#), 19; [Electronic Frontiers Australia](#), 8; [Australian Communications Consumer Action Network](#), 8.

⁷³⁵ Submissions to the Discussion Paper: [SBS](#), 11-12; [Guardian Australia](#), 20; [Free TV Australia](#), 12; [Nine](#), 7. See also submissions to the Discussion Paper: [Commercial Radio Australia](#); [ARTK](#) and [ABC](#) which opposed any narrowing of the existing exemption.

⁷³⁶ Submission to the Discussion Paper: [elevenM](#), 23.

⁷³⁷ Submission to the Discussion Paper: [Digital Rights Watch](#), 20.

⁷³⁸ Submission to the Discussion Paper: [Calabash Solutions](#), 10.

⁷³⁹ Submission to the Discussion Paper: [Privacy 108](#), 14.

⁷⁴⁰ Submission to the Discussion Paper: [Guardian Australia](#), 20; [SBS](#), 11; [Free TV Australia](#), 12.

⁷⁴¹ Submission to the Discussion Paper: [SBS](#), 11-12.

⁷⁴² Submissions to the Discussion Paper: [Nine](#), 7; [Free TV Australia](#), 12.

⁷⁴³ Submission to the Discussion Paper: [Free TV Australia](#), 12; [Nine](#), 7.

⁷⁴⁴ Submission to the Discussion Paper: [SBS](#), 12.

⁷⁴⁵ Submission to the Discussion Paper: [OAIC](#), 63.

⁷⁴⁶ Submission to the Discussion Paper: [OAIC](#), 63.

⁷⁴⁷ Submission to the Discussion Paper: [Digital Rights Watch](#), 20.

⁷⁴⁸ Australian Press Council, [Statement of Privacy Principles](#) (December 2015) Privacy Principle 4, quoted in Submission to the Discussion Paper: [OAIC](#), 62.

While media organisations would incur some financial and operational costs in extending security measures to activities that are currently exempt,⁷⁴⁹ these are unlikely to be unduly burdensome for those media organisations that are covered by the Act in respect of activities not covered by the journalism exemption.⁷⁵⁰ Additional OAIC guidance and support would also assist organisations to comply, particularly small businesses if the small business exemption is modified or removed.

9.7.2 Proposal – apply modified Notifiable Data Breach reporting obligations

Submissions to the Discussion Paper highlighted that, as a corollary to the security requirements in APP 11, compliance with the NDB reporting obligations are an important component of entities' data security practices.⁷⁵¹ The Discussion Paper noted that the UK Data Protection Act, which has a data protection notification scheme, applies modified reporting obligations where an entity reasonably believes that notifying an individual affected by a data breach would be incompatible with journalism.⁷⁵²

The OAIC submitted that a similar approach to the UK could be adopted, so that an organisation would notify the OAIC of the eligible data breach but need not notify the affected individual 'where they meet the criteria of the journalism exemption and reasonably believe that notification to the individual would be incompatible with journalism.'⁷⁵³ SBS did not support the extension of data breach notification requirements to journalism, but submitted that if the NDB scheme was to be applied the approach taken in the UK should be considered.⁷⁵⁴

elevenM and SBS contemplated situations in which notifying an affected individual of a data breach might affect public interest investigative journalism.⁷⁵⁵ elevenM considered it possible that, in such cases, 'the public interest in preserving the secrecy of the investigation pending its completion may outweigh the interest of affected individuals in being notified,' and proposed that notification to affected individuals be *delayed* in such cases.⁷⁵⁶

A modified version of the NDB scheme should apply to acts and practices in the course of journalism. The NDB provisions require eligible data breaches to be notified to the OAIC and individuals affected by the breach. The NDB scheme should be modified in line with the UK approach, to take account of situations where directly reporting a breach to an individual is incompatible with journalism.

9.4 Require media organisations to comply with security and destruction obligations in line with the obligations set out in APP 11.

9.5 Require media organisations to comply with the reporting obligations in the NDB scheme. There will need to be some modifications so that a media organisation would not need to notify an affected individual if the public interest in journalism outweighs the interest of affected individuals in being notified.

749 Submission to the Discussion Paper: [Calabash Solutions](#), 10.

750 Submission to the Discussion Paper: [OAIC](#), 63.

751 Submissions to the Discussion Paper: [OAIC](#), 216; [Social Services Portfolio](#), 33; [ADIA](#), 9.

752 GDPR, art 34; *Data Protection Act 2018* (UK), sch 2, pt 5, sub-para 26(9)(c)(i). See [Discussion Paper](#), 65.

753 Submission to the Discussion Paper: [OAIC](#), 62.

754 Submission to the Discussion Paper: [SBS](#), 12.

755 Submission to the Discussion Paper: [elevenM](#), 23; [SBS](#), 12.

756 Submission to the Discussion Paper: [elevenM](#), 23.

Contents | Part 2:

10.	Privacy policies and collection notices	94
11.	Consent and online privacy settings	102
12.	Fair and reasonable test	110
13.	Additional protections	122
14.	Research	133
15.	Organisational accountability	140
16.	Children's privacy	146
17.	People experiencing vulnerability	158
18.	Rights of the individual	166
19.	Automated decision-making	188
20.	Direct marketing, targeting and trading	194
21.	Security, Destruction and Retention of Personal Information	221
22.	Controllers and processors of personal information	230
23.	Overseas data flows	234
24.	Cross-Border Privacy Rules and domestic certification	247

Part 2: Protections

10. Privacy policies and collection notices

A large number of submitters considered that collection notices and privacy policies play a crucial role in fostering transparency over entities' personal information handling practices.⁷⁵⁷ The OAIC submitted that the transparency provided by privacy policies and collection 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.⁷⁵⁸

However, submissions also expressed concern that many privacy policies and collection notices are complex, lengthy, legalistic and vague, which can undermine individuals' understanding of how their personal information will be handled.⁷⁵⁹ The *Digital Platforms Inquiry's* assessment of large online platforms found that lengthy and complex privacy policies were common, and that many employed ambiguous descriptions of how user data is handled and were difficult to navigate.⁷⁶⁰

The Discussion Paper sought feedback on several proposals that would encourage the development of clearly expressed collection notices and require the provision of collection notices in a greater range of circumstances, in order to improve the transparency of personal information handling and reduce information asymmetries between APP entities and individuals.

10.1 The current law

10.1.1 Privacy policies – APP 1

APP 1 requires entities to maintain a 'clearly expressed' and 'up-to-date' privacy policy that addresses the matters listed in APP 1.4.⁷⁶¹ The APP Guidelines indicate that a 'clearly expressed' privacy policy should be 'easy to understand (avoiding jargon, legalistic and in-house terms), easy to navigate, and only include information that is relevant to the management of personal information by the entity'.⁷⁶² An APP entity should regularly review and update its privacy policy to ensure that it reflects the entity's information handling practices, such as part of an entity's annual planning processes.⁷⁶³

The APP entity must take such steps as are reasonable in the circumstances to make its privacy policy available free of charge and 'in such form as is appropriate'.⁷⁶⁴ Where an individual requests a privacy policy in a particular form, the APP entity must take reasonable steps to accommodate that request.⁷⁶⁵ APP entities are generally expected to make a privacy policy available by publication on a website.⁷⁶⁶ Where it is foreseeable that the privacy policy may be accessed by individuals with accessibility needs, or where individuals request a copy of the privacy policy in an accessible form, appropriate accessibility measures should be put in place.⁷⁶⁷

10.1.2 Collection notices – APP 5

APP 5 requires entities to take such steps (if any) as are reasonable in the circumstances to notify individuals about the collection of their personal information. The collection notice must be provided at or before the time an APP entity collects personal information (or as soon as practicable afterwards) and must address the matters listed in APP 5.2, or 'otherwise ensure that the individual is aware' of those matters.⁷⁶⁸

The APP Guidelines provide examples of 'reasonable steps' that an APP entity could take to notify or ensure awareness of the APP 5 matters, including prominent display of the matters in a sign-up form, providing a readily accessible link to an APP 5 notice or verbal communication of the matters over a telephone call.⁷⁶⁹ The APP Guidelines acknowledge that in certain circumstances, it may not be reasonable to provide notice to an individual, such as where:

757 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](#), 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.

758 Submission to the Issues Paper: [OAIC](#), 68.

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

760 ACCC, [DPI Report](#) 401–407.

761 Privacy Act sch 1, APP 1.3–1.4.

762 OAIC, [APP Guidelines](#) (July 2019) [1.8].

763 Ibid [1.9].

764 Privacy Act sch 1, APP 1.5.

765 Ibid APP 1.6.

766 Ibid APP 1.5. See also, OAIC, [APP Guidelines](#) (July 2019) [1.37]–[1.38]. OAIC guidance notes that '[o]nline publication may not be appropriate in some circumstances, for example, where the APP entity does not have an online presence or, where individuals who regularly interact with the entity may not have internet access' and suggests alternative means of delivering a privacy policy at [1.38].

767 OAIC, [APP Guidelines](#) (July 2019) [1.36]–[1.37], [1.41].

768 Privacy Act sch 1, APP 5.1.

769 OAIC, [APP Guidelines](#) (July 2019) [5.6].

- the individual is already aware of the APP 5 matters
- an entity collects personal information from an individual on a recurring basis in relation to the same matter, and there has been no material change in the nature of the collection
- notification may pose a serious threat to life, health or safety
- notification may jeopardise the purpose of collection or the integrity of the personal information collected and there is a clear public interest in the purpose of collection
- notification would be inconsistent with another legal obligation, or
- the impracticability of notification, including the time and cost, outweighs the benefit of notification.⁷⁷⁰

The APP Guidelines further note that ‘it may be reasonable for an entity to notify some but not all of the APP 5 matters’ such as where the collecting entity’s identity is obvious from the circumstances.⁷⁷¹

10.2 The interaction between privacy policies and collection notices

Telstra considered that the current wording of APP 5 is logistically challenging and that ‘many large entities instead provide notice of the relevant matters in the form of their privacy policy, which generally contains all information required in an APP 5 notice at a high level.’⁷⁷² 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.⁷⁷³ ResMed submitted that the requirement to provide an APP 5 collection notice and maintain an APP 1 privacy policy is duplicative and unique amongst international data protection laws.⁷⁷⁴

However, other submissions highlighted the benefits of maintaining both APP 1 and APP 5, and considered that the two principles play distinct roles. Professor Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise submitted that APP 5 collection notices have the objective of *enabling consumer decision-making* for a *particular collection*, and therefore should be designed to be accessible, readable and succinct for the average consumer. By contrast, long-form privacy policies play an important role in *facilitating regulatory monitoring*. In their view, privacy policies ‘can and should remain detailed’ as detailed information enables regulatory monitoring by expert intermediaries (such as civil society groups and researchers) and privacy and consumer protection law regulators, even though they are likely to ‘remain unread by the vast majority of consumers.’⁷⁷⁵ The NSW Council for Civil Liberties noted that the provision of detailed and actionable information ‘is particularly important in allowing expert intermediaries, such as privacy advocates, to obtain sufficient information to inform non-experts of the effects of data practices.’⁷⁷⁶

The OAIC also observed that APP 5 collection notices should contain information that is relevant to the *particular collection* of personal information, and has the purpose of facilitating individuals’ privacy self-management. By contrast, APP 1 privacy policies provide high-level information to the world at large about how an organisation *generally* handles personal information.⁷⁷⁷

On this basis, it is proposed that both APP 1 privacy policies and APP 5 collection notices should be retained, as each serves a distinct and important function. An APP 1 privacy policy is necessary at all times and covers the entity’s entire personal information handling practices. It facilitates monitoring of compliance and is valuable for particularly concerned individuals, civil society groups, researchers or regulators. On the other hand, APP 5 collection notices, when required, should be concise, easy for the average consumer to understand, and should only contain information that is relevant to the particular collection of personal information.

Existing APP Guidelines clarify the circumstances in which APP entities may consider providing individuals with a hyperlink to a privacy policy in order to fulfil their notification obligations under APP 5.⁷⁷⁸ In the 7-Eleven determination, the IC also clarified that mere publication of a ‘privacy policy on a website does not amount to compliance with APP 5’ and that in the case at hand, it was not reasonable to assume that customers would have searched for the respondent’s Privacy Policy online and read through it before entering the store.⁷⁷⁹ It was further noted that 7-Eleven should have included a collection notice on, or in the vicinity of, the tablet screen prior to the collection of biometric data.⁷⁸⁰

⁷⁷⁰ Ibid [5.7].

⁷⁷¹ Ibid [5.8].

⁷⁷² Submission to the Discussion Paper: [Telstra](#), 12–13. See also, [ResMed](#), 3.

⁷⁷³ Submission to the Issues Paper: [ANZ](#), 7.

⁷⁷⁴ Submission to the Discussion Paper: [ResMed](#), 3.

⁷⁷⁵ Submission to the Discussion Paper: [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 18. See relatedly, [Privcore](#), 3.

⁷⁷⁶ Submission to the Discussion Paper: [New South Wales Council for Civil Liberties](#), 15.

⁷⁷⁷ Submission to the Issues Paper: [OAIC](#), 69; Submission to the Discussion Paper: [OAIC](#), 67–68. See relatedly, [Privcore](#), 3.

⁷⁷⁸ [OAIC](#), [APP Guidelines](#) (July 2019) [5.5].

⁷⁷⁹ 7-Eleven [Determination](#), [120]–[122]. See, Submission to the Discussion Paper: [OAIC](#), 66.

⁷⁸⁰ Ibid [122].

10.3 Clear collection notices

Unlike APP 1, there is no legislative requirement in APP 5 that requires collection notices to be clear or up-to-date, although the APP Guidelines encourage entities to ensure the matters are ‘expressed clearly.’⁷⁸¹ The Discussion Paper proposed that APP 5 be updated to require collection notices to be ‘clear, current and understandable.’

Submitters were largely supportive of the proposal on the basis that it would enhance the clarity of APP 5 collection notices⁷⁸² and would encourage entities to develop them in a user-friendly, interactive and visually engaging way.⁷⁸³ The OAIC submitted that APP entities would need to consider the appropriate length of their APP 5 notice in order to comply with the requirements for notices to be clear and understandable.⁷⁸⁴ It was noted that the proposal bears similarities to equivalent requirements in overseas jurisdictions, including Europe’s GDPR.⁷⁸⁵

The Australian Banking Association, SBS and ANZ sought clarification about the possible interpretation of ‘current’ and whether this would impose a standard review period over collection notices even where no circumstances have changed.⁷⁸⁶ It was suggested that the term ‘current’ is ambiguous⁷⁸⁷ and that in the context of ongoing collections of personal information, it could mean a:

- notice continues to be accurate
- notice is updated at regular intervals, or
- notice is provided at each collection.⁷⁸⁸

ANZ proposed that in the context of ongoing collections of personal information over a long period of time, such as a banking relationship, notice provided when the relationship commences should be considered ‘current’ while it continues to be accurate, in order to avoid notice fatigue.⁷⁸⁹ The OAIC submitted that a requirement for collection notices to be ‘current’ should require ‘APP entities to update their documentation when their practices change, such as information being used for a new purpose.’⁷⁹⁰ In light of this feedback, an alternative could be to use the term ‘up-to-date’ instead of ‘current’ to more clearly convey the intention that collection notices procedures would only need to be updated when practices change. The term ‘up-to-date’ would also achieve greater alignment with the existing requirements of APP 1.3.

Some suggested that the test be expanded to also require that APP 5 notices be ‘concise’,⁷⁹¹ made available in languages other than English, and accessible for those experiencing disability.⁷⁹² It is considered that the term ‘concise’ would clarify the role of the APP 5 notification process as distinct from APP 1 privacy policies. The term ‘understandable’ would accommodate notification in other languages where appropriate and would require the use of plain language.⁷⁹³ Similar to the obligations for privacy policies, where individuals request a copy of a privacy notice in accessible form, appropriate accessibility measures should be put in place.

The proposed changes would retain the principles-based approach of the Privacy Act⁷⁹⁴ and would be flexible enough to permit different approaches across sectors. The requirements could also be supported through the use of APP codes for particular sectors or personal information-handling practices, or Commissioner-issued guidelines.⁷⁹⁵

781 OAIC, [APP Guidelines](#) (July 2019) [5.5].

782 Submissions to the Discussion Paper: [OAIC](#); [Australian Banking Association](#); [New South Wales Information and Privacy Commission](#); [Electronic Frontiers](#); [Office of the Victorian Information Commissioner](#); [Salinger Privacy](#); [Foundation for Alcohol Research and Education](#); [Deloitte Australia](#); [New South Wales Council for Civil Liberties](#); [Snap Inc](#); [Consumer Policy Research Centre](#); [Privacy 108](#); [Obesity Policy Coalition](#); [Australian Institute of Health and Welfare](#); [National Australia Bank](#); [Department of Health \(Cth\)](#); [Helen Gregorczyk, University of Queensland](#); [Google](#); [Australian Privacy Foundation](#); [Equifax](#).

783 Submissions to the Discussion Paper: [OAIC](#), 66-7; [Deloitte Australia](#), 15.

784 Submission to the Discussion Paper: [OAIC](#), 67.

785 Submissions to the Discussion Paper: [AANA 3](#); [New South Wales Information and Privacy Commission](#), 3. GDPR art 12(1) requires communications to the data subject to be presented in a ‘concise, transparent, intelligible and easily accessible form, using clear and plain language.’ See also, Bill C-27 s 62(1) which requires privacy policies to be readily available and in ‘plain language’.

786 Submissions to the Discussion Paper: [Australian Banking Association](#), 13; [SBS](#), 19; [ANZ](#), 13.

787 Submission to the Discussion Paper: [SBS](#), 19.

788 Submission to the Discussion Paper: [ANZ](#), 13.

789 Ibid.

790 Submission to the Discussion Paper: [OAIC](#), 67.

791 Submission to the Discussion Paper: [UNSW Allens Hub](#), [Deakin CSRI and IEEE SSIT](#), 8.

792 Submissions to the Discussion Paper: [Kimberlee Weatherall](#), [Tom Manousaridis and Melanie Trezise](#), 17; [Benevolent Society](#), 3.

793 See relatedly, Submission to the Discussion Paper: [ANZ](#), 13; [New South Wales Council for Civil Liberties](#), 15.

794 Submission to the Discussion Paper: [OAIC](#), 67.

795 Ibid. See also, [Discussion Paper](#), 69.

10.1 Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise, and understandable. Appropriate accessibility measures should also be in place.

10.4 The contents of privacy policies and collection notices

The Discussion Paper proposed to reduce the number of matters that must be addressed in an APP 5 collection notice. The intent of this proposal was to promote concise APP 5 collection notices, by limiting their contents to information that would be most pertinent to an individual's decision-making at the point of collection.⁷⁹⁶ The Discussion Paper suggested that the matters set out in APP 5.2(c), (e), (i) and (j) could be moved into APP 1.4, and that collection notices could also address the types of personal information collected, as well as the purposes for which the entity may use or disclose that personal information. At present, the APPs provide that the following matters must be addressed in an APP 1 privacy policy and APP 5 notification, respectively:

APP 1 – Privacy Policy	APP 5 – Collection Notice
<p>An APP privacy policy must be 'about the management of personal information' by the entity, and must address:</p> <ul style="list-style-type: none"> a) The kinds of personal information that the entity collects and holds b) How the entity collects and holds personal information c) The purposes for which the entity collect, holds, uses and discloses personal information d) How an individual may access personal information that is held by the entity and seek the correction of such information e) How an individual may complain about a breach of the APPs, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint f) Whether the entity is likely to disclose personal information to overseas recipients, and g) If the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy. 	<p>APP entities must take such steps as are reasonable in the circumstances to notify, or ensure that the individual is aware of, the following matters:*</p> <ul style="list-style-type: none"> a) The identity and contact details of the entity b) Where the entity collects personal information from someone other than the individual or where the individual may not be aware of the collection—the circumstances of that collection c) If the collection is legally required or authorised—the fact that collection is required or authorised and details of the legal requirement or authorisation d) The purposes for which the entity collects the personal information e) Consequences for the individual if all or some of the personal information is not collected f) Other entities or persons, or types of entities or persons, to which the entity usually discloses the personal information g) That the APP privacy policy contains details on how to make access and correction requests h) That the APP privacy policy contains details on how to lodge a complaint i) Whether the entity is likely to disclose personal information to overseas recipients, and j) If the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification. <p><i>* It may be reasonable in the circumstances for an entity to notify of some but not all of the APP 5 matters.⁷⁹⁷</i></p> <p><i>** Matters in bold were those that the Discussion Paper proposed could be shifted into privacy policies.</i></p>

⁷⁹⁶ Ibid, 70.

⁷⁹⁷ OAIC, [APP Guidelines](#) (July 2019) [5.8].

Many were supportive of the proposal for a shortened list of matters⁷⁹⁸ and considered that the removed matters could be better addressed in a privacy policy. The Australian Banking Association noted that the extensive list of matters that currently require notification under APP 5.2 often results in transparent but lengthy notices which individuals are less likely to read.⁷⁹⁹

However, other submissions expressed concern about the proposed removal of some matters from APP 5.2.⁸⁰⁰ KPMG and the OAIC submitted that collection notices should continue to disclose whether a collection of personal information is required or authorised by law, and whether the APP entity is likely to disclose personal information to overseas recipients.⁸⁰¹ The OAIC considered that these matters may inform an individual's decision as to whether they wish to engage with a service.⁸⁰²

In light of submitters' concerns about the removal of APP 5.2 (c) and (i),⁸⁰³ it is considered that on balance, the benefits of this proposal do not outweigh the challenges this proposal could raise.

The OAIC acknowledged that the list of matters to be notified under APP 5.2 is lengthy, but considered that 'APP 5 only requires APP entities to take reasonable steps to notify the individual of such matters referred to in subclause 5.2' which provides a degree of flexibility in the principle and 'allows APP entities to limit notice to what is needed in the circumstances.'⁸⁰⁴ On this basis, many APP entities would not provide notice of all matters in APP 5.2. For example, some entities are not legally required or authorised to collect personal information, or may not disclose personal information overseas, and would not be required to address these in a collection notice. Furthermore, the Review notes that existing OAIC guidance clarifies that an APP 5 notice does not need to include 'internal purposes that form part of normal business practices, such as auditing, business planning, billing or de-identifying personal information.'⁸⁰⁵ In addition, Proposals 10.1 and 10.3 of this chapter may assist to encourage entities to develop simple and concise collection notices.

Some submissions suggested that APP 5.2 could focus on 'unusual' or 'unexpected' forms of personal information handling on the basis that individuals mostly want to know whether the entity is using their information for anything unusual, high risk or intrusive.⁸⁰⁶ It is considered that entities should be required to disclose in a collection notice whether they undertake a high privacy risk activity, as described in Chapter 13. APP 5.2 currently requires notification of the existence of access and correction requests,⁸⁰⁷ and it is considered that this should be extended to encompass the new individual rights proposed in Chapter 18, and withdrawal of consent, erasure and objection.⁸⁰⁸

798 Submissions to the Discussion Paper: [Australian Banking Association](#); [Electronic Frontiers](#); [Salinger Privacy](#); [Foundation for Alcohol Research and Education](#); [Deloitte Australia](#); [New South Wales Council for Civil Liberties](#); [Consumer Policy Research Centre](#); [Experian Australia](#); [Obesity Policy Coalition](#); [Atlassian](#); [Australian Council on Children and the Media](#); [Australian Privacy Foundation](#); [Equifax](#).

799 Submission to the Discussion Paper: [Australian Banking Association](#), 13.

800 Submissions to the Discussion Paper: [KPMG](#), 15; [OAIC](#), 68-69; [Department of Health \(Cth\)](#), 7.

801 Submissions to the Discussion Paper: [KPMG](#), 15; [OAIC](#), 68-69.

802 Submission to the Discussion Paper: [OAIC](#), 68-69.

803 Submissions to the Discussion Paper: [KPMG](#), 15; [OAIC](#), 68-69; [Department of Health \(Cth\)](#), 7.

804 Ibid 69.

805 Submission to the Discussion Paper: [OAIC](#), 69; [OAIC](#), [APP Guidelines](#) (July 2019) [5.16].

806 Submission to the Discussion Paper: [ADMA](#), 17; [Guardian Australia](#), 14.

807 Privacy Act sch 1, APP 5.2(g).

808 See relatedly, Submission to the Discussion Paper: [OAIC](#), 69.

10.2 The list of matters in APP 5.2 should be retained. OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the individual in the circumstances, need to be addressed in a notice.

The following new matters should be included in an APP 5 collection notice:

- **if the entity collects, uses or discloses personal information for a high privacy risk activity —the circumstances of that collection, use or disclosure**
- **that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and**
- **the types of personal information that may be disclosed to overseas recipients.**

Note: See Chapter 18 (Rights of the individual), Chapter 19 (Automated decision-making), Chapter 21 (Security, retention and destruction) for additional matters that would be required to be addressed in a privacy policy.

10.5 Standardisation of privacy policies and collection notices

The Discussion Paper proposed that standardised collection notices be considered in the development of an APP code, such as the Online Privacy Code ('OP Code'),⁸⁰⁹ which could include the standardisation of layouts, terminology and privacy icons. Standardised information delivery has been used successfully in other regulatory contexts, including the use of standardised food nutrition tables⁸¹⁰ and standardisation would 'allow consumers to develop expertise in reviewing and understanding the scope of collection policies.'⁸¹¹ It was suggested that consumer comprehension testing would be important to ensure that standardisation is effective⁸¹² and that the standardisation process be industry led.⁸¹³

Submitters were highly supportive of the proposal and considered that it would simplify compliance for APP entities and would assist individuals to understand the content of collection notices.⁸¹⁴ The OAIC submitted that standardised collection notices would make it easier for individuals to compare different services.⁸¹⁵ The Consumer Policy Research Centre submitted that as part of implementation, the Government should undertake comprehensive consumer experience research using representative samples of the Australian population (including varying levels of digital literacy).⁸¹⁶ Some submissions observed that standardisation would make collection notices more structured, and therefore more readily machine readable, and that innovators could develop tools that automatically analyse notices so that people can be alerted to elements that are contrary to their interests or preferences.⁸¹⁷ Several stakeholders submitted that standardised notices should be voluntary for an initial period, so that their effectiveness can be reviewed before determining whether they should be mandatory.⁸¹⁸

809 See, Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth) sch 1.

810 [Discussion Paper](#), 70.

811 Submission to the Issues Paper: [CAIDE and MLS](#), 6.

812 ACCC, [DPI Report](#) 463.

813 Submission to the Discussion Paper: [OAIC](#), 70.

814 Submissions to the Discussion Paper: [AANA](#); [Australian Banking Association](#); [Electronic Frontiers](#); [KPMG](#); [Salinger Privacy](#); [Foundation for Alcohol Research and Education](#); [Deloitte Australia](#); [New South Wales Council for Civil Liberties](#); [Dr Henry Fraser](#); [Consumer Policy Research Centre](#); [Experian Australia](#); [OAIC](#); [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#); [Obesity Policy Coalition](#); [Australian Institute of Health and Welfare](#); [Department of Health \(Cth\)](#); [Australian Council on Children and the Media](#); [Fintech Australia](#); [Australian Privacy Foundation](#).

815 Submission to the Discussion Paper: [OAIC](#), 70.

816 Submission to the Discussion Paper: [Consumer Policy Research Centre](#), 3.

817 Submissions to the Discussion Paper: [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 17. See also, [Dr Henry Fraser](#), 4; [OAIC](#), 70.

818 Submissions to the Discussion Paper: [Australian Banking Association](#), 14; [National Australia Bank](#), 4.

International data protection laws also contemplate the future development of standardised privacy notices or methods through which individuals may exercise privacy rights, including the GDPR⁸¹⁹ and the *California Consumer Privacy Act of 2018* (CCPA).⁸²⁰ New Zealand's Privacy Commissioner has developed a Privacy Statement Generator, which enables entities to quickly create a privacy policy in a standardised template.⁸²¹ The UK ICO has developed detailed guidelines on the methods by which entities can provide privacy information, which includes the use of just-in-time notices and privacy icons.⁸²² In 2021, Italy's data protection authority ran a public design competition for privacy icons for the purposes of privacy notices under Articles 13 and 14 of the GDPR, and has released the winning entries for public use under Creative Commons.⁸²³

As noted in the Discussion Paper, it is impractical to develop one standardised template, lexicon or icon for use across *all* APP entities due to the wide range of contexts in which the Act applies. For example, the collection notice methods of an online retailer, government agency, medical practitioner or closed-circuit television (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. Instead, standardised templates should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. Standardised templates would assist online retailers to draft collection notices and enable an individual to more easily engage with detail in a familiar presentation, while a similar but simple single-sided poster structure with clear icons or diagrams might be more helpful for a CCTV operator's more limited purposes. Standardisation could take place through OAIC guidance, which could provide standardised templates and layouts, and provide guidance on standardised terminology and icons.⁸²⁴ Consideration could also be given to mandating standardised notices in future APP codes that may apply to particular sectors or personal information-handling practices.

It is considered that this proposal to standardise communication with individuals should be expanded to encompass privacy policies, in addition to APP 5 collection notices.

10.3 Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP Codes that may apply to particular sectors or personal information-handling practices.

819 GDPR art 12(7). The European Commission is empowered to set out how to provide standardised icons, and what those icons should represent, though has yet to commence this work.

820 CCPA §§ 1798.185(a)(4)(c).

821 New Zealand Office of the Privacy Commissioner, '[Privacy Statement Generator](#)' (Web Page).

822 UK ICO, '[The Right to Be Informed](#)' (Web Page, March 2018).

823 European Data Protection Board, '[The Italian DPA launches a contest calling for creative ideas from all quarters](#)' (Web Page, 14 April 2021); Garante Per La Protezione Dei Dati Personali (Italy), '["Transparent Information": winners of the contest launched by Italian SA announced](#)' (Web Page, 15 December 2021).

824 See for example UK ICO, '[The Right to Be Informed](#)' (Web Page, March 2018).

10.6 The circumstances in which notice is required

The *Digital Platforms Inquiry* recommended that all collections of personal information be accompanied by a collection notice (whether directly from the consumer or indirectly as a third party), unless the individual already has the information or an overriding legal or public interest reason applies.⁸²⁵

On this basis, the Discussion Paper proposed that APP 5 be amended to require notice under APP 5 unless the notification would be ‘impossible’ or would involve ‘disproportionate effort.’ It was considered that the proposal could require APP 5 notices to be provided in a greater range of circumstances, including indirect collections, though the Discussion Paper sought feedback on whether the proposal would result in any practical difference from the existing ‘reasonable steps’ test in APP 5.1.⁸²⁶

Submissions provided mixed views on the merits of the proposal. Supportive submissions were of the view that the proposal would place a more stringent obligation on APP entities to notify, which would increase the transparency of indirect personal information collections.⁸²⁷

Some submitters considered that the exception would not result in any material difference to the current principle,⁸²⁸ which requires entities to take ‘such steps (if any) as are reasonable in the circumstances’. The Office of the Victorian Information Commissioner submitted that the proposed wording would indicate that ‘in some circumstances, providing a collection notice to an individual may not be practicable or feasible’ which would have ‘the same or similar effect as the existing requirements in practice.’⁸²⁹

Other submitters opposed the proposal on the basis that ‘impossible’ and ‘disproportionate effort’ was too high a bar to meet.⁸³⁰ It was suggested that the proposed wording would not exempt notice in circumstances where notification would compromise a public interest, and some thought that legislative exceptions that reflect the APP Guidelines would be required should the proposal proceed.⁸³¹ The OAIC noted that the current requirement for entities to take ‘such steps (if any) as are reasonable in the circumstances’ creates a flexible requirement without the need for specific exceptions to the notification requirement.⁸³² On this basis, the OAIC recommended maintaining the existing wording of APP 5.1.

In October 2021, APP 5.1 was considered in the context of the personal information handling practices of Clearview AI, Inc (Clearview), who collected biometric information from third party sources using an automated image scraper.⁸³³ While this information was not collected directly from individuals, the IC determined that Clearview was required to take more rigorous steps to notify under APP 5 noting ‘the sensitivity of the information collected and potential adverse consequences for individuals as a result of the collection.’⁸³⁴

The APP Guidelines also provide 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.’⁸³⁵ The APP Guidelines further note that where an entity ‘collects personal information from another entity’, it may be a reasonable step to ensure ‘that the other entity has notified or made the individual aware of the relevant APP 5 matters on its behalf (such as through an enforceable contractual arrangement).’⁸³⁶ Given the existing provision in APP 5.1 has been applied to require notice even where an entity collects personal information from third party sources, there is little merit in proceeding with Proposal 8.4 of the Discussion Paper.

⁸²⁵ ACCC, [DPI Report](#) Recommendation 16(b).

⁸²⁶ [Discussion Paper](#), 73.

⁸²⁷ Submissions to the Discussion Paper: [Deloitte Australia](#); [New South Wales Information and Privacy Commission](#); [Electronic Frontiers](#); [Salinger Privacy](#); [Foundation for Alcohol Research and Education](#); [Australian Council on Children and the Media](#); [Australian Privacy Foundation](#).

⁸²⁸ Submissions to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 4-5. See also, [Obesity Policy Coalition](#), 6.

⁸²⁹ Submission to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 4-5.

⁸³⁰ Submissions to the Discussion Paper: [Australian Banking Association](#), 14-15; [Free TV Australia](#), 33-34; [Experian Australia](#), 10; [Insurance Council of Australia](#), 9; [Meta](#), 26. See also, [KPMG](#), 15.

⁸³¹ Submissions to the Discussion Paper: [Telstra](#), 13; [OAIC](#), 71; [Privacy 108](#), 16-17. See relatedly, [Free TV Australia](#), 33-34; [Ai Group](#), 9.

⁸³² Submission to the Discussion Paper: [OAIC](#), 70-71.

⁸³³ Clearview [Determination](#).

⁸³⁴ *Ibid* [188]–[189].

⁸³⁵ OAIC, [APP Guidelines](#) (July 2019) [5.2].

⁸³⁶ *Ibid* [5.6].

11. Consent and online privacy settings

The Discussion Paper sought feedback on whether consent to information-handling should be obtained in additional circumstances⁸³⁷ and whether it should be further defined in the Act.

11.1 The current law

Consent is currently only required under the Act for a limited range of collections, uses and disclosures of personal information. Unless an exception applies, consent is needed to collect sensitive information,⁸³⁸ and may also allow APP entities to use or disclose personal information for a secondary purpose.⁸³⁹ 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,⁸⁴⁰ or as a basis for cross-border disclosures of personal information.⁸⁴¹

The current definition of consent in the Act states that consent can be express or implied.⁸⁴² 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 it be informed, voluntary, current and specific, and 'the individual has the capacity to understand and communicate their consent'. The following guidance is given 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...⁸⁴³

11.2 Should consent be required in additional circumstances?

The DPI Report recommended that consent be required for any collection, use or disclosure of personal information, unless the personal information is necessary for performance of a contract, for compliance with a legal requirement, or is otherwise necessary for a public interest reason.⁸⁴⁴

Submissions to this Review generally opposed giving consent a more prominent role in authorising personal information handling under the Act.⁸⁴⁵ There was broad agreement that while consent is an important mechanism, it is most effective when used in a narrow range of situations where individuals most need to exert control over their personal information.⁸⁴⁶ Submissions to the Discussion Paper have noted that:⁸⁴⁷

- requiring consent in additional circumstances would lead to '*consent fatigue*': where individuals are overwhelmed with the number of consent requests that they receive, and are less able to effectively engage with those consents

837 See, ACCC, [DPI Report](#) Recommendation 16(c).

838 Privacy Act 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.

839 Ibid APP 6.1(a).

840 Ibid APP 7.3, 7.4.

841 Ibid APP 8.2.

842 Ibid s 6.

843 OAIC, [APP Guidelines](#) (July 2019) [B.40]–[B.42].

844 ACCC, [DPI Report](#) Recommendation 16(c).

845 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](#), 22; [Telstra Corporation Ltd and Telstra Health Pty Ltd](#), 9; [Association for Data-driven Marketing & Advertising \(ADMA\)](#), 17; [Experian](#), 11; [elevenM](#), 2; [New South Wales Council for Civil Liberties](#), 8; [Professor Kimberlee Weatherall](#), 6–8; [Privacy 108](#), 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.

846 Ibid.

847 Submissions to the Discussion Paper: [OAIC](#); [Office of the Victorian Information Commissioner](#); [The Australia Institute – Centre for Responsible Technology](#); [Australian Banking Association](#); [Consumer Policy Research Centre](#); [Telstra](#); [Snap Inc](#); [FreeTV Australia](#); [IIS Partners & GroundUp Consulting](#); [National Australia Bank](#); [Experian Australia](#). See also, [UNSW Allens Hub](#), [Deakin CSRI and IEEE SSIT](#), [Ramsay Australia](#). See also [Discussion Paper](#), 75.

- consent unreasonably places the *burden of privacy protection on individuals*: where individuals are required to consider complex data handling practices and unknown privacy harms that may materialise in the future rather than being able to be confident that the collection, use or disclosure will not be harmful
- it would be *unnecessarily burdensome on APP entities* to obtain consent in many situations: where a collection, use or disclosure of personal information would be reasonably expected by the individual or broader community, and
- consent is only meaningful where the individual has a *real choice*: 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.

The OAIC observed that consent is not currently required for ‘routine personal information handling’ and submitted that it should be reserved for high privacy risk situations.⁸⁴⁸ It thought that requiring consent for reasonably expected personal information handling may reduce it to a tick-box exercise which ‘will detract the value of consent in higher-risk situations where it will actually be valuable’.⁸⁴⁹

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 time and energy to dedicate to understanding the specifics of a business’s data handling processes, which ‘should be treated with respect and called upon sparingly’.⁸⁵⁰ Daniel Solove has argued that ‘there are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity’.⁸⁵¹

On this basis, it is not recommended that the Act be changed to increase the circumstances in which consent is required under the Act. Instead, the Review is proposing reforms to require that APP entities handle personal information fairly and reasonably, conduct PIAs before engaging in high privacy risk activities and not engage in certain personal information handling practices that pose significant risk of harm.⁸⁵² The Review is also proposing additional privacy rights, including a right to access and explanation, a right to object and to opt-out of certain data handling practices,⁸⁵³ and a right of erasure which would allow individuals to exercise more control over their personal information beyond the point of collection.

However, in the circumstances where consent is currently required, reforms could be introduced to improve the quality of consent obtained from individuals.

11.3 Valid consent

The ACCC and submitters to the Review have highlighted that some entities may deliberately conceal the nature of their data handling practices or employ choice architecture which influences consumer choice by appealing to certain psychological or behavioural biases, including ‘dark patterns’ which are user interfaces designed to ‘confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions’.⁸⁵⁴ Consents may also be vaguely worded or bundled in such a way⁸⁵⁵ that detracts from the effectiveness of consent, and may prevent individuals from understanding what they are consenting to, or prevent them from exercising choice as between a number of information-handling practices. To address these concerns, the Discussion Paper proposed that valid consent should be defined in the Act as ‘voluntary, informed, current, specific, and an unambiguous indication through clear action’.⁸⁵⁶

848 Submission to the Discussion Paper: [OAIC](#), 73. Submissions to the Issues Paper: [OAIC](#), 69-70; [Law Council of Australia](#), 17-18.

849 Ibid.

850 Submission to the Issues Paper: [New York Times](#), 2.

851 Daniel Solove, ‘Privacy Self-Management and the Consent Dilemma’ [2013] 126 *Harvard Law Review* 1880, 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.

852 See Chapters 12, 13, and 20.

853 See Chapters 18 and 20.

854 Submissions to the Issues Paper: [Consumer Policy Research Centre](#), 8; [OAIC](#), 72; [Financial Rights Legal Centre](#), [Consumer Action Law Centre and Financial Counselling Australia](#), 28. See also, ACCC, [Digital platform services inquiry](#) (Interim Report 5, September 2022) 67 and Norwegian Consumer Council, [Deceived by Design](#) (Report, June 2018).

855 Ibid. See also, ACCC, [DPI Report](#) 394-401.

856 [Discussion Paper](#), 76-78.

A broad range of submitters were supportive of the proposed definition of consent, including from civil society groups, academia and industry.⁸⁵⁷ It was thought that the proposed definition would largely codify existing OAIC guidance,⁸⁵⁸ provide additional clarity for APP entities regarding expected standards of consent, and would promote the adoption of stronger consumer-driven privacy practices.⁸⁵⁹ It was also observed that the proposal would align the Act with the definition of valid consent under the GDPR⁸⁶⁰ and that this alignment may reduce the compliance burden of entities that operate across international borders.⁸⁶¹

Some stakeholders sought clarity on whether the phrase ‘indication through clear action’ would preclude the use of implied consent in certain circumstances.⁸⁶² Some considered that this would effectively remove the Act’s recognition of implied consent which would cause practical problems in the context of medical research or in clinical healthcare settings.⁸⁶³ The OAIC observed that implied consent is important in the healthcare context, for example, ‘where a medical practitioner collects a specimen to send to a pathology laboratory for testing, it can be implied from the conduct of the individual that they consent to the laboratory collecting their health information, without the need for the laboratory to seek further express consent from the individual’.⁸⁶⁴ However, the OAIC was of the view that the phrase ‘unambiguous indication through clear action’ would still allow for consent to be implied in appropriate circumstances.⁸⁶⁵

For the avoidance of doubt, it is considered that the reference to ‘clear action’ should not be included in the proposed definition of consent so that implied consent may continue to be relied upon in these limited circumstances. However, an entity that wishes to rely on implied consent would still be required to demonstrate that the implied consent was ‘unambiguous’.⁸⁶⁶ This would continue to allow for implied consent in the clinical healthcare context, while restricting the use of implied consent in commercial settings where there is ambiguity as to the consumer’s intention or knowledge as to how information is proposed to be handled.

Several research stakeholders submitted that the proposed definition of consent could limit health researchers’ ability to use personal information for public interest research.⁸⁶⁷ These concerns warrant specific treatment and are considered further in Chapter 14 on Research.

11.1 Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.

- 857 Submissions to the Discussion Paper: [Australian Banking Association](#); [Office of the Victorian Information Commissioner](#); [Salinger Privacy](#); [Public Interest Advocacy Centre](#); [OAIC](#); [Deloitte Australia](#); [New South Wales Council for Civil Liberties](#); [Royal Australian and New Zealand College of Psychiatrists](#); [Electronic Frontiers](#); [IIS Partners & GroundUp Consulting](#); [Consumer Policy Research Centre](#); [Privacy 108](#); [ResMed](#); [Obesity Policy Coalition](#); [Foundation for Alcohol Research and Education](#); [Centre for AI and Digital Ethics](#). See also, [Minderoo Tech & Policy Lab](#), [UWA Law School](#); [Atlassian](#); [Department of Health \(Cth\)](#); [Australian Council on Children and the Media](#); [Fintech Australia](#); [Guardian Australia](#); [Australian Privacy Foundation](#); [Castan Centre](#); [Digital Rights Watch](#); [Centre for Media Transition](#); [ACCC](#); [Dr Katharine Kemp](#), [UNSW Sydney](#); [European Commission](#); [CHOICE](#); [elevenM](#).
- 858 OAIC, [APP Guidelines](#) (July 2019) [B.37]–[B.58].
- 859 See, Submissions to the Discussion Paper: [Deloitte Australia](#), 18; [OAIC](#), 73–75; [Public Interest Advocacy Centre](#), 9–10; [Centre for AI and Digital Ethics](#), 5.
- 860 See, Submissions to the Discussion Paper: [OAIC](#), 73–75; [Consumer Policy Research Centre](#), 4; [Centre for AI and Digital Ethics](#), 5; [Western Union](#), 3. C.f. [Snap Inc.](#), 4, who submitted that the GDPR’s definition of consent should be adopted verbatim.
- 861 Submission to the Discussion Paper: [OAIC](#), 74.
- 862 Submissions to the Discussion Paper: [Department of Health \(Cth\)](#), 8; [NHMRC - National Health and Medical Research Council](#), 2; [MIGA](#), 4.
- 863 See, Submissions to the Discussion Paper: [NHMRC - National Health and Medical Research Council](#), 2; [MIGA](#), 4; [Department of Health \(Cth\)](#), 8.
- 864 Submission to the Discussion Paper: [OAIC](#), 75.
- 865 Ibid.
- 866 OAIC, [APP Guidelines](#) (July 2019) [B.42].
- 867 Submissions to the Discussion Paper: [Population Health Research Network](#), 5; [Eckstein et al.](#), 3; [Department of Health \(Cth\)](#), 8.

Several submitters considered that the definition of consent could be supplemented with OAIC guidance⁸⁶⁸ Explanatory materials to the reforms could also provide detail on the intended interpretation of these terms. The following details could be of assistance in interpreting the proposed elements:

- 1) **Voluntary** – An individual must have a genuine opportunity to provide or withhold consent.⁸⁶⁹ 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'.⁸⁷⁰ The OAIC submitted that guidance could supplement this requirement by noting 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'.⁸⁷¹
- 2) **Informed** – An individual must be provided with sufficient information in an understandable form so that the individual is likely to be aware of the implications of providing or withholding consent to the handling of their personal information.⁸⁷² APP entities should ensure that they use clear and plain language when presenting consents to individuals.⁸⁷³
- 3) **Current** – The purpose for which the personal information is being handled must be sufficiently linked to the consent that the individual provided. Whether a particular consent is current would depend on the context.⁸⁷⁴ Consent can be considered as current where the purpose for which the personal information is handled has not *materially changed*.⁸⁷⁵ Periodic renewal of consent should not generally be required.⁸⁷⁶ However, the time that has elapsed since consent was given may be relevant in certain circumstances. OAIC guidance says that consent cannot be assumed to endure indefinitely, and it is good practice to inform individuals of the period that consent will be relied on in the absence of a material change of circumstances.⁸⁷⁷
- 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'. This element is directed at guarding against overly broad or 'bundled consents'. The level of specificity required may depend on circumstances including the sensitivity of the personal information,⁸⁷⁸ whether the proposed collection, use or disclosure is for a purpose that is essential or non-essential for the provision of a service,⁸⁷⁹ and whether the collection, use or disclosure would be reasonably expected by the individual.
- 5) **Unambiguous** – OAIC guidance provides that '*[c]onsent may not be implied if an individual's intent is ambiguous or there is reasonable doubt about the individual's intention*'.⁸⁸⁰ It is further noted that '[u]se of an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous'.⁸⁸¹

OAIC guidance could further clarify that the 'acceptance of a general or broad terms of use', 'hovering over, muting, pausing or closing a given piece of content,' or 'agreement obtained through use of dark patterns' are unlikely to constitute consent.⁸⁸² The proposed definition of consent would be an important safeguard for ensuring that individuals are able to make real choices about the handling of their information on the basis of transparent and clear information.

868 Submission to the Discussion Paper: [OAIC](#), 74. See also, [Public Interest Advocacy Centre](#), 9; [Deloitte Australia](#), 19; [Salinger Privacy](#), 20.

869 OAIC, [APP Guidelines](#) (July 2019) [B.46]–[B.49].

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

871 Submissions to the Issues Paper: [OAIC](#), 77. See also, [Dr Katharine Kemp](#), 20.

872 OAIC, [APP Guidelines](#) (July 2019) [B.50].

873 European Data Protection Board, [Guidelines 05/2020 on consent under Regulation 2016/679](#) (4 May 2020) 16.

874 Submissions to the Discussion Paper: [OAIC](#), 75; [Telstra](#), 14; UK ICO, '[Consent](#)' (Web Page, October 2022).

875 Submissions to the Discussion Paper: [Telstra](#), 15; [Deloitte Australia](#), 19; [Australian Banking Association](#), 15. See also, OAIC, [APP Guidelines](#) (July 2019) [B.52].

876 Submission to the Discussion Paper: [Telstra](#), 14–15; [OAIC](#), 75; [Deloitte Australia](#), 18–19; [FreeTV Australia](#), 22; [Office of the Victorian Information Commissioner](#), 5; [Atlassian](#), 6–7; [Ramsay Australia](#), 6; [MIGA](#), 3; [CSIRO](#), 6; [elevenM](#), 39.

877 OAIC, [APP Guidelines](#) (July 2019) [B.52].

878 Ibid [B.51]–[B.54].

879 Submission to the Issues Paper: [Deloitte](#), 20. 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.

880 OAIC, [APP Guidelines](#) (July 2019) [B.42].

881 Ibid [B.43]. See relatedly, GDPR Recital 32.

882 Submissions to the Discussion Paper: [Salinger Privacy](#), 20; [ADMA](#), 19.

11.4 Standardisation of consent requests

The Discussion Paper proposed that standardised consents be considered in developing APP codes, which could include the standardisation of layouts, wording, icons or consent taxonomies.⁸⁸³ It was suggested that standardised consent requests with consistent terminology would improve consumers' decision-making and comprehension of data handling practices.⁸⁸⁴

A number of submissions were supportive of the proposal to progress standardised consents.⁸⁸⁵ The Castan Centre submitted that standardised consents are a 'promising mechanism' for 'dealing with the issue of consent complexity and information overload'.⁸⁸⁶ The Law Council of Australia noted that the 'foundation' for this work has been created through the development of standardised consent taxonomies for the Consumer Data Right, which could be pursued in the context of the Privacy Act.⁸⁸⁷ Submitters considered that consumer comprehension testing would be an important part of the development of consent standards to ensure their efficacy.⁸⁸⁸

Given the substantial body of work being progressed in relation to standardising consents under the Consumer Data Right, the OAIC should work with the Treasury and the CDR Data Standards Body to ascertain whether standardisation research undertaken for the CDR could be leveraged more broadly for APP entities covered by the Act. The OAIC could progress development of standards and guidelines for how online services should design consent requests, utilising relevant work on this from CDR. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent (e.g. specificity) should be interpreted in the online context. Guidance could also leverage existing consent frameworks like those developed for the Consumer Data Right. OAIC guidance could also focus on particular modes of collection or types of information to seek to generate commonly understood terms for both consumers and APP entities. If the small business exception is modified (see Chapter 6), standardised consents could assist reduce compliance burden. Consideration could be given to further progressing standardised consents as part of any future APP codes.

11.2 The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.

11.5 Withdrawal of consent

The Discussion Paper proposed that an individual should be able to 'object or withdraw their consent at any time to the collection, use or disclosure of their personal information'.⁸⁸⁹ The ability to withdraw consent already exists, but it is not express in the Act. Multiple submitters pointed out that if consent is freely given, it must be capable of being freely withdrawn.⁸⁹⁰ Some submitters considered that this made the proposal somewhat redundant.⁸⁹¹

Salinger Privacy and the NSW Council for Civil Liberties noted that the right to withdraw consent in GDPR Article 7(3)

883 [Discussion Paper](#), 79.

884 *Ibid* 70, 79.

885 Submissions to the Discussion Paper: [Australian Banking Association](#); [Public Interest Advocacy Centre](#); [Salinger Privacy](#); [OAIC](#); [Deloitte Australia](#); [New South Wales Council for Civil Liberties](#); [Dr Henry Fraser](#); [Consumer Policy Research Centre](#); [Privacy 108](#); [Obesity Policy Coalition](#); [Foundation for Alcohol Research and Education](#); [Department of Health \(Cth\)](#); [Australian Council on Children and the Media](#); [Fintech Australia](#); [Australian Privacy Foundation](#); [Centre for Media Transition](#); [Optus](#); [Castan Centre](#); [ACCC](#); [Law Council of Australia](#); [elevenM](#).

886 Submission to the Discussion Paper: [Castan Centre](#), 15.

887 Submission to the Discussion Paper: [Law Council of Australia](#), 12-13. See also, Data61, 'Consumer Experience', *Consumer Data Standards* (Web Page, version 1.22.0).

888 Submissions to the Discussion Paper: [OAIC](#), 78; [Deloitte Australia](#), 19; [CHOICE](#), 10-11; [Centre for Media Transition](#), 10; [elevenM](#), 29.

889 See [Discussion Paper](#), Proposal 14.1.

890 Submissions to the Discussion Paper: [ADMA](#), 26; [Salinger Privacy](#), 30; [Electronic Frontiers](#), 11.

891 Submissions to the Discussion Paper: [ADMA](#), 26; [Electronic Frontiers](#), 11.

provides that 'It shall be as easy to withdraw as to give consent'.⁸⁹² The ADMA considered this was already the case at law.⁸⁹³ It was submitted that it should be made express that a withdrawal of consent does not make past reliance on consent unlawful.⁸⁹⁴ The GDPR provides for this in Article 7(3).

The proposed reforms to consent emphasise the necessity of 'valid' consent which includes the elements of 'voluntariness'. Similarly, the ability to withdraw consent should be expressly recognised in the Act to reinforce the importance of valid consent. Withdrawal of consent would not be subject to the exceptions to the Rights of the Individual. Consent is already subject to the general exceptions to the APPs. These exceptions would also apply where withdrawal of consent may not be possible or would be contrary to other public interests (such as research⁸⁹⁵ and medical services⁸⁹⁶). The proposed new rights of the individual may furnish individuals with the information they need to be able to effectively exercise a withdrawal of consent (see Chapter 18).

11.3 Expressly recognise the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent would not affect the lawfulness of how the personal information was handled before the consent was withdrawn.

11.6 Privacy settings for online services

The Discussion Paper sought feedback on whether it would be desirable to require online services to implement default privacy settings in certain circumstances, and whether online services should ensure that privacy settings are easy for individuals to access and use.⁸⁹⁷ It proposed two possible options to stakeholders:

- **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, and
- **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.

A broad range of submissions expressed support for pro-privacy default settings (Option 1), including those from civil society groups, academia, industry and the OAIC.⁸⁹⁸ It was suggested that the current expectation on consumers to adjust privacy settings across all sites and platforms they access places an undue cognitive load on consumers, who are already experiencing a sense of feeling overwhelmed in managing their privacy.⁸⁹⁹ The Deloitte 2020 Privacy Index found that 93 per cent of respondents expected a service to give consumers an option to opt-in to 'non-essential' uses of personal information, 'such as marketing' and 'sharing' personal information with other organisations.⁹⁰⁰ It was observed that the difference between an opt-in and an opt-out default can have a significant effect on consumer participation,⁹⁰¹ and that presenting one option as a default increases the chance it will be chosen.⁹⁰² The OAIC

892 Submissions to the Discussion Paper: [Salinger Privacy](#), 30; [New South Wales Council for Civil Liberties](#), 28.

893 Submission to the Discussion Paper: [ADMA](#), 26.

894 Submission to the Discussion Paper: [Federal Chamber of Automotive Industries](#), 22.

895 Submissions to the Discussion Paper: [NHMRC – National Health and Medical Research Council](#), 3; [CSIRO](#), 6.

896 Submissions to the Discussion Paper: [Australian Medical Association](#), 12; [Avant Mutual](#), 12-13.

897 [Discussion Paper](#), 98-99.

898 See for example Submissions to the Discussion Paper: [OAIC](#); [The Australia Institute – Centre for Responsible Technology](#); [Salinger Privacy](#); [Deloitte Australia](#); [New South Wales Council for Civil Liberties](#); [Snap Inc](#) (recommending that only 'certain high-risk or sensitive features such as location-sharing' be off by default); [Consumer Policy Research Centre](#), [Australian Privacy Foundation](#); [Centre for AI and Digital Ethics](#).

899 Submission to the Discussion Paper: [Consumer Policy Research Centre](#), 6-7.

900 Submission to the Discussion Paper: [Deloitte Australia](#), 27-28. See also, Deloitte, [Australian Privacy Index 2020](#) (Report, July 2020) 14.

901 Submissions to the Discussion Paper: [OAIC](#), 115-6; [New South Wales Council for Civil Liberties](#), 22-23; [The Australia Institute – Centre for Responsible Technology](#), 8.

902 Submission to the Discussion Paper: [OAIC](#), 115-6. See, Department of Prime Minister and Cabinet, [Harnessing the Power of Defaults – Governance Note](#), (Web Page, 9 December 2021) 4.

recommended that 'privacy settings should be set to privacy protective by default except for the collection, use or disclosure of personal information that is reasonably necessary to provide the particular product or service.'⁹⁰³

Several submissions opposed the introduction of pro-privacy default settings or expressed caution about the proposal.⁹⁰⁴ SBS considered that pro-privacy defaults would compromise its ability to generate revenue and may 'materially affect' its hybrid-funding model, as very few customers would opt-in to targeted advertising given that 'consumers rarely change default settings provided to them'.⁹⁰⁵ SBS submitted that its ability to use 'data, ratings and aggregate demographic information' to inform decisions about programming on its broadcast platform to better cater to audiences would be negatively impacted by pro-privacy defaults.⁹⁰⁶ Free TV Australia submitted that free-to-air television is an advertising funded business model and that it is '[i]mportant for the Australian media to require viewers to receive some advertising' as a condition of receiving free online streaming services.⁹⁰⁷ Free TV further submitted that the advertising-funded model for the Australian media is well-established, that a diversity of media voices is essential to the public good and that the 'the burden on taxpayers of funding multiple Australian media services would be great.'⁹⁰⁸

Telstra argued that pro-privacy defaults could result in consent fatigue if entities were required to seek individuals' consent through a change of privacy settings for activities that are essential to the effective functioning of a service. In a submission to the Issues Paper, IGEA 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.⁹⁰⁹

Submitters were generally supportive of Option 2. However, some expressed concern that a 'one click mechanism' would not be appropriate for all entities and in some instances could lead to consumers turning off essential functionality that they want or expect from a service.⁹¹⁰ Some considered that Option 1 and Option 2 may not necessarily be mutually exclusive and that both options be adopted to ensure that, where introduced, pro-privacy default settings are enabled, as well as easily accessible and clear for consumers to modify.⁹¹¹

The Act requires that only personal information and sensitive information that is reasonably necessary (or 'directly related' for agencies) for an entity's functions or activities may be collected. APP 6 provides that information may only be used for a secondary purpose separate to the primary purpose with consent or under an exception in APP 6.2 or 6.3.

This Report proposes that, in addition to current requirements in the Act, an entity be allowed to collect, use and disclose information only where it is fair and reasonable in the circumstances. These features together effectively operate as a requirement similar to Option 1 and give effect to the data minimisation principles underpinning the Act. To complement this approach, the OAIC proposed that the 'Commissioner could issue guidance on the types of personal information handling practices that may not be reasonably necessary to provide a particular product or service and the matters entities should consider when implementing privacy protective default settings.'⁹¹²

APP entities with online businesses should ensure privacy settings are clear and easily accessible for individuals to modify them, including to make them the most restrictive and privacy protective generally. OAIC guidance may be of assistance to online services to structure their privacy settings to ensure settings give full effect to the principles in the Act.

903 Submission to the Discussion Paper: [OAIC](#), 115-8. See also, [Castan Centre](#), 20.

904 See, e.g. Submissions to the Discussion Paper: [Telstra](#); [Free TV Australia](#); [Google](#); [SBS](#); [IGEA](#).

905 Submission to the Discussion Paper: [SBS](#), 21-22.

906 Ibid 21-22.

907 Submission to the Discussion Paper: [Free TV Australia](#), 31.

908 Ibid.

909 Submission to the Issues Paper: [Interactive Games and Entertainment Association](#), 13-14.

910 Submissions to the Discussion Paper: [SBS](#), 21; [Free TV Australia](#), 31; [Snap Inc](#), 5-6; [Google](#), 3.

911 Submissions to the Discussion Paper: [Deloitte Australia](#), 28; [Privacy 108](#), 23.

912 Submissions to the Discussion Paper: [OAIC](#), 116.

Online privacy settings would also be progressed as part of the Children's Online Privacy Code⁹¹³ which would apply to online services that are likely to be accessed by children. This Code would be modelled on the UK's Age Appropriate Design Code, which 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'.⁹¹⁴ The UK's Age Appropriate Design Code introduces prescriptive standards for pro-privacy defaults in relation to geolocation data, the public visibility of children's data, service personalisation, data sharing and nudge techniques.⁹¹⁵ The need for pro-privacy default settings should also be evaluated for any other future APP codes that may apply to online services.

11.4 Online privacy settings should reflect the privacy by default framework of the Act.

APP entities that provide online services should be required to ensure that any privacy settings are clear and easily accessible for service users.

⁹¹³ See Chapter 16.

⁹¹⁴ UK ICO, [Age appropriate design: a code of practice for online services](#) (September 2020).

⁹¹⁵ Ibid.

12. Fair and reasonable test

Stakeholders to the Review have highlighted personal information handling practices which do not meet community expectations.⁹¹⁶ The ACCC made several recommendations to address data practices of concern in its DPI Report.⁹¹⁷ These included recommendations to improve the quality of collection notices⁹¹⁸ and consent,⁹¹⁹ as well as to require that consent be obtained 'whenever a consumer's personal information is collected, used or disclosed by an APP entity, unless the personal information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason.'⁹²⁰ However, feedback provided to the Review has indicated that reform of privacy policy, collection notice and consent requirements alone will not adequately address emerging privacy risks in the digital age.⁹²¹

Where digital innovation is exponentially increasing the amount of personal information and sources from which it is collected, it is not reasonable that individuals should bear primary responsibility for ensuring that they do not experience harm as a result of an entity's information-handling practices. The diversity, change and novelty in digital information-handling practices may mean that individuals do not appreciate the scale, or even the existence, of privacy risks. The DPI Report recommended that in addition to reforms to improve the quality of privacy notices and consent, 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.'⁹²²

12.1 Current requirements for collecting, using or disclosing personal information

APPs 3, 5 and 6 establish the framework for the lawful collection, use and disclosure of personal information. Under APP 3, organisations must not collect personal information unless it is reasonably necessary for one or more of their functions or activities. For agencies, the collection must be reasonably necessary for, or directly related to, one or more of their function or activities.⁹²³

To collect sensitive information, an APP entity must also obtain an individual's consent or an exception must apply.⁹²⁴ APP 3 further stipulates that an APP entity must collect personal information only by lawful and fair means and must collect it directly from the individual unless it is unreasonable or impracticable for an organisation to do so, or in the case of an agency, consent has been obtained or such collection is authorised by law or a court or tribunal order.⁹²⁵

Under APP 5, at or before the time of collection, an APP entity must take such steps (if any) as are reasonable in the circumstances to notify the individual about various matters, including the purposes for which the APP entity collects the personal information.⁹²⁶

Under APP 6, personal information must be used or disclosed for the purpose for which it was collected (the primary purpose).⁹²⁷ Personal information may only be used or disclosed for a different purpose which is 'related to' (or 'directly related to' for sensitive information) the primary purpose if the individual would reasonably expect their information to be so used or disclosed.⁹²⁸ To use or disclose personal information for a secondary purpose which is unrelated to the primary purpose, the individuals' consent must be obtained, or another exception in APP 6.2 or 6.3 must apply.⁹²⁹

916 [Discussion Paper](#), Chapters 10 and 11.

917 ACCC, [DPI Report](#) Chapter 7.

918 Ibid Recommendation 16(b).

919 Ibid Recommendation 16(c).

920 Ibid 464.

921 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](#), 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; [Privacy 108](#), 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. Submissions to the Discussion Paper: [OAIC](#), 80; [Kimberlee Weatherall](#), [Tom Manousaridis and Melanie Trezise](#), 11-12; [Salinger Privacy](#), 20; [New South Wales Council for Civil Liberties](#), 18; [Telstra](#), 15; [Graham Greenleaf](#), [UNSW Sydney](#), 3-4; [Dr Katharine Kemp](#), [UNSW Sydney](#), 13-14; [CHOICE](#), 11; [Experian Australia](#), 12; [Electronic Frontiers](#), 9; [Centre for Media Transition](#), 5; [Castan Centre](#), 16-17; [Office of the Victorian Information Commissioner](#), 6. See also Daniel Solove, 'Privacy Self-Management and the Consent Dilemma' [2013] 126 *Harvard Law Review* 1880; ASIC, [Disclosure: Why it shouldn't be the default](#) (Report, October 2019).

922 ACCC, [DPI Report](#) 476-8.

923 Privacy Act sch 1, APP 3.1-3.2.

924 Ibid APP 3.3-3.4.

925 Ibid APP 3.5-3.6.

926 Ibid APP 5.1-5.2.

927 Ibid APP 6.1.

928 Ibid APP 6.2(a).

929 Ibid APP 6.1, 6.2(b)-(3), 6.3.

12.2 Limitations of the current approach

Feedback to the Review has highlighted the shortcomings of a regulatory approach in which individuals are expected to read and understand voluminous collection notices and privacy policies to evaluate current and future privacy risks, in order to decide whether to engage with an APP entity.⁹³⁰

Stakeholders have also suggested that entities have significant discretion in determining whether a collection is reasonably necessary for their functions and activities under APP 3, which could include practices that may not meet consumer expectations.⁹³¹ This is notwithstanding guidance in the Explanatory Memorandum to the Enhancing Privacy Protection Bill which provides that the test is an objective one and that the function or activity must be ‘legitimate for that type of entity’.⁹³² However, the Australian Privacy Law Handbook suggests that an intention by Parliament to impose such a test is not clear from the wording of the principle itself.⁹³³

Recent developments in Australian privacy case law have considered the role of legitimacy and proportionality in the context of assessing collections of personal information. 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’.⁹³⁴ The *Jurecek* decision has been cited and applied by the IC when interpreting APP 3 of the Act.⁹³⁵

However, submitters to the Review considered that the current framework is inadequate as it does not expressly require consideration of matters such as the impact on individuals, individuals’ reasonable expectations and proportionality. Data Synergies’ submission stated that the Act ‘does address reasonable necessity to effect a stated purpose, but does not squarely address reasonableness or proportionality of acts and practices of regulated entities in collecting, handling and disclosing personal information about individuals’.⁹³⁶ The European Commission’s submission also noted that APP 3.1 and 3.2 ‘appears to regulate the relationship between a chosen objective [purpose of processing] and the type of processing/ personal data being processed – without imposing particular restrictions as to the objective [purpose] that may be pursued’.⁹³⁷

The DPI Report observed 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’.⁹³⁸ The OAIC also highlighted that the APPs do not currently require entities to expressly consider whether personal information handling is within the reasonable expectations of an individual, except when using or disclosing for a secondary purpose under APP 6.2.⁹³⁹ Furthermore, the requirement for a collection to be fair and lawful is limited to the *means* by which personal information is collected, and has been narrowly interpreted as a collection ‘that does not involve intimidation or deception, and is not unreasonably intrusive’.⁹⁴⁰ Submitters to the Review also expressed concern that individuals can be required to consent to entities’ information-handling practices as a condition of accessing many digital services, including intrusive or harmful practices.⁹⁴¹

930 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](#), 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; [Privacy 108](#), 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. Submissions to the Discussion Paper: [OAIC](#), 80; [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 11–12; [Salinger Privacy](#), 20; [New South Wales Council for Civil Liberties](#), 18; [Telstra](#), 15; [Graham Greenleaf, UNSW Sydney](#), 3–4; [Dr Katharine Kemp, UNSW Sydney](#), 13–14; [CHOICE](#), 11; [Experian Australia](#), 12; [Electronic Frontiers](#), 9; [Centre for Media Transition](#), 5; [Castan Centre](#), 16–17; [Office of the Victorian Information Commissioner](#), 6.

931 ACCC, [DPI Report](#), 438. See relatedly, Submissions to the Issues Paper: [Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia](#), 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.

932 Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 75.

933 Jeremy Douglas-Stewart, *Australian Privacy Law Handbook* (Presidian Legal Publications, 2022) [7.1100].

934 [2016] VSC 285, [69]–[70].

935 7-Eleven [Determination](#), [59].

936 Submission to the Discussion Paper: [Data Synergies](#), 33.

937 Submission to the Discussion Paper: [European Commission](#), 3.

938 ACCC, [DPI Report](#) 478.

939 Submission to the Discussion Paper: [OAIC](#), 82.

940 OAIC, [APP Guidelines](#) [July 2019] [3.62].

941 [Discussion Paper](#), 82. Submissions to the Issues Paper: [OAIC](#), 71; [New South Wales Council for Civil Liberties](#), 8; [Queensland Law Society](#), 5; [Dr Katharine Kemp](#), 2; [Adobe](#), 4; [Salinger Privacy](#), 19; [Association for Data-driven Marketing & Advertising \(ADMA\)](#), 16; [Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia](#), 21–22.

In light of these concerns, the majority of submitters considered that reform of privacy policy, collection notice and consent requirements alone would not adequately address emerging privacy risks in the digital age.⁹⁴² They considered that minimum standards should be introduced which govern how entities may collect, use and disclose personal information, including by requiring that information-handling practices be within individuals' reasonable expectations and that their impact on individuals be a relevant consideration in whether and how APP entities collect, use and disclose personal information.⁹⁴³

12.3 Discussion Paper proposal

The Discussion Paper proposed that a collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances. It also proposed that the following legislated factors could accompany the test to assist entities in determining whether a collection, use or disclosure is fair and reasonable in the circumstances:

- 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 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.

12.3.1 Fair and reasonable test

A broad range of submitters, including academics, industry, notforprofits, government agencies and consumer advocacy groups expressed support for the proposal.⁹⁴⁴ Submitters considered that the fair and reasonable test would provide additional protections that reflect community expectations, raise the standard of personal information handling economy-wide and improve consumer trust of digital services.⁹⁴⁵

⁹⁴² 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](#), 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; [Privacy 108](#), 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. Submissions to the Discussion Paper: [OAIC](#), 80; [Kimberlee Weatherall](#), [Tom Manousaridis](#) and [Melanie Trezise](#), 11-12; [Salinger Privacy](#), 20; [New South Wales Council for Civil Liberties](#), 18; [Telstra](#), 15; [Graham Greenleaf](#), [UNSW Sydney](#), 3-4; [Dr Katharine Kemp](#), [UNSW Sydney](#), 13-14; [CHOICE](#), 11; [Experian Australia](#), 12; [Electronic Frontiers](#), 9; [Centre for Media Transition](#), 5; [Castan Centre](#), 16-17; [Office of the Victorian Information Commissioner](#), 6.

⁹⁴³ Submissions to the Issues Paper: [OAIC](#), 83-8; [Adobe](#), 5; [CHOICE](#), 1, 5-6; [Law Council of Australia](#), 5-6, 18-19; [Consumer Policy Research Centre](#), 12; [Salinger Privacy](#), 22-26; [Public Interest Advocacy Centre](#), 8; [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; [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. Submissions to the Discussion Paper: [Deloitte Australia](#), 21-22; [KPMG](#), 18; [OAIC](#), 80; [Kimberlee Weatherall](#), [Tom Manousaridis](#) and [Melanie Trezise](#), 11-12; [CHOICE](#), 11; [Office of the Victorian Information Commissioner](#), 6; [Salinger Privacy](#), 20; [New South Wales Council for Civil Liberties](#), 18; [Centre for Media Transition](#), 5; [Castan Centre](#), 16-17; [Snap Inc](#), 5; [ResMed](#), 4; [Consumer Policy Research Centre](#), 4.

⁹⁴⁴ Submissions to the Discussion Paper: [KPMG](#); [Kimberlee Weatherall](#), [Tom Manousaridis](#) and [Melanie Trezise](#); [OAIC](#); [Snap Inc](#); [Telstra](#); [Office of the Victorian Information Commissioner](#); [Privacy 108](#); [ResMed](#); [Eckstein et al](#); [Consumer Policy Research Centre](#); [Deloitte Australia](#); [Salinger Privacy](#); [NSW Council for Civil Liberties](#); [Graham Greenleaf](#), [UNSW Sydney](#); [Dr Katharine Kemp](#), [UNSW Sydney](#); [CHOICE](#); [Experian Australia](#); [Electronic Frontiers](#); [Centre for Media Transition](#); [Castan Centre](#); [Atlassian](#); [Department of Health \(Cth\)](#); [National Australia Bank](#); [Western Union](#); [Helen Gregorczyk](#), [University of Queensland](#); [Fintech Australia](#); [Australian Privacy Foundation](#); [Equifax](#); [Centre for AI and Digital Ethics](#); [Services Australia](#), [DIGI](#); [ABC](#); [elevenM](#); [Obesity Policy Coalition](#); [Foundation for Alcohol Research and Education](#); [Public Interest Advocacy Centre](#). See relatedly, [Digital Law Association](#); [Commonwealth Bank](#); [ANZ](#).

⁹⁴⁵ Submissions to the Discussion Paper: [OAIC](#), 80; [KPMG](#), 18; [Deloitte Australia](#), 21-22; [Office of the Victorian Information Commissioner](#), 6; [ResMed](#), 9; [Castan Centre](#), 16-17; [Western Union](#), 3-4; [elevenM](#), 30-31.

Other submissions did not support the proposed requirement on a number of grounds, including that APPs 3 and 6 already include references to fairness and reasonableness,⁹⁴⁶ that such a requirement would introduce substantial uncertainty⁹⁴⁷ and impose regulatory burden on APP entities.⁹⁴⁸ Some considered that it would place 'excessive discretionary power in the hands of the regulator.'⁹⁴⁹

Lawful bases for personal information handling

A number of submitters continued to advocate for the introduction of GDPR-style lawful bases for personal information handling.⁹⁵⁰ Some submitters suggested that lawful bases could co-exist with a baseline 'fair and reasonable' test.⁹⁵¹ Others specifically called for the introduction of a legitimate interests basis for personal information handling, either in place of, or in combination with, a new fair and reasonable test.⁹⁵² These submitters considered that a legitimate interests ground could provide clarity for APP entities that certain functions or activities are legitimate purposes for handling personal information, while ensuring that risks to the individual are appropriately taken into account.⁹⁵³ Others considered that introducing a legitimate interests ground was desirable on the basis of its interoperability with overseas legal frameworks.⁹⁵⁴

Adopting lawful bases for processing would fundamentally change the current principles-based approach in the Act. It would require reconfiguration of the APPs to accommodate lawful bases and potentially, the adoption of the concept of 'processing.' This would have implications for APPs 3 and 6 and other APPs, in particular APPs 5 and 8. As APPs 3 and 6 currently provide a flexible framework which allows for the collection, use and disclosure of personal information for the purposes set out in the GDPR's lawful bases, such fundamental change is considered unnecessary.

It is also not clear that it would result in a more privacy protective outcome for Australians. All lawful bases under the GDPR are also supplemented by the 'lawfulness, fairness and transparency' principle in Article 5 of the GDPR. Data processed under the 'legitimate interests' basis must also be assessed in terms of legitimacy of the data controller's purpose for processing and necessity of processing for that purpose, against the 'interests or fundamental rights or freedoms of the data subject.'⁹⁵⁵ In the Australian context, an overarching fair and reasonable test for the collection, use and disclosure of personal information, with legislated factors to assist with applying the test, would provide express guidance to APP entities and bodies responsible for interpreting the Act on how to evaluate fairness, and how to consider the balancing of individuals' interests against those of APP entities. This is particularly important where Australia has more limited human rights jurisprudence relative to Europe to assist with interpreting what is meant by 'the interests or fundamental rights or freedoms of the data subject' in a given situation.⁹⁵⁶

Objective or subjective test

Submissions indicated that the test would benefit from additional clarification as to whether it is to be assessed objectively or subjectively.⁹⁵⁷ Submitters suggested that an objective standard would be preferable to a subjective standard, which would place an unrealistic burden on APP entities⁹⁵⁸ or lead to the over-collection of information by APP entities in an effort to ascertain the vulnerabilities of all their users in order to avoid causing harm.⁹⁵⁹ Several submissions also considered that an objective standard would be more appropriate for addressing systemic harms.⁹⁶⁰

⁹⁴⁶ Submissions to the Discussion Paper: [Optus](#), 18; [Communications Alliance](#), 15.

⁹⁴⁷ Submissions to the Discussion Paper: [Privcore](#), 3-5; [Free TV Australia](#), 29-30; [Nine](#), 12; [IAB](#), 20-22; [Communications Alliance](#), 15; [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 7.

⁹⁴⁸ Submissions to the Discussion Paper: [CSIRO](#), 6-7.

⁹⁴⁹ Submissions to the Discussion Paper: [Free TV Australia](#), 29-30. See also [Nine](#), 12.

⁹⁵⁰ Submissions to the Discussion Paper: [Business Council of Australia](#), 7; [BSA The Software Alliance](#), 9-10; [Salesforce](#), 3; [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 6-7; [Information Technology Industry Council](#), 3; [DIGI](#), 15; [IAB](#), 20-22. See, GDPR art 6.

⁹⁵¹ Submissions to the Discussion Paper: [BSA The Software Alliance](#), 9-10; [Microsoft](#), 6; [DIGI](#), 15; [Salesforce](#), 3.

⁹⁵² Submissions to the Discussion Paper: [Business Council of Australia](#), 7; [Microsoft](#), 6; [BSA The Software Alliance](#), 9-10; [Salesforce](#), 3, [Google](#), 2-3; [Atlassian](#), 7; [DIGI](#), 15.

⁹⁵³ Submissions to the Discussion Paper: [BSA The Software Alliance](#), 9-10; [Salesforce](#), 3; [Google](#), 2-3; [IAB](#), 20-22.

⁹⁵⁴ Submissions to the Discussion Paper: [Atlassian](#), 7; [Microsoft](#), 6; [Information Technology Industry Council](#), 3.

⁹⁵⁵ GDPR art 6(1)(f). See also, UK ICO, [Legitimate interests](#) (Web Page, January 2021).

⁹⁵⁶ See, Submission to the Discussion Paper: [Castan Centre](#), which notes the significance of the European Charter of Fundamental Rights and European Convention on Human Rights to the development of European rights jurisprudence.

⁹⁵⁷ Submissions to the Discussion Paper: [Salinger Privacy](#), 23; [Business Council of Australia](#), 7; [New South Wales Council for Civil Liberties](#), 18; [Electronic Frontiers](#), 10; [ADMA](#), 23. See relatedly, [Communications Alliance](#), 15.

⁹⁵⁸ See relatedly, Submission to the Discussion Paper: [Telstra](#), 15.

⁹⁵⁹ Submission to the Discussion Paper: [Salinger Privacy](#), 23.

⁹⁶⁰ Submissions to the Discussion Paper: [Salinger Privacy](#), 23; [New South Wales Council for Civil Liberties](#), 18; [Electronic Frontiers](#), 10.

An objective reasonable person standard has been employed effectively in data protection laws in Canada⁹⁶¹ and Singapore,⁹⁶² which require personal information handling to be for a purpose ‘that a reasonable person would consider appropriate’. The use of a reasonable person standard is also widely used in Australian law, and Australian courts will be well equipped to apply this standard. It is proposed that the test would be an objective one according to a reasonable person standard.

Certainty of the proposed test

A number of submissions suggested the proposed test would be too uncertain.⁹⁶³ Some expressed the view that ‘reasonableness’ as an overarching positive legal requirement is highly subjective.⁹⁶⁴ By contrast, others submitted that ‘fairness’ is broadly understood and well-grounded in related legal frameworks such as consumer protection law and financial services regulation.⁹⁶⁵ Some submitters supported the flexibility of the test, as it would allow the test to adapt to the particular circumstances of the case, as well as to changing societal expectations and new technologies.⁹⁶⁶ A number of submitters considered that the proposal would strike the right balance between flexibility and certainty.⁹⁶⁷

A number of international data protection laws include similar baseline standards, including the GDPR, Canada’s *Personal Information Protection and Electronic Documents Act 2000* (PIPEDA) and Singapore’s *Personal Data Protection Act 2012*.

Jurisdiction	Law	Provision
Europe and UK	GDPR and UK GDPR	Article 5(1) – ‘Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.’
Canada	<i>Personal Information Protection and Electronic Documents Act 2000</i> (PIPEDA)	Section 5(3) – ‘An organization may collect, use or disclose personal information only for purposes that a <i>reasonable person would consider are appropriate</i> in the circumstances.’
Singapore	<i>Personal Data Protection Act 2012</i> (PDPA)	Section 18 – ‘An organisation may collect, use or disclose personal data about an individual only for purposes that a <i>reasonable person would consider appropriate</i> in the circumstances’

Figure 12.1: Equivalent baseline protections in selected overseas data protection legislation.

Guidance issued by the UK ICO notes that the fairness principle in Article 5(1) of the UK GDPR 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.’⁹⁶⁸ The European Data Protection Board (EDPB) has advised that the fairness principle in Article 5(1) recognises ‘the reasonable expectations of the data subjects, considering possible adverse consequences processing may have on them, and having regard to the relationship and potential effects of imbalance between them and the controller’.⁹⁶⁹

⁹⁶¹ *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 5(3).

⁹⁶² *Personal Data Protection Act 2012* (Singapore) s 18.

⁹⁶³ Submissions to the Discussion Paper: [Privcore](#), 3-5; [FreeTV Australia](#), 29-30; [Nine](#), 12; [IAB](#), 20-22; [Communications Alliance](#), 15.

⁹⁶⁴ Submissions to the Discussion Paper: [ADMA](#), 23; [Communications Alliance](#), 25.

⁹⁶⁵ Submissions to the Discussion Paper: [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 28; [OAIC](#), 81; [Electronic Frontiers](#), 9; [elevenM](#), 30-31. See relatedly, [CHOICE](#).

⁹⁶⁶ Submissions to the Discussion Paper: [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 27; [OAIC](#), 80; [KPMG](#), 18; [Centre for Media Transition](#), 5.

⁹⁶⁷ Submissions to the Discussion Paper: [Helen Gregorcuk, University of Queensland](#); [Centre for Media Transition](#), 5; [Castan Centre](#), 17; [Professor David Lindsay](#), 21-22. See also, [Deloitte Australia](#), 23.

⁹⁶⁸ UK ICO, [Lawfulness, fairness and transparency](#) (Web Page, January 2021).

⁹⁶⁹ European Data Protection Board, [Guidelines 2/2019 on the processing of personal data under Article 6\(1\)\(b\) GDPR in the context of the provision of online services to data subjects](#) (October 2019) 5. See also, European Data Protection Board, [Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#) (October 2020) 17-18; European Data Protection Board, [Guidelines 3/2022 on Dark patterns in social media platform interfaces](#) (March 2022) 8-9.

The EDPB further provides that operative elements of the fairness principle include, among other matters:

- Autonomy – Data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as over the scope and conditions of that use or processing
- Interaction – Data subjects must be able to communicate and exercise their rights in respect of the personal data processed by the controller
- Expectation – Processing should correspond with data subjects' reasonable expectations
- Non-discrimination – The controller shall not unfairly discriminate against data subjects, and
- Non-exploitation – The controller should not exploit the needs or vulnerabilities of data subjects.⁹⁷⁰

Professor Lee Bygrave has suggested that requirements of balance and proportionality are inherent in the notion of fairness in data protection law. He states that, 'fairness also implies that persons are not unduly pressured into supplying data on themselves to others or agreeing to new uses of the data once supplied' and that fairness 'implies protection from abuse by data controllers of their monopoly position.'⁹⁷¹ Dr Damian Clifford and Dr Jef Ausloos have argued that the fairness principle in Article 5(1) of the GDPR can be divided into elements of procedural fairness and 'fair balancing',⁹⁷² with the latter incorporating notions of proportionality and necessity.⁹⁷³ However, the authors also reflected that the use of fairness as a substantive test in the GDPR needs to be further specified.⁹⁷⁴

Fairness

Protections based on fairness are found in other Commonwealth legislation, such as the unfair terms regime in the ACL.⁹⁷⁵ Under the ACL, a consumer contract or small business contract will be 'unfair' where it causes a significant imbalance in the parties' rights and obligations, is not reasonably necessary in order to protect the legitimate interests of the party who would be advantaged by the term, and would cause detriment to a party if it were to be relied upon.⁹⁷⁶ Judicial interpretation of this provision has noted that 'the requirement of a "significant imbalance" directs attention to the substantive unfairness of the contract'.⁹⁷⁷

Reasonableness

The concept of reasonableness appears throughout the Act. OAIC guidance indicates that the term reasonableness bears its ordinary meaning as being based upon or according to reason and capable of sound explanation.⁹⁷⁸ It is also used in Australian law in contexts involving proportionality analysis. It is employed by Australian courts when considering whether a law that limits a right or principle is justified, by asking whether the law is reasonably appropriate and adapted to serve a legitimate end.⁹⁷⁹ It is also used in indirect discrimination provisions in Australian anti-discrimination law.⁹⁸⁰ For example, in considering whether a condition was 'reasonable in all the circumstances' under the *Sex Discrimination Act 1984 (Cth)*, the Full Federal Court in *Re Secretary of the Department of Foreign Affairs and Trade v Helen Styles and Philip Arthur Harrison* indicated that the court was required to consider whether the requirement or condition was objectively justified, 'balanc[ing] the nature and extent of the discriminatory effect, on the one hand, against the reasons advanced in favour of the requirement or condition on the other'.⁹⁸¹ In *Waters & Ors v Public Transport Corporation*, the High Court indicated that '[a] court or tribunal will consider whether the imposition of the condition was appropriate and relevant to the performance of the activity in question, and whether the activity could be performed without imposing a requirement or condition that was discriminatory'.⁹⁸²

970 European Data Protection Board, [Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#) (October 2020) 18.

971 Lee Bygrave, *Data Privacy Law, An international Perspective* (Oxford University Press, 2014) 146.

972 Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 1 *Yearbook of European Law* 130.

973 *Ibid* 178-179.

974 *Ibid* 131.

975 *Competition and Consumer Act 2010* (Cth) sch 2, ss 23, 24.

976 *Ibid* s 24.

977 *Lobux Pty Ltd v Willshaun Pty Ltd* [2022] FCA 204, [66].

978 OAIC, [APP Guidelines](#) (July 2019) [B.108].

979 *Brown v Tasmania* [2017] 261 CLR 328.

980 See for example *Sex Discrimination Act 1984* (Cth) s 7B.

981 [1989] FCA 342.

982 [1991] HCA 49.

12.3.2 Proposal – fair and reasonable test

The fair and reasonable test would provide a principles-based means of determining whether the handling of individuals' personal information, including practices of concern that were identified by the DPI Report and submissions to this Review, are permissible. These include practices such as the creation and sharing of detailed profiles on consumers, which may include information about an individual's interests, behaviours, movements, relationships, habits, socioeconomic status and health,⁹⁸³ the use of machine learning to infer traits about an individual without their knowledge,⁹⁸⁴ targeting content and advertising to individuals based on predicted vulnerabilities,⁹⁸⁵ the use of personal information for political microtargeting⁹⁸⁶ and the use of biometric data in certain contexts.⁹⁸⁷

The process of completing a privacy impact assessment (see Chapter 13) would assist entities to ensure that personal information handling is fair and reasonable in the circumstances. However, all collections, uses and disclosures of personal information, irrespective of whether a PIA is undertaken, would need to be fair and reasonable in the circumstances.

12.1 Amend the Act to introduce a requirement that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances.

It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.

12.3.3 Legislated factors for assessing fairness and reasonableness

Many submitters were of the view that the proposed legislated factors would be important to provide clarity as to how the requirement would be interpreted.⁹⁸⁸ The OAIC submitted that the factors would ensure that the test is interpreted by APP entities and the courts 'from a uniquely privacy law perspective'.⁹⁸⁹ OAIC guidance, and enforcement through determinations and judicial consideration, will map the contours of the fair and reasonable test over time. This has been successful in the context of Canada's 'appropriate purpose' test,⁹⁹⁰ which has produced case law⁹⁹¹ and regulatory guidance issued by the Office of the Privacy Commissioner of Canada (OPC Canada) that clarify the operation of the test.⁹⁹² Similarly, OAIC guidance could clarify practices that are generally likely to meet the test, including uncontentionous or socially beneficial practices, or practices that are likely to breach the test.

It was submitted that the factors should not be exhaustive,⁹⁹³ and that they should operate as interpretative considerations for whether data handling as a whole is fair.⁹⁹⁴ A small number of submissions proposed that each

983 ACCC, [DPI Report](#) 386-393; UK ICO, [Update Report into Adtech and Real Time Bidding](#) (Report, 20 June 2019) 20; Submissions to the Discussion Paper: [Dr Katharine Kemp, UNSW Sydney](#); [Centre for Media Transition](#); Submissions to the Issues Paper: [Consumer Policy Research Centre](#), 30. See also, Norwegian Consumer Council, *Out of Control: How Consumers are Exploited by the Online Advertising Industry*, (Report, January 2020). The Norwegian Consumer Council analysed 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.

984 ACCC, [DPI Report](#) 445-446; Submissions to the Discussion Paper: [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 9-13.

985 ACCC, [DPI Report](#) 445-448.

986 Ibid 446.

987 Submissions to the Discussion Paper: [Dr Ben Egliston, Lucinda Nelson and Dr Marcus Carter](#); AHRC, [Human Rights and Technology](#) (Final Report, March 2021) 116.

988 See for example Submissions to the Discussion Paper: [OAIC](#), 81; [Salinger Privacy](#), 21-22; [New South Wales Council for Civil Liberties](#), 19; [Privacy 108](#), 19; [Centre for Media Transition](#), 10.

989 Submission to the Discussion Paper: [OAIC](#), 81.

990 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 5(3).

991 See for example *Eastmond v Canadian Pacific Railway* [2004] FC 852; *Turner v Telus Communications Inc* [2005] FC 1601; *R v Spencer* [2014] 2 SCR 212; *AT v Globe24h.com* [2017] FC 114.

992 Office of the Privacy Commissioner of Canada, [Guidance on inappropriate data practices: Interpretation and application of subsection 5\(3\)](#) (Web Page, May 2018).

993 Submissions to the Discussion Paper: [OAIC](#), 81; [Deloitte Australia](#), 23; [Commonwealth Bank](#), 2; [Privacy 108](#), 19; [New South Wales Council for Civil Liberties](#), 19; [Equifax](#), 10; [Centre for Media Transition](#), 10; [Business Council of Australia](#), 7.

994 Submissions to the Discussion Paper: [OAIC](#), 81; [Services Australia](#), 9; [Telstra](#), 15; [Deloitte Australia](#), 23; [Helen Gregorcuk, University of Queensland](#), [Equifax](#), 10; [Centre for Media Transition](#), 10; [Avant Mutual](#), 9; [MIGA](#), 4.

legislative factor *should* have to be satisfied individually in each case,⁹⁹⁵ or that the factors should be addressed in OAIC guidance to allow for future flexibility.⁹⁹⁶ However, submitters generally agreed that the factors should not operate as standalone tests or requirements that have to be met in each case, as:

- this would promote a contextual assessment of fairness, which is needed as different circumstances will require a different balancing of factors,⁹⁹⁷ and
- a prescriptive list may draw attention away from the entity's consideration of the overall fairness of an activity.⁹⁹⁸

The ACL provides similar indicia of fairness in the context of the unfair terms regime,⁹⁹⁹ in addition to examples of contractual terms that may be unfair.¹⁰⁰⁰ In Canada, judicial consideration of the 'appropriate purpose' test in Section 5(3) of PIPEDA has developed factors for evaluating whether personal information handling complies with that provision, 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.¹⁰⁰¹

These factors have been proposed to be codified in legislation in Canada's Bill C-27.¹⁰⁰²

Legislated factors relevant to assessing fairness and reasonableness would provide APP entities with clarity in considering whether their acts and practices satisfy the test. Including the factors in legislation would provide binding guidance to the IC and the courts when applying the test in different factual circumstances. The legislative factors should be non-exhaustive and not operate as standalone tests, as different circumstances will require a balancing of different considerations to ensure a contextual assessment of fairness.

1) *Reasonable expectations*

This factor would require consideration of whether a reasonable individual would expect the personal information to be collected, used or disclosed in the circumstances. It is likely that a reasonable person would expect certain kinds of information to be subject to stronger standards of privacy protection, for example, sensitive information, location data or smart home data.¹⁰⁰³ The nature of the product or service offered and the purpose for which personal information is being collected, used or disclosed may also influence what a reasonable person would expect. A reasonable person may also expect a higher degree of privacy protection for services that are likely to be used by vulnerable cohorts of individuals, such as children.

Submissions to both the Issues Paper and Discussion Paper have argued that a description of how personal information will be handled in an entity's privacy policy *alone* is not enough for the entity to demonstrate that individuals could have reasonably expected it.¹⁰⁰⁴ Submitters raised concerns about the possibility of intrusive data-handling practices going unchallenged as unduly influencing the assessment of this factor.¹⁰⁰⁵ This concern has also been raised in the context of the legitimate interests lawful basis assessment under the GDPR.¹⁰⁰⁶ In this regard the ALRC has noted that, while '[c]ommunity expectations of privacy no doubt change... [p]rivacy has been valued by so many for so long that not only is it not dead, as some have dramatically claimed, but it should continue to be reasonable to expect privacy in many circumstances'.¹⁰⁰⁷

⁹⁹⁵ Submissions to the Discussion Paper: [Calabash Solutions](#), 14; [Dr Katharine Kemp, UNSW Sydney](#), 13-14.

⁹⁹⁶ Submissions to the Discussion Paper: [KPMG](#), 18; [Commonwealth Bank](#), 2; [Deloitte Australia](#), 23; [Centre for AI and Digital Ethics](#), 6.

⁹⁹⁷ Submissions to the Discussion Paper: [OAIC](#), 81; [MIGA](#), 4; [Deloitte Australia](#), 23; [Salinger Privacy](#), 21-22.

⁹⁹⁸ Submissions to the Discussion Paper: [Deloitte Australia](#), 23; [Helen Gregorcuk, University of Queensland](#), [Equifax](#), 10; [Avant Mutual](#), 9.

⁹⁹⁹ *Competition and Consumer Act 2010* (Cth) sch 2, s 24.

¹⁰⁰⁰ *Ibid* s 25.

¹⁰⁰¹ *Turner v Telus Communications Inc* [2005] FC 1601, [48].

¹⁰⁰² [Bill C-27](#), s 12(2).

¹⁰⁰³ See, Discussion Paper Submission: [OAIC](#), 82; [ACCC](#), [DPI Report](#) 385-386; [OAIC](#), [Australian Community Attitudes to Privacy Survey 2020](#) (Report, September 2020): The 2020 ACAP Survey indicated that 62 per cent of respondents felt uncomfortable about digital platforms and other online businesses tracking their location.

¹⁰⁰⁴ Submission to the Discussion Paper: [New South Wales Council for Civil Liberties](#), 18-19; Submission to the Issues Paper: [The Allens Hub for Technology, Law and Innovation and the Australian Society for Computers and Law](#), 7.

¹⁰⁰⁵ Submissions to the Discussion Paper: [Public Health Association of Australia](#), 7; [Financial Rights Legal Centre and Financial Counselling Australia](#), 9.

¹⁰⁰⁶ Irene Kamara and Paul De Hert, [Understanding the Balancing Act behind the Legitimate Interests of the Controller Ground: A Pragmatic Approach](#) (Working Paper, August 2018) 17.

¹⁰⁰⁷ ALRC Report 123, ['A test for what is private'](#) [6.17].

2) *Kinds, sensitivity and amount of personal information*

The second factor recognises that a reasonable person would consider it fair and reasonable for certain types of information to be treated with a higher degree of care. The OAIC proposed that this factor should also refer to 'kinds' of personal information (in addition to sensitivity and amount) to better align with the NDB scheme's factors for determining whether serious harm is likely to occur as a result of a data breach.¹⁰⁰⁸

Telstra proposed that 'sensitivity' should be construed as a reference to the current legislative definition of sensitive information.¹⁰⁰⁹ However, similar to the position under the NDB scheme, sensitivity may encompass sensitive information as defined in section 6 or other information that would be considered 'sensitive' according to the ordinary meaning of the term.¹⁰¹⁰

This factor would also take into account the amount of personal information collected, used and disclosed, which would support the principle of data minimisation.¹⁰¹¹ Privacy risks can be reduced or avoided when a data minimisation approach is adopted.

3) *Functions and activities of the entity*

The third factor recognises the importance of the functions and activities of the entity, and the objective that the entity is trying to achieve, in determining whether a reasonable person would consider personal information handling to be fair. It would require consideration of whether a proposed collection, use or disclosure is reasonably necessary for the functions and activities of the agency. This is a crucial aspect of the balance that must be reached between the interests of the APP entity and the individual. This factor recognises that individuals do not have an absolute interest in privacy and that in many cases, personal information handling activities provide benefits to society.

For example, the processing of personal information may be an important part of securing societal interests such as the health and safety of other individuals, or for socially beneficial healthcare research. Similarly, APP entities may be required to process personal information as part of delivering critical services such as banking or telecommunications, or for processing payment for products and services that they have offered to consumers. It is envisaged that a reasonable person would consider it fair and appropriate for these legitimate and important practices to be undertaken.

OAIC guidance could list practices that will ordinarily meet the fair and reasonable personal information handling test, including legitimate business activities such as fraud detection and prevention; monitoring, detecting, and protecting a network with cybersecurity measures and updating products and services to ensure they are safe, accurate and reliable.¹⁰¹²

4) *Risk of unjustified adverse impact or harm*

This factor would require consideration of the risk of unjustified adverse impact or harm that personal information handling poses to individuals. The nature, seriousness and likelihood of the risk materialising from the activities of the APP entity are likely to influence a reasonable person's view on whether the personal information handling is fair and reasonable. It may be the case that some services pose a low level of risk that a reasonable person would consider appropriate, whereas other services may pose a *cumulatively* unacceptable risk.

This factor would recognise the privacy harms that can sometimes result from the handling of personal information, which could include:

- direct or indirect financial loss
- physical, psychological or emotional 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.¹⁰¹³

1008 Submission to the Discussion Paper: [OAIC](#), 82.

1009 Submission to the Discussion Paper: [Telstra](#), 15.

1010 Privacy Act s 26WG; Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 [Cth] 73.

1011 See relatedly, 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.

1012 See relatedly, Submission to the Discussion Paper: [BSA | The Software Alliance](#), 9.

1013 Data Synergies, [Privacy Harms: A paper for the Office of the Australian Information Commissioner](#) [June 2020] 43.

Data protection regulators in Singapore and the UK¹⁰¹⁴ have acknowledged that personal data handling that exposes individuals to harm or adverse impacts may contravene their appropriate purpose or fairness requirements, respectively.

The reference to '*unjustified*' adverse impact or harm acknowledges that at times, the handling of personal information is needed to fulfil societal interests which are not always advantageous to the individual concerned. Guidance issued by the UK ICO provides that '[p]ersonal data may sometimes be used in a way that negatively affects an individual without this necessarily being unfair' and that '[w]hat matters is whether or not such detriment is justified.'¹⁰¹⁵ For example, personal information which is collected, used and disclosed to administer Australia's taxation system or for law enforcement may have an adverse, albeit in some cases justified, consequence for the individual concerned.¹⁰¹⁶

5) *Whether the impact on privacy is proportionate to the benefits*

This factor would assess whether any impact on privacy is proportionate to the benefit. This factor is linked to factors 3 and 4 above, insofar as the objective that the entity is trying to achieve must be balanced against its risks. The impact may be on a single individual or many individuals and the benefit may be to the affected individual(s) or some other party, including the APP entity. The distribution of impact and benefit would be relevant, particularly where it was unequal as between the APP entity and individuals.

The following matters could be included in explanatory memorandum as matters that are relevant to the application of this factor:

- (a) whether the collection, use or disclosure intrudes to an unreasonable extent upon the personal affairs of the affected individual
- (b) whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits,¹⁰¹⁷ and
- (c) any actions or measures taken by the entity to mitigate impacts to privacy.

6) *Transparency of the collection, use or disclosure*

It was argued that this factor would be of limited benefit, as APP 1 and APP 5 already require entities to be transparent in how they handle personal information.¹⁰¹⁸ The OAIC did not support this factor on the basis the test should focus on the substantive impacts of APP entities' activities and whether they are proportionate.¹⁰¹⁹

7) *Best Interests of the Child*

This factor would 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 16.

8) *The objects of the Act*

The final factor would enable consideration of the objects of the Act when assessing whether a reasonable person would consider a collection, use or disclosure to be fair in the circumstances. In light of proposal 3.2, which would recognise the public interest in privacy in the objects of the Act, this would ensure that an appropriate and proportionate balance is struck between the public interest in protecting the privacy of individuals,¹⁰²⁰ the interests of APP entities and other public interests.

1014 Personal Data Protection Commission (SG), [Advisory Guidelines on Key Concepts in the Personal Data Protection Act](#) (February 2021); UK ICO, [Lawfulness, fairness and transparency](#) (Web Page, January 2021).

1015 Ibid.

1016 Submissions to the Discussion Paper: [Australian Federal Police](#), 7. See relatedly, [Equifax](#), 10.

1017 *Turner v Telus Communications Inc* [2005] FC 1601, [48]; [Bill C-27](#), s 12(2); 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).

1018 Submissions to the Discussion Paper: [Department of Health \(Cth\)](#), 9; [Meta](#), 30.

1019 Submission to the Discussion Paper: [OAIC](#), 85.

1020 Ibid 86.

12.2 In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account:

- (a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances**
- (b) the kind, sensitivity and amount of personal information being collected, used or disclosed**
- (c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency**
- (d) the risk of unjustified adverse impact or harm**
- (e) whether the impact on privacy is proportionate to the benefit**
- (f) 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, and**
- (g) the objects of the Act.***

The EM would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include:

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

*The final wording of any legislative provisions will be developed through the legislative drafting process.

12.4 Integration with existing APP 3 and APP 6 requirements

The Discussion Paper sought feedback on whether the situations contemplated by APPs 3.4 and 6.2 in relation to sensitive information and secondary purposes should be subject to the overarching fair and reasonable test. It was proposed that on balance, 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.¹⁰²¹ It was submitted that the Act's existing exceptions should remain unchanged, as these are often relied on for secondary uses and disclosures by APP entities (for example, the law enforcement exception).¹⁰²²

¹⁰²¹ [Discussion Paper](#), 91.

¹⁰²² See also Submission to the Discussion Paper: [Services Australia](#), 7.

Aside from consent and the exception in APP 6.2(a), the fair and reasonable test should not apply to the exceptions in APPs 3.4 and 6.2(b)-(e). As stated in the Discussion Paper, many of these exceptions already incorporate concepts of reasonableness, making the fair and reasonable test unnecessary.¹⁰²³ In relation to personal information handling that is legally required or authorised, such as disclosures made in accordance with the CDR scheme, the appropriate safeguards are already provided through the scrutiny of the parliament in passing legislation and judicial interpretation in the development of case law which underpin the exception.

The Discussion Paper also sought feedback on how the test would interact with the consent exceptions in APPs 3.3 and 6.1(a). A number of submitters suggested the baseline test should apply regardless of whether consent has been obtained from an individual.¹⁰²⁴ The OAIC considered that while an entity should not be able to 'consent out' of the fair and reasonable test, it may still be relevant to the question of whether data handling is fair.¹⁰²⁵

This approach would mirror the operation of the overarching fairness principle in GDPR. In this regard, the EDPB 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'.¹⁰²⁶

The need to ensure that information-handling practices are fair and reasonable notwithstanding that consent has been obtained is significant in light of the use of 'dark patterns' by digital platforms which may nudge users towards choosing more privacy intrusive settings.¹⁰²⁷ The EDPB has issued guidance stating that if an 'the interface has insufficient or misleading information for the user and fulfils the characteristics of dark patterns, it can be classified as unfair'.¹⁰²⁸

It is also important that the test apply even where consent has been obtained to enable scrutiny of entities' information-handling practices where consent is made a condition of accessing a service. In these circumstances, where individuals feel they have no option but to consent, the fair and reasonable test would be an important safeguard against potentially harmful and invasive practices which go beyond what is reasonably necessary to provide the service.

The fair and reasonable requirement should replace the reference to a 'fair means' of collection in APP 3.5. 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'.¹⁰²⁹ APP 3.5 would therefore be replaced by a broader test which is not limited to the *means* of collection and applies to the use and disclosure of personal information,¹⁰³⁰ and would allow for a holistic assessment of the means, purposes and impacts of information handling.¹⁰³¹

12.3 The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained.

The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to the exceptions in APPs 3.4 and 6.2(b)-(e).

The reference to a 'fair means' of collection in APP 3.5 should be repealed.

¹⁰²³ See s 16A and 16B which include requirements for reasonable belief and reasonable necessity.

¹⁰²⁴ Submissions to the Discussion Paper: [Office of the Victorian Information Commissioner](#); [Electronic Frontiers](#); [Salinger Privacy](#); [New South Wales Council for Civil Liberties](#); [OAIC](#); [Castan Centre](#); [Dr Katharine Kemp](#), UNSW Sydney; [elevenM](#).

¹⁰²⁵ Submission to the Discussion Paper: [OAIC](#), 89-90.

¹⁰²⁶ European Data Protection Board, [Guidelines 05/2020 on consent under Regulation 2016/679](#), 5. See relatedly, European Data Protection Board, [Guidelines 8/2020 on the targeting of social media users](#), 18.

¹⁰²⁷ See for example Submission to the Discussion Paper: [Salinger Privacy](#), 29-30.

¹⁰²⁸ European Data Protection Board, [Guidelines 3/2022 on Dark patterns in social media platform interfaces](#), 8-9.

¹⁰²⁹ See relatedly, *Griffiths v Rose* [2011] FCA 30.

¹⁰³⁰ ACCC, [DPI Report](#) Recommendation 17(3), 478.

¹⁰³¹ Submission to the Discussion Paper: [OAIC](#), 89.

13. Additional protections

Certain types of personal information handling pose higher privacy risks to individuals. A broad range of submitters to the Review considered that high-risk practices should be more stringently regulated in the Privacy Act.¹⁰³²

13.1 High-risk practices

The Discussion Paper sought feedback on whether it would be desirable to ‘restrict’ certain high-risk practices in the Act. It set out a list of possible high-risk practices and proposed two models for how they could be regulated:

- **Option 1:** APP entities that engage in restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks.
- **Option 2:** Improve an individual’s ability to self-manage their privacy in relation to restricted practices. Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted practices, or by ensuring that explicit notice for restricted practices is mandatory.

A broad range of submitters to the Discussion Paper were supportive of Option 1,¹⁰³³ as it would require APP entities to hold more responsibility for proactively identifying and mitigating privacy risks on an ongoing basis.¹⁰³⁴ Some submitters expressly preferred Option 1 to Option 2 on the basis that APP entities should be accountable for the risks of their personal information handling practices, as opposed to placing the burden on individuals to self-manage their privacy.¹⁰³⁵ It was also suggested that the two options are not mutually exclusive and that both should be pursued.¹⁰³⁶

This chapter considers new requirements that could be placed on APP entities to manage high risk activities, as per Option 1. Chapters 4, 18 and 19 of this report consider the measures that were contemplated by Option 2, which will enable individuals to exercise greater control over their information.

13.1.1 Current requirements to identify and mitigate risks to privacy

An obligation to identify and mitigate privacy risk, as contemplated by Option 1, already exists in the Act to some degree. As outlined in Chapter 15, APP 1.2 requires that APP entities take such steps as are reasonable in the circumstances to implement practices, procedures and systems to ensure compliance with the APPs.¹⁰³⁷ This principle has been supplemented with OAIC-issued guidance which provides that APP entities should consider implementing, among other measures:¹⁰³⁸

- procedures for identifying and managing privacy risks at each stage of the information lifecycle,
- PIAs for new projects in which personal information will be handled, or when a change is proposed to existing personal information handling practices.

Compliance with APP 1.2 – agencies

The Privacy (Australian Government Agencies – Governance) APP Code 2017 (AGA Code) prescribes the steps that Australian government agencies must take to comply with APP 1.2. Agencies that undertake ‘high privacy risk projects’ are required to complete a PIA under the AGA Code. A PIA is a systematic assessment that identifies the impact that a project might have on the privacy of individuals and sets out recommendations for managing, minimising, or eliminating that impact.¹⁰³⁹

1032 Submissions to the Discussion Paper: [Law Council of Australia](#), [OAIC](#); [Office of the Victorian Information Commissioner](#); [The Australia Institute – Centre for Responsible Technology](#); [Salinger Privacy](#); [Foundation for Alcohol Research and Education](#); [Deloitte Australia](#); [Consumer Policy Research Centre](#); [Dr Henry Fraser](#); [Privacy 108](#); [ResMed](#); [Minderoo Tech & Policy Lab](#), [UWA Law School](#); [National Australia Bank](#); [Guardian Australia](#); [Australian Privacy Foundation](#); [Equifax](#); [Centre for AI and Digital Ethics](#); [Centre for Media Transition](#); [Digital Rights Watch](#); [Castan Centre](#); [Digital Law Association](#); [CHOICE](#); [Obesity Policy Coalition](#).

1033 Submissions to the Discussion Paper: [Law Council of Australia](#); [OAIC](#); [Australian Banking Association](#); [Deloitte Australia](#); [Snap Inc](#); [Consumer Policy Research Centre](#); [National Australia Bank](#); [Google](#); [Equifax](#); [Centre for Media Transition](#); [Castan Centre](#); [Digital Law Association](#); [DIGI](#); [Woolworths](#); [ANZ](#); [Meta](#).

1034 Submissions to the Discussion Paper: [Deloitte Australia](#), 25. See relatedly, [Centre for Media Transition](#), 11; [Digital Rights Watch](#), 13-15; [Castan Centre](#), 18-19; [CHOICE](#), 11.

1035 Submissions to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 6; [Consumer Policy Research Centre](#), 5; [Privacy 108](#), 22-23; [Digital Rights Watch](#), 13-15; [Google](#), 3; [Centre for Media Transition](#), 11. See relatedly, [Deloitte Australia](#), 25; [Australian Privacy Foundation](#), 10; [Castan Centre](#), 18-19; [DIGI](#), 16-17; [ANZ](#), 22; [CHOICE](#), 11.

1036 Submissions to the Discussion Paper: [New South Wales Council for Civil Liberties](#), 20-21; [Dr Henry Fraser](#), 5.

1037 Privacy Act sch 1, APP 1.2(a).

1038 OAIC, [APP Guidelines](#) (July 2019) [1.7].

1039 Privacy Act s 33D(3); see also, OAIC, [When do agencies need to conduct a privacy impact assessment?](#) (Web Page, 14 September 2020); OAIC, [Guide to undertaking privacy impact assessments](#) (Web Page, 2 September 2020); UK ICO, [Data Protection Impact Assessments](#) (Web Page, January 2021).

Under the AGA code, a 'high privacy risk project' is defined as one which involves any new or changed ways of handling personal information that are 'likely to have a significant impact on the privacy of individuals'.¹⁰⁴⁰ A 'significant impact' may be for one individual or a group of individuals, including for example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft.¹⁰⁴¹ OAIC guidance provides that agencies should consider undertaking a 'threshold assessment' to screen potentially high privacy risk projects to determine whether a PIA is required.¹⁰⁴² The IC may also direct an agency to undertake a PIA.¹⁰⁴³ Agencies must maintain a register of the PIAs that they have completed on their website.¹⁰⁴⁴

Compliance with APP 1.2 – organisations

While there is no express requirement in the Act for organisations to undertake PIAs, several recent IC determinations have interpreted APP 1.2 as requiring an organisation to complete a PIA before commencing certain high privacy risk activities. In October 2021, the IC issued a determination following a Commissioner-initiated investigation into the personal information handling practices of Clearview AI, Inc (Clearview), including the use of scraped personal information from the internet and biometrics for facial recognition.¹⁰⁴⁵ In addition to finding breaches of APP 3.3 and 5, the IC determined that it would have been a 'reasonable step' under APP 1.2 for Clearview to have conducted a PIA before allowing user access to its facial recognition tool.¹⁰⁴⁶ In December 2020, the failure of Flight Centre Travel Group to undertake a PIA prior to disclosing the personal information of customers to third parties contributed to a finding that it had breached APP 1.2.¹⁰⁴⁷

13.1.2 Introducing an express requirement to identify and mitigate privacy risks

Submissions generally agreed that APP entities that engage in high risk practices should be required to identify privacy risks and implement measures to mitigate those risks.¹⁰⁴⁸ Submitters considered that PIAs are an effective tool for achieving this, as they provide a systematic framework for entities to assess and address risks which can be used to manage the entity's compliance over time.¹⁰⁴⁹

The Law Council of Australia submitted that PIAs increase 'community confidence that emerging, higher risk practices are clearly identified as such, with tighter regulation and oversight' and considered that PIAs are analogous to environmental impact assessments that are required under environmental protection legislation.¹⁰⁵⁰ Woolworths submitted that PIAs allow them to address privacy risks in a meaningful way, and encourages them to ask 'should we?' questions, which promotes the ethical and responsible use of data.¹⁰⁵¹ Digital Rights Watch submitted that PIAs can be important documents for privacy researchers and civil society organisations to access, to hold organisations accountable, and also offer the OAIC additional documentation to support investigations.¹⁰⁵²

Under GDPR, data protection impact assessments (DPIAs) are required prior to undertaking:

- 'systematic and extensive' automated evaluation of individuals, including profiling, on which decisions are based that produce a legal or similarly significant effect
- the large-scale processing of special categories of data
- the systemic monitoring of a publicly accessible area on a large scale, or
- personal data processing that is otherwise likely to result in a high risk to the rights and freedoms of natural persons.¹⁰⁵³

¹⁰⁴⁰ Privacy (Australian Government Agencies – Governance) APP Code 2017 (Cth) cl 12.

¹⁰⁴¹ OAIC, [When do agencies need to conduct a privacy impact assessment?](#) (Web Page, 14 September 2020).

¹⁰⁴² Ibid.

¹⁰⁴³ Privacy Act s 33D.

¹⁰⁴⁴ Privacy (Australian Government Agencies – Governance) APP Code 2017 (Cth) cl 15.

¹⁰⁴⁵ OAIC, [OAIC and ICO conclude joint investigation into Clearview AI](#) (Web Page, 3 November 2021).

¹⁰⁴⁶ Clearview [Determination](#), [229]–[234]; see relatedly, 7-Eleven [Determination](#), [103].

¹⁰⁴⁷ Flight Centre Travel Group (Privacy) [2020] AICmr 57 [25 November 2020] [101]–[116].

¹⁰⁴⁸ Submissions to the Discussion Paper: [Law Council of Australia](#); [OAIC](#); [Australian Banking Association](#); [Deloitte Australia](#); [Snap Inc](#); [Consumer Policy Research Centre](#); [National Australia Bank](#); [Google](#); [Equifax](#); [Centre for Media Transition \(UTS\)](#); [Castan Centre](#); [Digital Law Association](#); [DIGI](#); [Woolworths](#); [ANZ](#); [Meta](#).

¹⁰⁴⁹ Submissions to the Discussion Paper: [Law Council of Australia](#); [Salinger Privacy](#); [Snap Inc](#); [The Australia Institute – Centre for Responsible Technology](#); [New South Wales Council for Civil Liberties](#); [Centre for AI and Digital Ethics](#); [Australian Banking Association](#); [ResMed](#); [Privacy 108](#); [National Australia Bank](#); [Australian Privacy Foundation](#); [Equifax](#); [Woolworths](#); [CHOICE](#). See relatedly, [Western Union](#).

¹⁰⁵⁰ Submission to the Discussion Paper: [Law Council of Australia](#), 14–15.

¹⁰⁵¹ Submission to the Discussion Paper: [Woolworths](#), 9.

¹⁰⁵² Submission to the Discussion Paper: [Digital Rights Watch](#), 14.

¹⁰⁵³ GDPR art 35(1), [3].

European data protection authorities must also publish lists of processing activities for which DPIAs are mandatory.¹⁰⁵⁴ For example, the UK ICO has issued guidelines that require DPIAs to be conducted where an entity uses profiling, ADM or special category data to decide on access to a service, opportunity or benefit and the use of biometric or genetic data in certain situations, among other circumstances.¹⁰⁵⁵ Several submitters to this Review supported the recognition of the GDPR's DPIA requirement in Australian law.¹⁰⁵⁶ National Australia Bank supported a requirement to undertake PIAs in relation to high risk practices, and suggested that the circumstances that should trigger a PIA requirement be aligned with Article 35(3) GDPR.¹⁰⁵⁷

Proposal 11.1 of the Discussion Paper included a list of specific high risk activities that could be subject to a requirement to mitigate privacy risks.¹⁰⁵⁸ Some submissions expressed support for this list of practices¹⁰⁵⁹ or proposed an alternative list of restricted practices.¹⁰⁶⁰ Other submitters considered that the proposed list of practices contained activities that were not inherently high risk.¹⁰⁶¹ By contrast, several submitters argued that some of the proposed 'restricted' practices should in fact be prohibited.¹⁰⁶² In this regard, Professor Graham Greenleaf argued that a legislated list of practices would 'impliedly legitimate some practices which it can be argued should be prohibited.'¹⁰⁶³ It was suggested that a list of legislated high risk practices may become dated or could require frequent legislative revision to respond to emerging technologies and privacy risks,¹⁰⁶⁴ and it was considered that APP codes or OAIC guidance may provide a more appropriate mechanism to address specific practices.¹⁰⁶⁵

Proposal – privacy impact assessments for high-risk activities

It is proposed that all APP entities be required to complete a PIA prior to undertaking a 'high privacy risk activity', which could be defined as any function or activity that is likely to have a significant impact on the privacy of individuals. This test would align with the circumstances in which a PIA is required under the AGA Code.¹⁰⁶⁶ The test could be supplemented with OAIC guidance that articulates factors that may indicate high privacy risks, and provides examples of activities that will generally require a PIA to be performed.¹⁰⁶⁷ The Act could also specify certain acts or practices for which a PIA is required, similar to Article 35 GDPR.¹⁰⁶⁸ An indicative list of high privacy risk activities that could be listed in the Act or OAIC guidance could include:¹⁰⁶⁹

- 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
- online tracking, profiling and the delivery of personalized content and advertising to individuals
- ongoing or real-time tracking of an individual's geolocation
- the use of biometric templates or biometric information for the purpose of verification or identification, or when collected in publicly accessible spaces (see Proposal 13.2, below)
- the sale of personal information, and
- the collection, use or disclosure of personal information for the purposes of ADM with legal or significant effects.¹⁰⁷⁰

¹⁰⁵⁴ Ibid art 35(4).

¹⁰⁵⁵ UK ICO, [Data Protection Impact Assessments](#) (Web Page, January 2021).

¹⁰⁵⁶ Submissions to the Discussion Paper: [Australian Banking Association](#), 19; [The Australia Institute – Centre for Responsible Technology](#), 7-8; [Salinger Privacy](#), 27-29; [New South Wales Council for Civil Liberties](#), 21; [ResMed](#), 5; [Meta](#), 32.

¹⁰⁵⁷ Submission to the Discussion Paper: [National Australia Bank](#), 6. See also, [Australian Banking Association](#), 19.

¹⁰⁵⁸ [Discussion Paper](#), 95.

¹⁰⁵⁹ Submissions to the Discussion Paper: [New South Wales Council for Civil Liberties](#), 22; [OAIC](#), 104; [Consumer Policy Research Centre](#), 5; [Western Union](#), 6; [Privacy 108](#), 22; [Castan Centre](#), 19.

¹⁰⁶⁰ Submissions to the Discussion Paper: [Salinger Privacy](#), 27-29; [CHOICE](#), 12. See also, [Digital Rights Watch](#), 14; [Australian Privacy Foundation](#), 10.

¹⁰⁶¹ Submissions to the Discussion Paper: [ANZ](#), 22; [Australian Banking Association](#), 19; [Optus](#), 20; [Experian](#), 16.

¹⁰⁶² Submissions to the Discussion Paper: [Graham Greenleaf, UNSW Sydney](#), 4; [Obesity Policy Coalition](#), 9; [Salinger Privacy](#), 29; [Foundation for Alcohol Research and Education](#), 14; [CHOICE](#), 12.

¹⁰⁶³ Submission to the Discussion Paper: [Graham Greenleaf, UNSW Sydney](#), 4.

¹⁰⁶⁴ Submissions to the Discussion Paper: [KPMG](#), 19; [Microsoft](#), 5; [IAB](#), 26. See relatedly, [Digital Law Association](#), 14.

¹⁰⁶⁵ Submissions to the Discussion Paper: [KPMG](#), 19; [Microsoft](#), 5.

¹⁰⁶⁶ Privacy (Australian Government Agencies – Governance) APP Code 2017 (Cth) cl 12. See also, Privacy Act, s 33D.

¹⁰⁶⁷ See, e.g., OAIC, [When do agencies need to conduct a privacy impact assessment?](#) (Web Page, 14 September 2020). This existing guidance for the Privacy (Australian Government Agencies – Governance) APP Code 2017 could be further developed for the purposes of a PIA requirement in the Privacy Act that applies to all APP entities, including private sector organisations..

¹⁰⁶⁸ GDPR art 35(1), (3).

¹⁰⁶⁹ See relatedly, Submissions to the Discussion Paper: [OAIC](#), 104. See also, [New South Wales Council for Civil Liberties](#); [Consumer Policy Research Centre](#); [Western Union](#); [Privacy 108](#); [Castan Centre](#).

¹⁰⁷⁰ The development of factors for inclusion in the Act or OAIC Guidance relevant to when an activity may be high risk would consider relevant context, such as research conducted in the public interest.

In completing a PIA, APP entities should identify and assess possible impacts to privacy that may result from the proposed high-risk activity.¹⁰⁷¹ Entities should also consider whether these privacy impacts are proportionate, as well as whether the proposed project would comply with the Privacy Act.¹⁰⁷² Finally, entities should identify and implement any available options to mitigate or eliminate the impacts to privacy that were identified earlier in the PIA process.¹⁰⁷³

OAIC guidance could also detail measures that entities should consider implementing to mitigate privacy risks, which could include collecting less personal information or using de-identified information.¹⁰⁷⁴ This guidance could detail the practical steps that would be appropriate for specific practices, such as the ongoing or real-time tracking of an individual's geolocation.¹⁰⁷⁵ Practice-specific APP codes could also be developed by the OAIC to create enforceable requirements (see Chapter 5).¹⁰⁷⁶

A possible outcome of a PIA could be that the privacy impacts are so significant that the proposed activity should not proceed. In addition to a breach of APP 1, entities that fail to undertake a PIA before commencing a high-risk activity, or fail to mitigate identified impacts to privacy to a reasonable extent, may be at risk of breaching other APPs or the proposed fair and reasonable personal information handling test (see Chapter 12).¹⁰⁷⁷ A PIA, once completed, should be retained and reviewed as necessary. It may be best practice in some circumstances for entities to conduct a periodic independent audit to ensure they continue to identify privacy risks and have taken appropriate steps to mitigate those risks.¹⁰⁷⁸ An entity would be required to produce a PIA on request by the IC as part of an assessment or other enforcement process.

This proposal would supplement APP 1.2 and would provide improved privacy protections for individuals and more certainty for organisations as to when a PIA is required. Consideration could be given to whether some small businesses that are covered by the Act, or may become covered by the Act in the future should the small business exemption be removed, should be exempted from the PIA requirement on the basis that they are less able to absorb its associated regulatory costs. The Department of Industry, Science and Resources is seeking feedback on a proposal to require impact assessments to be undertaken if there is a medium or high risk of adverse impacts from an AI or ADM application. The proposed requirement would be mandatory for Commonwealth agencies, and voluntary for private sector organisations. Consideration should be given to how to streamline the requirements for activities that would require both an impact assessment and a PIA to avoid placing duplicative obligations on APP entities.

13.1 APP entities must conduct a privacy impact assessment for all activities with high privacy risks.

- **A privacy impact assessment should be undertaken prior to the commencement of the high-risk activity.**
- **An entity should be required to produce a privacy impact assessment to the OAIC on request.**
- **The Privacy Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals.' OAIC guidance should be developed which articulates factors that may indicate a high privacy risk, and provides examples of activities that will generally require a privacy impact assessment to be completed. Specific high-risk practices could also be set out in the Act.**

1071 See, OAIC, [Guide to undertaking privacy impact assessments](#) (Web Page, 2 September 2020); UK ICO, [Data Protection Impact Assessments](#) (Web Page, January 2021).

1072 Ibid.

1073 Ibid.

1074 See, Submission to the Discussion Paper: [OAIC](#), 97.

1075 Ibid.

1076 Ibid.

1077 Ibid. See also, Submission to the Discussion Paper: [Salinger Privacy](#), 35.

1078 See relatedly, Submission to the Discussion Paper: [OAIC](#), 98.

13.1.3 Facial recognition technology and biometrics

Facial recognition is a form of biometric technology that involves the use of an individual's physical facial features to identify them, or infer characteristics about them.¹⁰⁷⁹ The use of facial recognition technology (FRT) in some contexts has prompted public concern¹⁰⁸⁰ about its impacts on individual privacy and human rights.¹⁰⁸¹ For example, the AHRC has observed that FRT may be used to infer information about an individual's mood or personality traits.¹⁰⁸² Some forms of FRT may be inaccurate and can produce high error rates for individuals of a particular racial group, gender or other protected trait.¹⁰⁸³ This can result in unlawful discrimination or significant impacts to individuals where an FRT application is used to directly make decisions about an individual's rights or entitlements.¹⁰⁸⁴

The level of risk to privacy and human rights that a particular FRT application poses will depend on the nature of the application itself and the way in which it is deployed. For example, 'one-to-one' matching confirms whether a single headshot photograph matches a different photograph of the same person held by that entity.¹⁰⁸⁵ On the other hand, 'one-to-many' matching is considered to be more privacy intrusive,¹⁰⁸⁶ as it involves comparing a person's face against a database of stored biometric information of many individuals.¹⁰⁸⁷ Different use cases for FRT may also pose different levels of risk to human rights. For example, the use of FRT to authenticate access to a smart phone¹⁰⁸⁸ may pose less risk than the use of FRT to analyse a prospective employee's mood and personality traits.¹⁰⁸⁹

In March 2021, the AHRC recommended that Australia's federal, state and territory governments introduce legislation to regulate the use of FRT and other biometric technology to expressly protect human rights, which would apply to decisions that have a legal, or similarly significant effect for individuals or where there is a high risk to human rights.¹⁰⁹⁰

In September 2022, the UTS Human Technology Institute released a Model Law for the regulation of FRT (UTS Model Law).¹⁰⁹¹ The UTS Model Law takes a risk-based approach to restrict and, in some cases prohibit, FRT by requiring entities that use or develop FRT systems to assess and address privacy and human rights impacts through a Facial Recognition Impact Assessment (FRIA). The UTS Model Law proposes to apply legal requirements that are calibrated to the assessed risk level of the particular FRT application. These legal requirements include compliance with an FRT technical standard, completion and publication of a 'Stage 2' FRIA that outlines the proposed functionality and technical limitations of the FRT system, and prohibiting high-risk FRT uses unless an exception applies. The UTS Model Law also proposes transparency requirements for all FRIAs through registration with a regulator and publication in a searchable repository made available to the public.¹⁰⁹²

In essence, the UTS Model Law contemplates an enhanced risk assessment process for FRT in light of the sensitivity of face data, which can hold a 'concentration of important, sensitive information about people – data that can reveal or store information about someone's gender, age, ethnicity, health conditions, emotional state, and behaviour'.¹⁰⁹³ While it is proposed that PIAs should be required for all high-risk practices (Proposal 13.1) there may be merit in adopting the enhanced risk assessment process set out in the UTS Model Law given the special nature of face data and the particular risks posed by FRT. Future work will be undertaken to consider the UTS Model Law in further detail and determine the extent to which the UTS Model Law could be accommodated into the Privacy Act framework.

Further consultation will be required to determine if there are other uses of biometric information that should attract additional obligations under the Act or another regime. This will require an assessment of the risks posed by different uses of biometric information and the most appropriate regulation to address these potential harms. As

1079 AHRC, *Human Rights and Technology* (Final Report, March 2021) 111-2.

1080 Simran Gill, 'CHOICE raises concern over Bunnings, Kmart and the Good Guys use of facial recognition technology', *ABC News* (online), 15 June 2022; OAIC, *Australian Community Attitudes to Privacy Survey 2020* (Report, September 2020) 81-5.

1081 See relatedly, Clearview *Determination*; 7-Eleven *Determination*.

1082 AHRC, *Human Rights and Technology* (Final Report, March 2021) 111. See also, European Data Protection Supervisor, *Facial Emotion Recognition* (26 May 2021).

1083 *Ibid.*

1084 *Ibid.*

1085 *Ibid.* 113. Submission to the Discussion Paper: [OAIC](#), 112.

1086 *Ibid.*

1087 AHRC, *Human Rights and Technology* (Final Report, March 2021) 113.

1088 *Ibid.* 113. Submission to the Discussion Paper: [OAIC](#), 112.

1089 Drew Harwell, 'A face-scanning algorithm increasingly decides whether you deserve the job', *The Washington Post* (online), 6 November 2019.

1090 AHRC, *Human Rights and Technology* (Final Report, March 2021) 116.

1091 Human Technology Institute (UTS), *Facial recognition technology: Towards a model law* (Report, September 2022).

1092 *Ibid.*

1093 *Ibid.* 14.

noted in Chapter 4, biometric information is sensitive information if it is used for the purpose of automated biometric verification or identification. Other biometric information that is not a template or used for automated biometric identification but which can identify an individual will be personal information. However, not all biometric information will meet the threshold of reasonably identifiable required for personal information but the use of this information may still pose risks to individuals. Consideration of how best to regulate biometric technologies into the future will require a coordinated approach across government.

13.2 Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require privacy impact assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies.

13.1.4 Guidance on high risk practices

The development of practice-specific OAIC guidance for high privacy risk activities may be beneficial to provide clarity to regulated entities in more prescriptive and technology-specific terms.¹⁰⁹⁴ Practice-specific guidance is already commonly issued in Australia and overseas. For example, the OAIC has recently issued guidance for specific contexts including:

- privacy guidance for businesses collecting COVID-19 vaccination information¹⁰⁹⁵
- guidance for businesses collecting personal information for contact tracing,¹⁰⁹⁶ and
- posting photos and videos.¹⁰⁹⁷

The UK ICO has issued guidance on AI,¹⁰⁹⁸ direct marketing¹⁰⁹⁹ and political campaigning,¹¹⁰⁰ among other matters. Additional guidance of this nature could assist entities to comply with the Act, including the proposed fair and reasonable personal information handling test. Practice-specific OAIC guidance could address emerging privacy risks and technologies, including the indicative list of high privacy risk activities set out for the purposes of Proposal 13.1, above.

13.3 The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks. Practice-specific guidance could outline the OAIC's expectations for compliance with the Act when engaging in specific high-risk practices, including compliance with the fair and reasonable personal information handling test.

¹⁰⁹⁴ See relatedly, Submissions to the Discussion Paper: [Salinger Privacy](#); 24; [KPMG](#); 19; [Deloitte Australia](#), 26.

¹⁰⁹⁵ OAIC, [Privacy guidance for businesses collecting COVID-19 vaccination information](#) [Web Page, 12 November 2021].

¹⁰⁹⁶ OAIC, [Guidance for businesses collecting personal information for contact tracing](#) [Web Page, 29 May 2020].

¹⁰⁹⁷ OAIC, [Posting photos and videos](#) [Web Page, 13 June 2019].

¹⁰⁹⁸ UK ICO, [Guidance on AI and data protection](#) [July 2020]; UK ICO and Alan Turing Institute, [Explaining decisions made with AI](#) [May 2020].

¹⁰⁹⁹ UK ICO, [Direct marketing](#) [March 2018].

¹¹⁰⁰ UK ICO, [Guidance for the use of personal data in political campaigning](#) [March 2020].

13.2 Prohibiting high-risk practices

The Discussion Paper sought feedback on whether any particular functions or activities warranted prohibition under the Act. The Discussion Paper noted that any prohibitions would need to be appropriately targeted to avoid proscribing socially beneficial or legitimate practices.¹¹⁰¹ It was also suggested that prohibitions could be implemented through Commissioner-issued guidance, similar to the approach taken by the Office of the Privacy Commissioner of Canada¹¹⁰² in relation to Canada's 'appropriate purpose' test.¹¹⁰³ Submissions to the Discussion Paper proposed that certain personal information handling activities pose unacceptable privacy risks and should be prohibited outright, either in the Act, regulations or in OAIC guidance.¹¹⁰⁴ The practices that were suggested for prohibition included:

- handling children's personal information for the purpose of commercial online tracking, profiling or behavioural advertising¹¹⁰⁵
- handling sensitive information or information about a vulnerability for the purpose of harmful online tracking, profiling or behavioural advertising¹¹⁰⁶
- the use of use of facial recognition and other automated biometric systems in certain circumstances¹¹⁰⁷
- the scraping of personal information from online platforms in certain circumstances,¹¹⁰⁸ and
- the handling of personal information for profiling that that is shown to cause harm or discrimination.¹¹⁰⁹

Professor Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise submitted that legislative prohibitions could target practices that can be expected to have particular effects on individuals, rather than being tied to particular types of technology or data practices, which could include practices that are 'are known or likely to cause significant harm to the individual and that lead to unfair, unethical or discriminatory treatment.'¹¹¹⁰

A high threshold must be met in order to prohibit a particular function or activity, and there are relatively few examples of overseas privacy laws that prohibit personal information handling practices outright. However, there are a number of emerging law reform proposals overseas to prohibit harmful data practices:

1101 [Discussion Paper](#), 97.

1102 Office of the Privacy Commissioner of Canada, [Guidance on inappropriate data practices: Interpretation and application of subsection 5\(3\)](#) (Web Page, May 2018).

1103 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 5(3).

1104 Submissions to the Discussion Paper: [OAIC](#); [UNSW Allens Hub](#), [Deakin CSRI and IEEE SSIT](#); [Salinger Privacy](#); [Deloitte Australia](#); [Consumer Policy Research Centre](#); [Guardian Australia](#); [Australian Privacy Foundation](#); [Centre for AI and Digital Ethics](#); [CHOICE](#); [New South Wales Council for Civil Liberties](#); [Privacy 108](#); [Digital Rights Watch](#); [Obesity Policy Coalition](#); [Foundation for Alcohol Research and Education](#).

1105 Submissions to the Discussion Paper: [OAIC](#), 114; [UNSW Allens Hub](#), [Deakin CSRI and IEEE SSIT](#), 9; [Castan Centre](#), 19; [Obesity Policy Coalition](#), 10; [Foundation for Alcohol Research and Education](#), 14.

1106 See relatedly, Submissions to the Discussion Paper: [UNSW Allens Hub](#), [Deakin CSRI and IEEE SSIT](#), 9; [Castan Centre](#), 19 and [Consumer Policy Research Centre](#), 5, who suggested prohibitions for the handling of personal information in ways that have been shown to cause harm and discrimination to a person's emotional stress or mental health circumstances, physical health, or a person's inexperience in a market and potential financial vulnerability.

1107 Submissions to the Discussion Paper: [OAIC](#), 114; [Salinger Privacy](#), 29; [The Australia Institute – Centre for Responsible Technology](#), 8, 13. See also AHRC, *Human Rights and Technology* (Final Report, March 2021) 116.

1108 Submission to the Discussion Paper: [OAIC](#), 114; [UNSW Allens Hub](#), [Deakin CSRI and IEEE SSIT](#), 9.

1109 Submissions to the Discussion Paper: [UNSW Allens Hub](#), [Deakin CSRI and IEEE SSIT](#), 9; [Castan Centre](#), 19; [Consumer Policy Research Centre](#), 5; [Professor Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 26.

1110 Submission to the Discussion Paper: [Professor Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 26.

Proposed Legislation or Treaty	Proposed Prohibitions
Europe – Proposed Digital Services Act ¹¹¹¹	Prohibition of ‘targeting or amplification techniques that process, reveal or infer’ the personal data of children or special category data for the purpose of displaying advertisements. ¹¹¹²
United Nations – General Comment No. 25 on Children’s Rights in Relation to the Digital Environment ¹¹¹³	Recommended prohibition of the ‘profiling or targeting of children for commercial purposes’ on the basis of their actual or inferred characteristics, including group or collective data. ¹¹¹⁴
Europe – Proposed AI Act ¹¹¹⁵	Prohibition of the following uses of AI: <ul style="list-style-type: none"> a) AI systems that ‘materially distort a person’s behaviour’ in a manner that causes or is likely to cause that person or another person physical or psychological harm b) AI systems that exploit ‘any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person’ in a manner that causes or is likely to cause that person or another person physical or psychological harm c) The use of AI systems by government that evaluates the trustworthiness of individuals based on their social behaviour or predicted personal or personality characteristics, which leads to certain forms of detrimental or unfavourable treatment, and d) The use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless an exception applies.¹¹¹⁶

Table 13.1: International law reform proposals to prohibit harmful data practices.

In light of feedback received, Chapter 20 proposes to prohibit the targeting of children in certain circumstances, as well as targeting on the basis of sensitive information. The requirement to undertake PIAs for high-risk practices (Proposal 13.1 and 13.2) and the interpretation of the fair and reasonable personal information handling test and associated OAIC guidance would also operate to prohibit highly intrusive and harmful practices, or those that have a disproportionate privacy impact.

13.3 Third party collections and information originally sourced by unlawful means

The Discussion Paper proposed that in circumstances where an APP entity does not collect personal information directly from an individual, the APP entity should be required to take reasonable steps to satisfy itself that the information was originally collected in accordance with APP 3.¹¹¹⁷ It was further noted that OAIC guidance could provide examples of reasonable steps that may be taken, which could include contractual warranties or enquiries regarding the personal information handling practices of the entity that originally collected the personal information.¹¹¹⁸

1111 Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services ([Digital Services Act](#)) and amending Directive 2000/31/EC.

1112 Ibid Amendment 500.

1113 United Nations Committee on the Rights of the Child, [General Comment No. 25 \(2021\) on Children’s Rights in Relation to the Digital Environment](#) (2 March 2021).

1114 Ibid 7 [42].

1115 Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence ([Artificial Intelligence Act](#)) COM/2021/20.

1116 Ibid Article 5(1).

1117 [Discussion Paper](#), 92.

1118 Ibid.

This proposal responded to concerns raised in the OAIC's submission about entities collecting personal information from another entity where it was reasonably apparent that the information was originally collected by unlawful means, such as where personal information is sourced from the perpetrator of a data breach.¹¹¹⁹ Several submissions expressed support for the proposal¹¹²⁰ and some were supportive on the basis that it would require APP entities to undertake due diligence to prevent them from assuming the third party from which they collect personal information has complied with the Act.¹¹²¹

A number of submitters expressed concerns about the proposal.¹¹²² It was noted that some entities are required to collect information from a broad range of third parties in order to perform their core functions and activities, particularly in government and insurance contexts,¹¹²³ and that in such cases it may be unrealistically burdensome for an APP entity to undertake due diligence in relation to all personal information collected from each of these third parties.¹¹²⁴ For example, Services Australia collects payroll and employment information from the Australian Tax Office as part of administering payments to individuals, which is collected from Australian employers rather than the individual directly.¹¹²⁵ The Medical Insurance Group Australia considered that practical challenges may arise in the healthcare sector and that it would be unreasonable to expect a specialist doctor to take steps to ensure that a GP's collection of personal information contained in a referral letter had met all the requirements of APP 3.¹¹²⁶

Optus submitted that more practical solutions could be explored, such as requiring contractual warranties (where reasonable), rather than imposing a positive requirement on entities to satisfy themselves of another entity's compliance.¹¹²⁷ Optus further observed that:

An APP entity should not be expected to police the collection handling procedures of its potential service partners... [I]t is not practical, nor reasonable to have peer-regulating legislation given that APP entities often do not have the expertise, nor the resources to make determinations on whether the original collection was fair and lawful, or fair and reasonable, especially if that collection was made in a different sector or industry.¹¹²⁸

A requirement to take reasonable steps would mean the circumstances of the third-party collection, including the relationship between the individual and the original collecting entity and the expense involved in different steps which a third-party collector could take to satisfy the obligation, would be relevant to what steps would be reasonable. In some circumstances, no steps would be reasonable, for example, where a GP has provided a referral to a specialist it would generally not be necessary for the specialist to take steps to satisfy themselves that the information was originally collected from the individual in accordance with APP 3. However, where third party collection of information was an ongoing practice, the steps required would be higher, and could include seeking warranties through contractual arrangements. OAIC guidance could assist with providing examples of reasonable steps that could be taken, depending on the circumstances of the third-party collection. Consideration should also be given to whether there should be any exceptions to this requirement for socially beneficial activities or activities in the public interest.

1119 Submission to the Issues Paper: [OAIC](#), 44.

1120 Submissions to the Discussion Paper: [OAIC](#); [Obesity Policy Coalition](#); [New South Wales Council for Civil Liberties](#); [Privacy 108](#); [Equifax](#); [CPA Australia](#); [Meta](#); [CHOICE](#); [DIGI](#).

1121 Submissions to the Discussion Paper: [New South Wales Council for Civil Liberties](#), 19. See relatedly, [elevenM](#), 32.

1122 Submissions to the Discussion Paper: [Services Australia](#), [Insurance Council of Australia](#), [Optus](#), [CSIRO](#), [Calabash Solutions](#), [Experian](#), [Avant Mutual](#), [Geoscience Australia](#), [MIGA](#), [Australian Medical Association](#), [Nine](#). See relatedly, [National Australia Bank](#) and [Telecommunications Industry Ombudsman](#).

1123 Submissions to the Discussion Paper: [Services Australia](#), 7; [Insurance Council of Australia](#), 11.

1124 Submission to the Discussion Paper: [Insurance Council of Australia](#), 11.

1125 Submission to the Discussion Paper: [Services Australia](#), 7.

1126 Submission to the Discussion Paper: [MIGA](#), 4-5.

1127 Submission to the Discussion Paper: [Optus](#), 19.

1128 Ibid.

13.4 Include an additional requirement in APP 3.6 to the effect 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.

OAIC guidelines could provide examples of reasonable steps that could be taken.

13.4 Defining primary and secondary purposes

The Discussion Paper proposed to define the concept of a primary and secondary purpose in the Act.¹¹²⁹ The proposed changes were designed to:

- make clear that a primary purpose is that which is set out in a collection notice which is given to individuals under APP 5, and
- limit the degree of discretion that entities have to determine that a use or disclosure, with only an indirect connection to the original purpose for collection, is authorized under APP 6.¹¹³⁰

13.4.1 Feedback on Discussion Paper proposal

Submitters expressed a strong level of interest in this proposal. Submitters that did not support the proposal included the OAIC, government agencies, representatives of the healthcare and research sectors, industry representatives and businesses.¹¹³¹ The prevailing concern was that the proposals would expand rather than restrict entities' discretion in determining what a primary and secondary purpose was.

The OAIC and elevenM both considered that the proposal 'would elevate an APP entity's statement of the primary purpose of collection over any analysis of the true or actual purpose based on context or circumstances'.¹¹³² This could encourage entities to broadly define their primary purposes which could in turn undermine the protection against unjustified secondary use or disclosure in APP 6, as entities could avoid the prohibition on subsequent handling by bundling a large number of primary purposes in their collection notices.¹¹³³ Submitters also suggested the proposal would encourage longer and more legalistic collection notices, which was inconsistent with other proposals in the Discussion Paper that sought to reduce notice fatigue and make notice clearer and more understandable.¹¹³⁴ The OAIC and others also noted that it was unclear how the definition of primary purpose would apply in circumstances where notice was not required under APP 5 or where the IC did not consider the purposes included in a collection notice were reasonably necessary for the entities' functions or activities.¹¹³⁵

¹¹²⁹ [Discussion Paper](#), 92-93.

¹¹³⁰ *Ibid* 93.

¹¹³¹ Submissions to the Discussion Paper: [OAIC](#); [Murdoch Children's Research Institute](#); [Population Health Research Network](#); [Australian Medical Association](#); [CSIRO](#); [Geoscience Australia](#); [Avant Mutual](#); [Experian](#); [KPMG](#); [Australian Computer Society](#); [ResMed](#); [Fundraising Institute Australia](#) and [Public Fundraising Regulatory Association](#); [Commonwealth Bank of Australia](#); [Services Australia](#); [ADMA](#); [Optus](#); [DIGI](#); [Australian Federal Police](#); [Google](#); [Equifax](#); [elevenM](#); [Federal Chamber of Automotive Industries](#); [FinTech Australia](#); [MIGA](#); [Australian Genomics](#); [Ramsay Australia](#); [AANA](#).

¹¹³² Submissions to the Discussion Paper: [elevenM](#), 32; [OAIC](#), 92-3.

¹¹³³ Submission to the Discussion Paper: [elevenM](#), 'Consider, for example, a mobile phone service provider wishing to use or sell subscriber location or usage data for advertising purposes. As a secondary purpose, this would require the service provider to obtain consent or establish that such use/disclosure is related to the primary purpose of collection and reasonably expected. Under proposal 10.4, provided this further use was notified as a 'primary purpose', nothing further would be required': 32-3. See also: [Australian Computer Society](#), 'if this opens up potential for use of personal information for secondary purposes such as marketing, then it is unlikely to be a beneficial change for consumers': 3.

¹¹³⁴ Submissions to the Discussion Paper: [OAIC](#), 93; [elevenM](#), 33; [ADMA](#): 24 – 5.

¹¹³⁵ Submissions to the Discussion Paper: [OAIC](#), 93. See also: [MIGA](#), 5.

Submitters were similarly concerned about the proposed narrowing of the concept of secondary purpose.¹¹³⁶ The OAIC cautioned against inadvertently preventing the subsequent use or disclosure of personal information for 'widely accepted secondary purposes...essential to the entity's functioning and reasonably expected by the community'.¹¹³⁷ Some submitters noted that proposed subsequent handling may not always be relevant to the functions or activities of the entity that collected the personal information, particularly where law enforcement activity is concerned.¹¹³⁸ Both Services Australia and the Social Services Portfolio gave further examples of secondary purposes that may no longer be permitted under APP 6 if the proposed definition were implemented, including disclosures necessary to investigate fraudulent activity and where there is concern for an individual's safety or welfare.¹¹³⁹

Submitters raised particular concerns about the proposal's impact on the provision of healthcare and research in response to the Discussion Paper's question about whether the proposed definition of secondary purpose would inadvertently restrict the socially beneficial use of personal information, such as public interest research.¹¹⁴⁰ The Australian Department of Health, AMA, Australian Genomics, Murdoch Children's Research Institute and Ramsay Australia shared this view with regard to secondary sharing of personal information primarily collected for healthcare purposes.¹¹⁴¹

These concerns, however, ran counter to the views of some submitters that supported the proposal. These submitters said the proposal's benefits outweighed the consequential restriction on the operation of APP 6.¹¹⁴² UNSW Allens Hub, Deakin CSRI and IEEE SSIT said the potential impact on research activity, for example, was an acceptable consequence of the proposal because, in any case, 'data collected for research purposes should flag such purposes as a *primary purpose* and disclose that purpose at the time the data is collected'.¹¹⁴³ Its submission further noted that 'surreptitious collection of personal information would be unlikely to pass ethics review in a university context except in narrow circumstances'.¹¹⁴⁴ Electronic Frontiers Australia recommended that consent should be required before using personal information for 'any secondary purpose not directly related to or reasonably necessary to support the primary purpose'.¹¹⁴⁵

In light of the above concerns, Proposal 10.4 of the Discussion Paper is not put forward as a final proposal. While the proposal was intended to provide greater transparency to individuals about how their information is used, the proposal could instead encourage entities to bundle collection notices to avoid the restrictions set out in APP 6. This would fail to remedy the burden on individuals to closely inspect collection notices to protect themselves from privacy harms.¹¹⁴⁶

Other proposals put forward in the Discussion Paper could address the concerns raised about primary and secondary purposes. In particular, the proposal in Chapter 15 to require APP entities to determine and record the primary and secondary purposes for which personal information is handled. The proposed fair and reasonable test for collection, use and disclosure in Chapter 12 would ensure entities considered their specified primary and secondary purposes and the personal information sought to be collected and used for those purpose as against the potential impact on the individual. These obligations would provide protection against collection and use of personal information for harmful primary purposes where notice was not given, and from secondary use and disclosure that might undermine the wellbeing of the individual concerned even where the APP entity had sought consent under APP 6.¹¹⁴⁷ Additionally, the proposed requirements for valid consent in Chapter 11, including that consent must be informed, voluntary and unambiguous, would guard against consent being obtained for vaguely worded secondary purposes which are unrelated to a valid primary purpose.

1136 See for example Submissions to the Discussion Paper: [Optus](#), 19 – 20 regarding secondary uses of technical information; [KPMG](#), 18; [elevenM](#), 33; [ResMed](#), 4; [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 7; [ADMA](#) on the secondary use for internal research to improve a product or service: 25; [Google](#) on the limits on 'what might reasonably be expected from a customer beyond a primary purpose for data collection': 2.

1137 Submission to the Discussion Paper: [OAIC](#), 94.

1138 Submissions to the Discussion Paper: [Australian Federal Police](#), 7; [Social Services Portfolio](#), 22.

1139 Submissions to the Discussion Paper: [Services Australia](#), 8; [Social Services Portfolio](#), 23.

1140 Submissions to the Discussion Paper: [Population Health Research Network](#), 5; [Consumer Policy Research Centre](#), 4; [ResMed](#), 4; [Experian Australia](#), 14; [Murdoch Children's Research Institute](#), 6; [Avant Mutual](#), 9; [CSIRO](#), 8; [Geoscience Australia](#), 7.

1141 Submissions to the Discussion Paper: [Department of Health \(Cth\)](#), 10; [Australian Medical Association](#), 8; [Australian Genomics](#), 4; [Murdoch Children's Research Institute](#), 6; [Ramsay Australia](#): 6 – 7.

1142 Submissions to the Discussion Paper: [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 24; [Privacy 108](#), 21. See also [Salinger Privacy's](#) qualified support for the proposed definition of secondary purpose: 24; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 8. See also proposals to introduce a 'tertiary purpose' for socially beneficial purpose: [Financial Rights Legal Centre and Financial Counselling Australia](#), 10; [Consumer Policy Research Centre](#), 4 (who otherwise felt the proposed definition 'narrows the scope of the data being used for socially beneficial purposes'); [ADMA](#), 25 (who otherwise did not support the proposal as worded).

1143 Submission to the Discussion Paper: [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 8.

1144 Ibid.

1145 Submission to the Discussion Paper: [Electronic Frontiers Australia](#), 14.

1146 Submission to the Discussion Paper: [OAIC](#), 93.

1147 Submission to the Discussion Paper: See [OAIC](#), 93–4; [Australian Genomics](#), 5; [Services Australia](#), 8 in reference to the fair and reasonable test.

14. Research

The Act provides that the collection, use and disclosure of personal information and sensitive information by agencies and organisations to conduct research can occur in certain circumstances without the need to obtain individuals' consent. This recognises the public interest in human-based research. While the Discussion Paper did not specifically address the research exceptions under the Act, submitters raised concerns about the impact of various proposals canvassed in the Discussion Paper on research.¹¹⁴⁸ Some stakeholders also suggested the specific research exceptions should be revisited in light of these proposals.¹¹⁴⁹

14.1 Current framework for collection, use and disclosure for research

An APP entity seeking to collect sensitive information for research, or to use or disclose personal or sensitive information which has already been collected for the secondary purpose of research, must either obtain the consent of the relevant individual or rely on one of the research exceptions in the Act. The Act currently has separate research exceptions for agencies and organisations. Section 95 permits agencies to derogate from the APPs in the course of medical research.¹¹⁵⁰ Private sector organisations can collect, use and disclose health information for research 'relevant to public health or public safety' or for 'the compilation or analysis of statistics relevant to public health or public safety' without consent where it is impracticable to obtain the individual's consent'.¹¹⁵¹

To rely on these exceptions, both agencies and organisations must adhere to guidelines issued by the National Health and Medical Research Council (NHMRC) and approved by the IC under sections 95 and 95A. When approving the guidelines, the IC must be satisfied that the public interest in research substantially outweighs the public interest in maintaining adherence to the APPs.¹¹⁵² These guidelines require a Human Research Ethics Committee (HREC) to similarly weigh the public interest in the proposed research activity to determine if it substantially outweighs the public interest in protecting privacy.¹¹⁵³ In making this assessment, a HREC considers, among other things, the likely outcomes and benefits to particular groups of people or to the wider community.¹¹⁵⁴ HRECs must report decisions to the NHMRC, which provides an annual compliance report to the IC.

This approach aligns with current ethical standards applicable to all human research in Australia. Two of the guiding principles in the National Statement on Ethical Conduct in Human Research, are that:

- (i) the proposed research is justifiable by its potential benefit which may include 'contribution to knowledge and understanding, to improved social welfare and individual wellbeing, and to the skill or expertise of researchers',¹¹⁵⁵ and
- (ii) that the likely benefit of the research must justify any risks of harm or discomfort to participants.¹¹⁵⁶

Stakeholder consultation indicated that notwithstanding the exceptions, research is usually conducted using deidentified information or with participants' express consent as part of the ethics process.¹¹⁵⁷ Some submitters considered HRECs are also not always best placed to engage in the balancing exercise in determining if the public interest in research 'substantially outweighs' the public interest in privacy.¹¹⁵⁸ Therefore, to support public interest research in Australia, there is a need to ensure that the consent proposals in this report are adapted appropriately for research.

1148 Submissions to the Discussion Paper: [CSIRO](#), 1; [Geoscience Australia](#), 1; [Australian Institute of Health and Welfare](#), 1-2; [Department of Health \(Cth\)](#); [Australian Information Industry Association](#), 4; [KPMG](#), 13; [Salinger Privacy](#), 40-41; [UNSW Allens Hub](#), [Deakin CSRI and IEEE SSIT](#), 8-9; [Australian Genomics](#); [Avant Mutual](#), 9; [Australian Medical Association](#), 1; [Department of Health Western Australia](#), 11; [National Health and Medical Research Council](#); [Murdoch Children's Research Institute](#), 2; [OAIC](#); [Australian Digital Health Agency](#), 1; [Society of Australian Genealogists](#), 2-3; [Research Australia](#); [Population Health Research Network](#), 2; [Association of Australian Medical Research Institutes](#), 1; [Attorney-General's Department research consultation roundtable](#) [1 April 2022].

1149 Submissions to the Discussion Paper: [Australian Institute of Health and Welfare](#), 1; [National Health and Medical Research Council](#), 3; [Attorney-General's Department medical and research consultation roundtable](#) [16 December 2021]; [Attorney-General's Department research consultation roundtable](#) [1 April 2022].

1150 Privacy Act s 95.

1151 Exceptions for organisations operate via the permitted health situations under s 16B(2) and (3); APPs 3.4 and 6.2 and s 95AA.

1152 Privacy Act ss 95(2), 95A(2) and (3).

1153 National Health and Medical Research Council, [Guidelines approved under Section 95A of the Privacy Act 1988](#) [2015] 10; National Health and Medical Research Council, [Guidelines approved under Section 95 of the Privacy Act 1988](#) [2015] 5.

1154 National Health and Medical Research Council, [Guidelines approved under Section 95A of the Privacy Act 1988](#) [2015] 23-24; National Health and Medical Research Council, [Guidelines approved under Section 95 of the Privacy Act 1988](#) [2015] 5.

1155 National Health and Medical Research Council, [National Statement on Ethical Conduct in Human Research](#) Principle 1.1(a), 10.

1156 Ibid Principle 1.6, 10.

1157 [Attorney-General's Department research consultation roundtable](#) [1 April 2022], Submission to the Discussion Paper: [CSIRO](#), 6.

1158 Submission to the Discussion Paper: [Eckstein et al](#), 3-4.

14.2 Impacts of consent proposals on research

Several research stakeholders had concerns about the proposal in Chapter 11, that valid consent must be voluntary, informed, current, specific, and unambiguous. The concerns were specifically around the elements of ‘current’ and ‘specific’.

14.2.1 ‘Broad’ consent for research

Stakeholders expressed concern that requiring specific consent could limit health researchers’ ability to use personal information for future public interest research that may not be anticipated at the point of collection. The Population Health Research Network thought the definition could ‘preclude extended or unspecified consent for the future use of data in research’ and that the definition is not as nuanced as the approach in the National Statement on Ethical Conduct in Human Research.¹¹⁵⁹

Dr Lisa Eckstein et al noted that genomic research in particular has moved towards models that include broad consent and that ‘[w]hile it should remain an individual choice whether to agree to future data sharing, this option should be structured so as to facilitate various forms of consent.’¹¹⁶⁰

Other research stakeholders expressed concern about whether ‘current’ and ‘specific’ consent would require researchers to recontact patients to seek their consent throughout research projects.¹¹⁶¹ CSIRO noted the ‘administrative burden would be overwhelming if those consents had to be continuously assessed, refreshed and renewed and [that] participants are already often intimidated by the initial consent process’.¹¹⁶² It suggested the effect of these proposals would be a reduced willingness to participate in research.¹¹⁶³

This challenge has been recognised in Europe’s GDPR, which also maintains an element that requires consent to be ‘specific’.¹¹⁶⁴ Recital 33 of GDPR provides the following clarification on how that definition should be applied in relation to public interest research:

It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.¹¹⁶⁵

In the UK, the consultation on the UK Government’s recent review of UK GDPR, *Data: A New Direction*, observed that Recital 33 permits data subjects to give ‘broad consent’ for areas of scientific research and that ‘by providing broad consent, a person consents to their data being used not only for a narrow, specified research purpose, but for broader areas of scientific research.’¹¹⁶⁶ It was noted that in a research context, ‘the nature of processing activities may not be fully determined at the outset, limiting the extent or specificity of information available to the data subject.’¹¹⁶⁷ However, the consultation recognised that the status of Recital 33 is uncertain as it is not reflected in the operative provisions of GDPR,¹¹⁶⁸ and on this basis, the UK has proposed to incorporate ‘broad consent’ for public interest research into legislation.¹¹⁶⁹

Broad consent for research should also be permitted in the Australian context to facilitate important human-based research. This would ensure that research recognised by the Act is not hampered by the requirements that consent must be current and specific where the research purposes are not able to be specified with precision at the point of collection. To ensure that the exception is only available in appropriate circumstances, its scope should be limited to research to which the research exceptions in the Act apply.

1159 Submission to the Discussion Paper: [Population Health Research Network](#), 5.

1160 Submission to the Discussion Paper: [Eckstein et al](#), 3.

1161 Submissions to the Discussion Paper: [CSIRO](#), 6; [Geoscience Australia](#), 7; [Australian Digital Health Agency](#), 2-3; [Australian Institute of Health and Welfare](#)

1162 Submission to the Discussion Paper: [CSIRO](#), 6.

1163 *Ibid* 6.

1164 GDPR art 4(11) provides that consent must 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’.

1165 GDPR recital 33.

1166 Department for Digital, Culture, Media and Sport (UK), [Data: A New Direction](#) (Consultation Document, September 2021) 16.

1167 *Ibid*.

1168 *Ibid*.

1169 Department for Digital, Culture, Media and Sport (UK), [Data: A New Direction](#) (Government Response, June 2022).

Broad consent in Australia should be modelled on the approach in the GDPR. Individuals could give broad consent for 'certain areas' instead of limiting the project. Guidelines on recital 33 by the European Commission Data Protection Working Party explain that 'broad consent' does not disapply specific consent, but rather where projects cannot be specified at the outset, it allows specifying future uses at a more general level.¹¹⁷⁰ For example, in the EU, broad consent could be given to take a bio-sample for the purposes of a study which seeks to identify a particular health risk. That consent could then extend to further studies to identify treatment options for that risk. The UK ICO guidance advises that even where general areas of research are described for broad consent, where possible individuals should be provided granular options to consent only to certain areas of research or parts of research projects.¹¹⁷¹

14.1 Introduce a legislative provision that permits broad consent for the purposes of research:

- **Broad consent should be available for all types of research to which the research exceptions in the Act (and proposed by this chapter) would also apply.**
- **Broad consent would be given for 'research areas' where it is not practicable to fully identify the purposes of collection, use or disclosure of personal or sensitive information at the point when consent is being obtained.**

14.3 The rationale for exceptions to consent for research

The exceptions to consent for research accommodate the potential societal benefits of research that might otherwise be prohibited by the APPs. Obtaining consent for research is not always practicable, particularly for further uses of legitimately collected personal information. While consent to use of personal or sensitive information for research may have been part of an original consent, it may not capture unexpected situations, such as research conducted in response to the COVID-19 pandemic. Dove and Chen have noted that 'by treating data processing for scientific research (e.g. biobanking, genomic research, epidemiological research) as equivalent to data processing for banking or digital marketing, citizens would suffer from slower research breakthroughs and translational research discoveries that bring new diagnostics, drugs, and devices to market'.¹¹⁷² Researchers might not have access to the names and contact details of the individuals connected to an original consent in order to contact them to seek consent to use their personal information for secondary research purposes. Even where contact details are available, they might be outdated, individuals may have changed addresses or phone numbers or died in the intervening years. The latter could be a barrier to research that relies on information collected in a clinical context, where patients were in treatment for a life-limiting medical condition.

The exceptions recognise that being unable to obtain consent should not prevent research with potentially significant public benefit from proceeding. This is particularly the case for research that aims to contribute to the provision of public goods, such as food safety standards, air and water quality levels, pandemic preparedness and other public health measures – matters that the public do not typically expect to be left to individual choice.¹¹⁷³ This is also the case for research involving secondary data analysis more broadly. Where technology and methodological approaches are constantly evolving, sensitive information which may be valuably utilised in research may have been collected significantly before such use was recognised.¹¹⁷⁴

¹¹⁷⁰ European Commission, *Guidelines on Consent under Regulation 2016/679* 28.

¹¹⁷¹ UK ICO, 'What are the rules on consent for scientific research?' (Web Page, October 2022).

¹¹⁷² Edward S Dove and Jiahong Chen, 'Should consent for data processing be privileged in health research? A comparative legal analysis' (2020) 10(2) *International Data Privacy Law* 118.

¹¹⁷³ *ALRC Report 108*, citing the Australian Bureau of Statistics [65.35].

¹¹⁷⁴ Submissions to the Discussion Paper: *CSIRO*, 8; *Australian Genomics*, 4.

14.4 Scope of research permissible under current research exceptions

The Australian Institute of Health and Welfare submitted that the Review should revisit particular recommendations from the ALRC Report 108, on the basis that their implementation would ‘significantly enhance’ the conduct of research in Australia.¹¹⁷⁵ It highlighted recommendation 65-2 to amend the Privacy Act to ‘extend the arrangements relating to the collection, use or disclosure of personal information without consent in the area of health and medical research to cover the collection, use or disclosure of personal information without consent in human research more generally’.¹¹⁷⁶ The term ‘health and medical research’ was a reference to the ‘public health or public safety’ exception for organisations and ‘medical research’ exception for agencies. These exceptions have not materially changed in scope since the ALRC’s review.

The guidelines under section 95A of the Act (which apply to organisations) take an expansive view of ‘public health or public safety’. The guidelines define ‘public health’ to include ‘activities such as education, economics, technology, legislation and management, which protect and enhance the health of all people and to prevent illness, injury and disability’ and ‘public safety’ to include ‘the condition for all people of being safe and free from danger or risks’.¹¹⁷⁷ The OAIC takes a narrower approach in its Guide to Health Privacy, which states that ‘public health or public safety’ research and statistical analysis include activities that ‘impact on, or provide information about’ public health or public safety. It cites examples of ‘communicable diseases, cancer, heart disease, mental health, injury control, diabetes and the prevention of childhood diseases’.¹¹⁷⁸ ‘Public health or public safety’ is not defined further in the Act itself, but ‘medical research’ is defined to include epidemiological research.¹¹⁷⁹

The guidelines under section 95 of the Act (which apply to agencies) do not further define ‘medical research’, but require HRECs to consider whether the proposed activity is ‘likely to contribute to:

- the identification, prevention or treatment of illness or disease
- scientific understanding relating to health
- the protection of the health of individuals and/or communities
- the improved delivery of health services, or
- scientific understanding or knowledge’.¹¹⁸⁰

The section 95A guidelines similarly require HRECs to consider the potential contribution to:

- the identification, prevention or treatment of illness, injury or disease
- scientific understanding relating to public health or safety
- the protection of the health of individuals and/or communities
- the improved delivery of health services
- enhanced scientific understanding or knowledge, or
- enhanced knowledge of issues within the fields of social science and the humanities relating to public health or public safety’.¹¹⁸¹

The breadth of the above factors and definitions suggest the Act accommodates a significant portion of valuable research activity. They also reflect the view that research can be valuable for its contribution to scientific knowledge, in addition to its usefulness for informing population-based policies and interventions. Despite this, there is evidence to suggest the exceptions are underutilised. Consultations conducted with government stakeholders following the release of the Discussion Paper indicated that key agencies with statutory functions to conduct research are not relying on the section 95 medical research exception, in part due to its perceived narrowness.¹¹⁸²

¹¹⁷⁵ Submission to the Discussion Paper: [Australian Institute of Health and Welfare](#), 2. See also [National Health and Medical Research Council](#), 3.

¹¹⁷⁶ [ALRC Report 108](#), rec 65-2.

¹¹⁷⁷ National Health and Medical Research Council, [Guidelines approved under Section 95A of the Privacy Act 1988](#) (2015) 9.

¹¹⁷⁸ OAIC, [Guide to Health Privacy](#) (2019) 2.

¹¹⁷⁹ Privacy Act s 6(1)(a).

¹¹⁸⁰ National Health and Medical Research Council, [Guidelines approved under Section 95 of the Privacy Act 1988](#) (2015) 5.

¹¹⁸¹ National Health and Medical Research Council, [Guidelines approved under Section 95A of the Privacy Act 1988](#) (2015) 23.

¹¹⁸² [Attorney-General’s Department research consultation roundtable](#) (1 April 2022).

In recommending that the exceptions should be expanded for both agencies and organisations to ‘human research’ more generally, the ALRC concluded there was ‘no in-principle reason’ to limit the scope to health and medical research.¹¹⁸³ The ALRC noted the strong public interest in other types of research, including in the fields of criminology and social sciences and that the barriers to consent were not unique to health and medical research.¹¹⁸⁴

Submissions to the ALRC suggested criminological research typically includes information collected through a variety of processes that do not involve obtaining consent for secondary research as part of the initial collection, such as police and court reports.¹¹⁸⁵ Others noted that social science research can involve the investigation of topics associated with a reduced willingness to engage or an inability to contact individuals, such as family violence, homelessness or the experiences of children at school and at home.¹¹⁸⁶ The ALRC also noted the comparative broadness of the research exceptions in other jurisdictions, such as the UK, Canada and New Zealand.¹¹⁸⁷

14.4.1 Proposal – Broaden the scope of research covered by the exceptions

There is merit to expanding the scope of the current research exceptions. It would recognise the public interest in the controlled further use of personal and sensitive information for other types of research that seek to contribute to society, as well as clarifying the application of the exceptions to basic and applied research. If the scope of the exceptions is expanded, the existing safeguards would continue to apply. Agencies and organisations would need to obtain HREC approval for the proposed handling of personal and sensitive information without consent, for which they would need to demonstrate the impracticability of obtaining consent and that the activity cannot proceed on the basis of de-identified information.

An expansion or clarification of the scope of research permitted under the research exceptions could also enhance the use of the DAT Act. The DAT Act scheme permits the sharing of public sector data containing personal information among government agencies (including states and territories) and with universities for research without consent where section 95 of the Privacy Act applies and other requirements are met.¹¹⁸⁸ The purpose of the DAT Act is to serve the public interest by promoting better availability of public sector data with appropriate safeguards. This could be particularly useful for research undertaken by researchers in partnership with public sector agencies.

While the ALRC’s justifications for broader research exceptions remain relevant, the proposed scope of ‘human research’ suggested by the ALRC may cause confusion about the extent to which the proposed activity must seek to ensure direct outcomes for humans. It may inadvertently preclude certain fields, such as environmental and climate change research. Recital 159 of the GDPR states that the processing of personal data for scientific research purposes should be interpreted in a broad manner including, for example, technological development and demonstration, fundamental research, applied research and privately funded research.¹¹⁸⁹ The UK Government recently committed to creating statutory definitions of ‘scientific research’, ‘historical research’ and ‘statistical purposes’ as part of its consultation on proposals to reform the UK’s data protection laws.¹¹⁹⁰ These reforms are intended to improve clarity for researchers and provide more certainty. Respondents to the UK Government’s consultation argued adopting the text of the relevant GDPR recitals into the operative text of the UK GDPR would improve clarity for researchers and provide more certainty.¹¹⁹¹

1183 [ALRC Report 108](#), [65.40].

1184 *Ibid.*, [65.40].

1185 *Ibid.*, [65.33].

1186 *Ibid.*, [65.33].

1187 *Ibid.*, 2160.

1188 However, express consent would still be required under the DAT Act to share biometric data even where the section 95(1) exception applied.

1189 GDPR recital 159.

1190 Department for Digital, Culture, Media and Sport (UK), [Data: A New Direction](#) (Government Response, June 2022).

1191 *Ibid.*

Research exceptions are also contained in the privacy laws of some states and territories. For example, Queensland allows health agencies to use and disclose personal information if it is impracticable to seek the individual's consent and is necessary for research, or the compilation of statistics, relevant to public health or public safety, if the use or disclosure is conducted in accordance with guidelines approved by the chief executive of the health department.¹¹⁹² Similar provisions are included in the privacy laws of NSW,¹¹⁹³ Victoria,¹¹⁹⁴ Tasmania¹¹⁹⁵ and the Northern Territory.¹¹⁹⁶ The scope and harmonisation of research exceptions could be a matter for further consideration by the state and territory working group, discussed further in Chapter 29.

14.2 Consult further on broadening the scope of research permitted without consent under the Act for both agencies and organisations.

14.5 A single, combined exception and guidelines for research

The ALRC also made the broader recommendation to combine the research exceptions and guidelines under sections 95 and 95A to create a single set of legally binding rules for research applicable to both organisations and agencies.¹¹⁹⁷ The NHMRC submitted to the Review that consideration should be given to developing one set of research guidelines regulating the collection, use and disclosure of health information in the conduct of research, as proposed by the ALRC.¹¹⁹⁸

The ALRC noted stakeholder concerns that differences between the two guidelines had created confusion among researchers and potentially 'conservative and incorrect decision making' which was 'hindering the conduct of effective health and medical research'.¹¹⁹⁹ In addition to the inconsistencies between the two sets of guidelines, the mechanism by which they work also differs. The section 95A guidelines and their enabling exceptions (sections 16B(2) and (3)) apply to organisations' collection, use or disclosure of health information only.¹²⁰⁰ In comparison, section 95 applies to personal information more broadly and offers agencies derogation from any of the APPs. However, agencies are limited to medical research. Organisations are permitted to conduct research as well as the compilation or analysis of statistics relevant to public health or public safety.¹²⁰¹ Further, despite the breadth of section 95, the section 95 guidelines primarily address use and disclosure under APP 6. This leaves it unclear whether derogation is in fact permissible for other APPs. Combining the exceptions would enable the development of a consistent set of research exceptions for all APP entities under APPs 3 and 6.¹²⁰²

The ALRC further recommended the single set of research rules should be developed and issued by the Privacy Commissioner rather than the NHMRC.¹²⁰³ This recommendation followed the ALRC's consideration that, if the scope of the exceptions were broadened to human research more generally, the NHMRC would no longer be the most appropriate body to develop the guidelines, given its focus on health and medical research.¹²⁰⁴ The ALRC noted that the Privacy Commissioner was well-placed to play a coordinating role in the development of new guidelines, which would require consultation with a variety of stakeholders, including those outside the health and medical research field.¹²⁰⁵ It also said that generally the IC should 'retain primary responsibility' for any derogation from the Act's protections, as

1192 *Information Privacy Act 2009* (Qld) NNP 2.

1193 *Privacy and Personal Information Protection Act 1998* (NSW) s 27B.

1194 *Privacy and Data Protection Act 2014* (VIC) IPP 2.

1195 *Personal Information Protection Act 2004* (Tas) PIPP 2.

1196 *Information Act 2002* (NT) IPP 2.

1197 [ALRC Report 108](#), Recommendations 65-1(a), 65-8 and 65-9.

1198 Submission to the Discussion Paper: [National Health and Medical Research Council](#), 3.

1199 [ALRC Report 108](#), [65.3] and citing NHMRC, CSIRO and the then Department of Health and Ageing, 2155-6.

1200 These exceptions apply via APPs 3.4(c) and 6.2(d).

1201 And, in the case of collection, 'the management, funding or monitoring of a health service': s 16B(2)(a)(iii).

1202 [ALRC Report 108](#), [65.16] and Recommendations 65-8 and 65-9.

1203 *Ibid*, Recommendation 65-1(b).

1204 *Ibid*, [65.8]; [65.19].

1205 *Ibid*, [65.19].

in the case of public interest determinations under the Act.¹²⁰⁶ The NHMRC's submission to the ALRC and the Review's Discussion Paper indicated its support for this recommendation.¹²⁰⁷ The ALRC noted that the then Office of the Privacy Commissioner expressed support for a single set of rules to regulate research but did not agree that they should be developed by the Privacy Commissioner.¹²⁰⁸

14.5.1 Proposal – develop a single research exception with one set of research guidelines

Combining the research exceptions and developing one set of research guidelines should be progressed subject to further consultation. Consideration should also be given to the appropriate body to develop the guidelines in light of the expanded scope of the research exceptions.

Streamlining the research exceptions and guidelines would reduce complexity for researchers and reduce administrative burden for the NHMRC and HRECs in maintaining and applying two sets of guidelines when approving research without consent under the Act. It would also simplify regulation of research projects involving public-private partnerships.

Important safeguards should remain, including the requirement to demonstrate the impracticability of obtaining consent or de-identifying the information. In addition, these safeguards could be specified in the Act for all APP entities (section 95 currently does not include these provisions) and the scope of permissible action for agencies could be narrowed from all of the APPs to collection, use or disclosure under APPs 3 and 6 (as in the case for organisations). This process could assist in determining relevant safeguards, including with respect to security requirements, which are currently not included in the section 95 guidelines.

14.3 Consult further on developing a single exception for research without consent and a single set of guidelines, including considering the most appropriate body to develop the guidelines.

¹²⁰⁶ Ibid, [65.17].

¹²⁰⁷ Ibid, [65.14] Submission to the Discussion Paper: [National Health and Medical Research Council](#), 3.

¹²⁰⁸ Ibid, [65.13].

15. Organisational accountability

Organisational accountability requires that entities implement privacy management processes which internally reflect their responsibility for compliance with applicable privacy laws and for managing privacy risks on an ongoing basis.¹²⁰⁹ Organisational accountability measures can encourage the proactive mitigation of privacy-related risks, result in better legal compliance and build community trust in the entity as a responsible steward of personal information.¹²¹⁰ The implementation of these measures also ensures that the burden of privacy management does not unduly rest with individual data subjects.¹²¹¹

15.1 The current law

APP 1.2 requires APP entities to implement practices, procedures and systems to ensure compliance with the APPs.¹²¹² APP entities must also implement practices, procedures and systems to enable them to deal with inquiries or complaints from individuals.¹²¹³

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'.¹²¹⁴ The APP Guidelines note that APP 1.2 imposes a distinct and separate obligation upon entities, which requires them to take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance.¹²¹⁵

Unlike some comparable overseas data protection regimes,¹²¹⁶ APP 1.2 does not prescribe specific measures that APP entities must implement.¹²¹⁷ However, the APP Guidelines provide examples of measures that an APP entity 'should consider implementing',¹²¹⁸ which could include:

- procedures for identifying and managing privacy risks at each stage of the information lifecycle
- security systems for protecting personal information
- privacy impact assessments for new projects in which personal information will be handled, or when a change is proposed to existing personal information handling practices
- procedures for identifying and responding to privacy breaches
- procedures for handling access and correction requests, as well as complaints and inquiries
- procedures that give individuals the options of not identifying themselves, or using a pseudonym in certain circumstances
- governance mechanisms to ensure compliance with the APPs (such as designated privacy officers and regular reporting to the entity's governance body)
- regular staff training on how the APPs apply and the entity's privacy practices, procedures and systems, as well as appropriate supervision of staff regularly handling personal information
- mechanisms to ensure that agents and contractors of the entity comply with the APPs, and
- proactive review and audit of the entity's privacy policy and privacy practices, procedures and systems.

¹²⁰⁹ UK ICO, [Accountability and Governance](#) (Web Page, January 2021); Article 29 Data Protection Working Party, [Opinion 3/2010 on the principle of accountability](#) (13 July 2010) 2-4; Office of the Privacy Commissioner of Canada (OPC) and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia, [Getting Accountability Right with a Privacy Management Program](#) (Report, April 2012) 1; OAIC, [APP Guidelines](#) (July 2019) [1.1]. See also, Submission to the Discussion Paper: [OAIC](#), 167-9; [The Australia Institute – Centre for Responsible Technology](#); 10-11; [Digital Law Association](#), 9.

¹²¹⁰ Ibid. See also, Submission to the Discussion Paper: [Data Synergies](#), 34-5, Centre for Information Policy Leadership, [What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework](#) (Report, May 2020) 4-6.

¹²¹¹ Submissions to the Discussion Paper: [OAIC](#), 168, [Data Synergies](#), 34-5, [Deloitte Australia](#), 44, [elevenM](#), 55.

¹²¹² Privacy Act sch 1, APP 1.2(a).

¹²¹³ Ibid APP 1.2(b).

¹²¹⁴ Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 73.

¹²¹⁵ OAIC, [APP Guidelines](#) (July 2019) [1.4]–[1.7].

¹²¹⁶ See for example GDPR arts 24-25, 30, 35-39; *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (PIPEDA), sch 1, cl 4.1-4.2.

¹²¹⁷ Submission to the Discussion Paper: [OAIC](#), 167.

¹²¹⁸ OAIC, [APP Guidelines](#) (July 2019) [1.7].

Australian government agencies must also comply with more prescriptive organisational accountability requirements as set out in the Privacy (Australian Government Agencies – Governance) APP Code 2017. The Code prescribes how APP 1.2 is to be complied with by agencies¹²¹⁹ and includes express requirements to:

- have a privacy management plan that documents specific, measurable privacy goals and targets as well as how the agency will comply with the Act,
- designate a privacy officer, whose functions include handling privacy enquiries and complaints, maintaining a record of personal information holdings, preparing privacy impact assessments and conducting an annual review of the entity's privacy management plan,
- designate a privacy champion, whose functions include providing leadership within the agency on privacy issues,
- conduct PIAs for all high privacy risk projects as well as maintain a published register of PIAs,
- provide appropriate privacy training in staff inductions and annual training for staff who have access to personal information in the course of performing their duties, and
- regularly review and update privacy practices, procedures and systems, to ensure their currency and adequacy for the purposes of compliance with the APPs.

15.2 Need for additional accountability requirements

While APP 1.2 has been interpreted so that entities must implement certain organisational accountability measures in particular circumstances,¹²²⁰ recent determinations by the IC have found that some entities are failing to implement important accountability measures such as privacy impact assessments in certain circumstances.¹²²¹

In addition to commenting on Proposal 20.1 in the Discussion Paper to introduce a specific record-keeping requirement, a number of submitters advocated for further organisational accountability requirements. These were considered necessary to shift the emphasis from individuals being primarily responsible for self-managing their privacy to organisations taking appropriate responsibility for effective privacy management. The measures included requiring risk-based 'privacy by design' to encourage proactive privacy preserving approaches to information management, appointing internal privacy officers and requiring that further specific records be kept and privacy impact assessments be undertaken.¹²²²

The reforms proposed in this Report will require careful consideration of the nature of information collected, held and disclosed by entities and whether personal information handling is fair and reasonable in the circumstances, along with enhanced individual rights that entities will need to manage. Accordingly, supplementing APP 1 with a limited number of additional requirements is warranted. The proposed additional requirements are likely to drive behavioural change in how entities approach privacy, ensuring that privacy considerations are built into internal governance systems and processes, more effectively than current non-binding OAIC guidance.

15.2.1 Recording the purposes for personal information handling

Proposal 20.1 of the Discussion Paper provided that APP entities should be required 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.

A range of stakeholders were supportive of this proposal, including submitters from government, industry and civil society groups.¹²²³ It was considered that this proposal would enhance accountability over high-risk secondary uses and would encourage entities to ensure that a proposed secondary use or disclosure would qualify for a secondary purpose exception in APP 6.¹²²⁴ Submitters that did not support the proposal were concerned about the administrative burden that such a requirement would impose,¹²²⁵ particularly in the context of healthcare¹²²⁶ or research.¹²²⁷

¹²¹⁹ Privacy (Australian Government Agencies – Governance) APP Code 2017 [Cth] cl 8.

¹²²⁰ See for example, Flight Centre Travel Group (Privacy) [2020] AICmr 57 (25 November 2020) [101]–[116]; Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. (Privacy) [2021] AICmr 34 (30 June 2021) [125]–[131].

¹²²¹ Flight Centre Travel Group (Privacy) [2020] AICmr 57 (25 November 2020) [114]; Clearview [Determination](#), [229]–[234]; see also, 7-Eleven [Determination](#), [103]; see relatedly, Submissions to the Discussion Paper: [Data Synergies](#), 26.

¹²²² Submissions to the Discussion Paper: [OAIC](#), [Law Council of Australia](#), [Deloitte Australia](#), [elevenM](#), [Privacy 108](#), [Australian Privacy Foundation](#), [The Australia Institute – Centre for Responsible Technology](#). See relatedly, [Western Union](#).

¹²²³ Submissions to the Discussion Paper: [Department of Health \(Cth\)](#), [KPMG](#), [Privacy 108](#), [Google](#), [Australian Privacy Foundation](#), [Digital Law Association](#), [OAIC](#), [Australian Institute of Health and Welfare](#), [Australian Council on Children and the Media](#), [Australian Communications Consumer Action Network](#).

¹²²⁴ Submissions to the Discussion Paper: [KPMG](#), 27; [Department of Health \(Cth\)](#) 16.

¹²²⁵ Submissions to the Discussion Paper: [Optus](#), [Australian Financial Markets Association](#), [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), [Insurance Council of Australia](#), [Australian Digital Health Agency](#).

¹²²⁶ Submissions to the Discussion Paper: [Ramsay Healthcare](#), 9; [Australian Medical Association](#), 15–16.

¹²²⁷ Submission to the Discussion Paper: [CSIRO](#), 12.

The Discussion Paper suggested there was no clear need for extending this proposed requirement so that entities record *all* the purposes for which they collect, use or disclose personal information, as this information should be recorded through the process of issuing a collection notice.¹²²⁸ However, several submitters, including the OAIC, suggested that Proposal 20.1 should not be limited to secondary purposes.¹²²⁹ It was considered that requiring APP entities to record all purposes for which they collect, use and disclose personal information could function as an internal governance measure that would facilitate and improve compliance with other substantive provisions of the APPs.¹²³⁰ For example, maintaining records about the purposes for which an entity collects, uses and discloses personal information may place entities in a better position to develop accurate collection notices and privacy policies, as well as to determine whether personal information must be destroyed or de-identified under APP 11.2.

Importantly, it was thought that it would also ensure that APP entities have a specific and *limited* purpose in mind before embarking on a collection of personal information under APP 3, or a use or disclosure under APP 6, which would support the principles of data minimisation and purpose limitation that are expressed in these principles.¹²³¹ Furthermore, as there may be circumstances in which it would not be reasonable to issue a collection notice,¹²³² the recording of purposes may not always take place through that process.

Comparable overseas data protection laws require regulated entities to record all purposes for which they handle personal information. Canada's existing private sector privacy law, PIPEDA, requires entities to:

- document the purposes for which personal information is collected, which should be specified at or before the time of collection,¹²³³ and
- when personal information is to be used for a purpose not previously identified, the new purpose shall be identified prior to use.¹²³⁴

Canada's proposed data protection reforms (Bill C-27) will require entities to record the purposes for which personal information will be collected, used or disclosed at the point of collection¹²³⁵ and to record new purposes as they arise.¹²³⁶

Europe's GDPR contains comparatively more prescriptive record keeping obligations, including requiring regulated entities to record the purposes for which they process personal data, the categories of personal data they process, the data subjects to which that personal data relates and recipients of personal data, among other matters.¹²³⁷

Under the Act, records about how an entity manages personal information should be maintained as part of compliance with APP 1.3 which requires entities to have a privacy policy. Records should also be maintained as part of an entity's compliance with APP 1.2 which requires entities to implement practices, procedures and systems to ensure an entity complies with the APPs. An entity must include information about the purposes for which it collects, holds, uses and discloses personal information in its privacy policy¹²³⁸ and collection notices must provide information about the purposes for which personal information is being collected.¹²³⁹ What is required to demonstrate compliance with APPs 1.2 and 1.3 will be proportionate to the complexity and risks of an entity's information handling. However, these APPs do not specifically oblige entities to determine and record the purposes for which personal information is collected, used and disclosed before collecting for a primary purpose or using or disclosing for a secondary purpose.

15.2.2 Proposal

In addition to the obligations in APP 1, there is merit in including an express requirement that entities determine and record the primary and secondary purposes for which personal information is handled. While the existing requirements are important for transparency, determining and recording the primary and secondary purposes for which personal information is collected, used and disclosed would assist entities with internal measures to assess the adequacy of current practices and comply with new obligations.

¹²²⁸ [Discussion Paper](#), 154.

¹²²⁹ Submissions to the Discussion Paper: [KPMG](#), 27; [Digital Law Association](#), 18; [OAIC](#), 174-5, [elevenM](#), 54-55.

¹²³⁰ Submission to the Discussion Paper: [OAIC](#), 175; [elevenM](#), 55.

¹²³¹ *Ibid.*

¹²³² See Chapter 10.

¹²³³ PIPEDA, sch 1, cl 4.2.1-4.2.3.

¹²³⁴ *Ibid* sch 1, cl 4.2.4.

¹²³⁵ [Bill C-27](#) s 12(3). See relatedly, s 13.

¹²³⁶ *Ibid* s 12(4).

¹²³⁷ GDPR art 30.

¹²³⁸ Privacy Act sch 1, APP 1.4(c).

¹²³⁹ *Ibid* APP 5.2(d).

Determining and recording purposes would assist entities to comply with the data minimisation principle of only collecting the personal information that is reasonably necessary for an identified purpose which underlie APPs 3 and 6. It would also assist entities in their processes for determining whether consent would need to be obtained from individuals before using the information for a secondary process, and for determining when personal information is no longer required for any identified purpose and should be destroyed or deidentified under APP 11.

The proposed requirement would support entities' assessment of whether their collection, use and disclosure of personal information is fair and reasonable as per proposal 12.1. An entity would be able to consider whether an individual would reasonably expect the personal information to be collected, used or disclosed for the identified purpose. The identified purposes for collection, use and disclosure of personal information could also be scrutinised for whether they are reasonably necessary for the entity's activities or functions. Where an entity proposes to handle the personal information of a child, identifying and recording relevant purposes would enable scrutiny of whether the purpose is in the child's best interests.

Determining and recording the purposes for collection, use and disclosure of personal information as part of an entity's information-management governance processes and systems would also support the entity's ability to adequately respond to individual rights requests and complaints. It would also support an entity's ability to demonstrate compliance with the Act where required.

15.1 An APP entity must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. If an APP entity wishes to use or disclose personal information for a secondary purpose, it must record that secondary purpose at or before the time of undertaking the secondary use or disclosure.

As for compliance with APP 1, the steps needed to comply with such a requirement should be reasonable and proportionate to privacy risks. In most cases, an APP entity would only need to record the *types* of purposes for which the entity generally handles types of personal information, rather than keep individual records for each piece of information. In cases where collection and use are self-evident from how the information is held (e.g. a customer contact list) no further record would be required unless the information were to be used for a secondary purpose. The requirement to record secondary purposes would apply at or before the point of *use or disclosure*, rather than at the point of collection when possible future secondary purposes may be unknown.

15.3 Privacy Officers

The Discussion Paper noted that some overseas jurisdictions require regulated entities to appoint a privacy officer as a privacy governance measure. Several submitters considered that APP 1.2 should require entities to appoint or designate a privacy officer within the APP entity.¹²⁴⁰

These submitters highlighted that privacy officers can be an important governance measure to ensure that day-to-day operational privacy compliance activities are undertaken and to foster a culture of respect for privacy within an APP entity.¹²⁴¹ Privacy officers may also act as a dedicated contact point for privacy matters within the entity, as well as a contact point for external privacy-related complaints and enquiries.¹²⁴² Public sector agencies are already required to designate a privacy officer under the Privacy (Australian Government Agencies – Governance) APP Code 2017.

¹²⁴⁰ Submissions to the Discussion Paper: [OAIC](#), [Deloitte Australia](#), [Privacy 108](#), [Western Union](#), [elevenM](#).

¹²⁴¹ Submission to the Discussion Paper: [OAIC](#), 172.

¹²⁴² Ibid.

This requirement is an important feature in overseas privacy frameworks. Europe's GDPR requires certain regulated entities to appoint a Data Protection Officer (DPO).¹²⁴³ The GDPR contains several prescriptive requirements that govern the nature of this appointment, including that the DPO have 'expert knowledge of data protection law'.¹²⁴⁴ A DPO must also have a degree of independence, be adequately resourced, report to the highest management level, and not 'receive any instructions regarding the exercise of their duties' or be dismissed for performing their duties.¹²⁴⁵

The UK Government's recent review of UK GDPR, *Data: A New Direction*, recommended replacing the requirement for entities to appoint a DPO with a 'new requirement to appoint a senior responsible individual' to be responsible for 'most of the tasks' of a DPO.¹²⁴⁶ The UK DCMS observed that it can be difficult to appoint someone who is 'truly independent' and the intent of the proposal is to ensure that an organisation-wide culture of data protection is established at a senior level.¹²⁴⁷

Canada's PIPEDA,¹²⁴⁸ Singapore's PDPA,¹²⁴⁹ and New Zealand's *Privacy Act* feature less-prescriptive requirements to appoint or designate individuals who are accountable for privacy compliance.¹²⁵⁰ The light-touch model employed in these jurisdictions may be preferable in the Australian context, insofar as express requirements to appoint an 'expert' and independent privacy officer may impose high regulatory costs on smaller APP entities. Such a model would permit the APP entity to determine what level of expertise is appropriate in their circumstances,¹²⁵¹ and could allow for the appointment of the responsible person from existing staff.

15.3.1 Proposal

Given the reforms proposed in this paper would require entities to carefully consider their information use and management practices and manage requests by individuals pursuant to enhanced individual rights, having an individual who has designated responsibility for privacy within APP Entities will result in enhanced privacy governance. The role should be recognised as an important one within the entity. For larger organisations, it would be expected that the privacy officer would be at a senior level that reports to the highest management level.

Consideration should be given to excepting or modifying this requirement for some small APP entities that are covered by the Act where they are less able to absorb its associated regulatory costs.

15.2 Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.

1243 GDPR art 37.

1244 Ibid.

1245 GDPR art 38.

1246 Department of Culture, Media and Sport (UK), [Data: A New Direction – Government Response to Consultation](#) (23 June 2022).

1247 Ibid.

1248 PIPEDA, sch 1, cl 4.1.

1249 *Personal Data Protection Act 2012* (Singapore) s 11(3).

1250 NZ Privacy Act s 201.

1251 Submission to the Discussion Paper: [OAIC](#), 172.

15.4 Privacy by design

The OAIC and other submitters recommended that APP 1 be amended to expressly require APP entities to implement a 'privacy by design' approach.¹²⁵² Privacy 108 considered that 'privacy by design' principles are unlikely to be adopted by APP entities unless the expectation is express in the APPs or in very direct guidance from the OAIC.¹²⁵³ Western Union considered privacy by design principles could be a helpful addition to Australian law as it would be in line with GDPR and other overseas jurisdictions (such as Canada) which would enable business to use similar practices for businesses in those jurisdictions.¹²⁵⁴ The Discussion Paper acknowledged the principle of privacy by design enshrined in Article 25 of GDPR.¹²⁵⁵

Privacy by design requires privacy considerations to be designed into projects dealing with personal information from the outset, rather than being 'bolted on' afterwards.¹²⁵⁶ It is aimed at 'at ensuring that privacy is taken into account in all stages of product design and deployment.'¹²⁵⁷ Privacy by design principles include privacy by default, privacy as a core engineering feature of IT and business practices, full lifecycle protection, transparency, and being user-friendly.¹²⁵⁸ Privacy harms are best addressed before they happen through consideration of privacy risks and best practice design embedded into a project or activity at the outset.

APP 1.2 is intended to promote a 'privacy by design' approach¹²⁵⁹ which, along with associated OAIC guidance,¹²⁶⁰ is comparable to the GDPR's privacy by design principle in Article 25(1) GDPR. Under APP 1.2, the organisational practices, procedures and systems that may be reasonable in the circumstances can depend on the nature of the personal information held, the risk of possible adverse consequences for individuals, the nature of the APP entity and the practicability of the steps, including time and cost involved (however an entity is not excused by reason only that it would be inconvenient, time-consuming or would impose some cost to do so).¹²⁶¹ The APP Guidelines note that the purpose of APP 1.2 is to require entities to take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance.¹²⁶²

In Chapter 13, it is also proposed that all APP entities be required to undertake a PIA for high privacy risk activities. PIAs are an important tool to support privacy by design,¹²⁶³ and will better ensure that entities consider information privacy risks before commencing such activities.

1252 Submissions to the Discussion Paper: [OAIC](#), 172; [Professor David Lindsay](#), 8; [elevenM](#), 55; [Australian Privacy Foundation](#), 15; [Privacy 108](#), 38; [Law Council of Australia](#), 18.

1253 Submission to the Discussion Paper: [Privacy 108](#), 38.

1254 Submission to the Discussion Paper: [Western Union](#), 9.

1255 [Discussion Paper](#), 151.

1256 OAIC, [Guide to undertaking privacy impact assessments](#) [2 September 2021]; see also, Submissions to the Discussion Paper: [Data Synergies](#), 25; [The Australia Institute – Centre for Responsible Technology](#), 11.

1257 Submission to the Discussion Paper: [Professor David Lindsay](#), 8, see also, European Data Protection Board, [Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#) [20 October 2020].

1258 Ann Cavoukian, [Privacy by Design: The 7 Foundational Principles](#) (Report, January 2011) .

1259 Explanatory Memorandum, Privacy Legislation Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 73; OAIC, [Guide to undertaking privacy impact assessments](#) [2 September 2021] see also, Submission to the Discussion Paper: [KPMG](#), 19.

1260 OAIC, [APP Guidelines](#) (July 2019) [1.7].

1261 *Ibid* [1.6].

1262 *Ibid* [1.4].

1263 OAIC, [Privacy by Design](#) [Web Page, 5 September 2021].

16. Children's privacy

The Discussion Paper sought feedback on several proposals that would introduce child-specific privacy protections into the Act. The Act does not currently contain specific protections for children¹²⁶⁴ who may be particularly vulnerable to online privacy harms.

The UN Convention on the Rights of the Child (CRC) recognises the need to extend particular care to children.¹²⁶⁵ Submissions to the Review noted that children increasingly rely on online platforms, social media, mobile applications and IoT connected devices in their everyday lives, and that many children and young people view their online and offline lives as 'inextricably linked'.¹²⁶⁶ While these services provide many benefits to children and young people, there is concern that children are increasingly being 'datafied'¹²⁶⁷ and that some entities may collect 'thousands of data points' from children, which could include information about their activities, location, gender, interests, hobbies, moods, mental health and relationship status.¹²⁶⁸

This personal information can be used to build profiles on children and to identify moments when they are particularly vulnerable in order to more effectively target and engage them, which may affect their autonomy and capacity to freely develop their identity.¹²⁶⁹ Submitters have also expressed concern that some entities may share or sell children's personal information, or engage in harmful forms of targeted advertising to children,¹²⁷⁰ including marketing that can promote unhealthy or harmful products or produce psychological or mental health changes such as negative body image.¹²⁷¹

However, the protection of children's privacy must be considered alongside children's rights to safety and protection, participation online and their use of the internet for access to information, freedom of expression and association.¹²⁷² The OAIC submitted that online environments 'give young people the chance to express themselves and build their identities'.¹²⁷³

Australian children and young people also reflected these concerns. Reset Australia's submission to the OP Bill on behalf of children and young people provided poll findings from 16 and 17 year old Australians about the handling of their data. 80 per cent of respondents agreed that more rules should be in place to limit how the data of people under 18 is collected and used¹²⁷⁴ and 82 per cent of young people had encountered advertising that was targeted in a way that made them feel uncomfortable.¹²⁷⁵ However, contributors to Reset's submission also observed how the internet allows them to connect with others and stay informed.¹²⁷⁶

The proposals in this chapter attempt to consider the full range of children's rights, including their privacy, safety and online participation by enshrining a principle that recognises the best interests of the child and recommending the development of a children's privacy code that is modelled on the UK's Age Appropriate Design Code.¹²⁷⁷

¹²⁶⁴ Normann Witzleb et al, *Privacy risks and harms for children and other vulnerable groups in the online environment* (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 7; [ALRC Report 108](#), [68.1].

¹²⁶⁵ [United Nations Convention on the Rights of the Child](#), adopted by the General Assembly of the United Nations on 20 November 1989. See also United Nations Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment* (2 March 2021).

¹²⁶⁶ Submissions to the Discussion Paper: [Commissioner for Children and Young People \(South Australia\)](#), 3; [OAIC](#), 120. Submissions to the Issues Paper: [Castan Centre for Human Rights – Monash University](#), 31-32; [Reset Australia](#), 7-8. See also, United Nations Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment* (2 March 2021) 1.

¹²⁶⁷ UK ICO, *Age Appropriate Design: A Code of Practice for Online Services*, 'Executive summary' (September 2020); Normann Witzleb et al, *Privacy risks and harms for children and other vulnerable groups in the online environment* (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 30, citing Deborah Lupton and Ben Williamson, 'The datafied child: The dataveillance of children and implications for their rights' (2017) 19(5) *New Media & Society* 780.

¹²⁶⁸ Ibid. Submission to the Issues Paper: [Reset Australia](#), 7-8. See also, Submission to the Discussion Paper: [OAIC](#), 120-121; Conor Duffy and John Stewart, 'Investigation reveals tracking by EdTech of millions of Australian school students during COVID lockdowns', *ABC* (online, 25 May 2022); United Nations Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment* (2 March 2021) 11.

¹²⁶⁹ Submission to the Issues Paper: [Reset Australia](#), 7-8. See also Darren Davison, 'Facebook targets "insecure" kids', *The Australian* (online, May 2017) and Normann Witzleb et al, *Privacy risks and harms for children and other vulnerable groups in the online environment* (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 30-31.

¹²⁷⁰ Normann Witzleb et al, *Privacy risks and harms for children and other vulnerable groups in the online environment* (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 29-33; Submission to the Discussion Paper: [OAIC](#), 120. See also, Conor Duffy, 'Facebook approves alcohol, vaping, gambling and dating ads targeting teens, lobby group finds', *ABC* (online, 28 April 2021).

¹²⁷¹ Ibid. See also, Kimberley Bernard, 'Young people at "significant" risk of poor body image after just minutes on TikTok, Instagram, researchers say', *ABC* (online, 29 September 2022).

¹²⁷² United Nations Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment* (2 March 2021) 1-3, 9-13. See also: Submissions to the Discussion Paper: [Commissioner for Children and Young People \(South Australia\)](#), 3-4; Professor Sonia Livingstone, Rishita Nandagiri and Mariya Stoilova, *Children's data and privacy online: Growing up in a digital age. An evidence review* (Report, January 2019) 3, 34; Lisa Archbold et al, 'Adtech and Children's Rights' (2021) 44(3) *University of New South Wales Law Journal* 857, 877.

¹²⁷³ Submission to the Discussion Paper: [OAIC](#), 120.

¹²⁷⁴ Submission to the OP Bill: [Reset Australia – Children & Young People Submission](#), 17.

¹²⁷⁵ Ibid 23.

¹²⁷⁶ Ibid 2.

¹²⁷⁷ UK ICO, *Age Appropriate Design: A Code of Practice for Online Services* (September 2020).

16.1 Defining a child

The Act does not define a child, nor does it make special provision for privacy protections that apply to persons under the age of 18. According to the CRC, a person below the age of 18 years is a child, unless majority is attained earlier under applicable law.¹²⁷⁸ Defining a child as an individual under 18 years of age will allow for the development of child-specific privacy protections in the Act. This position would also be consistent with the *Online Safety Act 2021* (Cth) (Online Safety Act),¹²⁷⁹ the UK Age Appropriate Design Code¹²⁸⁰ and Ireland's *Data Protection Act*.¹²⁸¹

16.1 Define a child as an individual who has not reached 18 years of age.

16.2 Capacity to consent

The Discussion Paper proposed that consent should be provided by a parent or guardian on behalf of a child where the child is under the age of 16. It sought feedback on the circumstances in which parent or guardian consent should be required, and whether parent or guardian consent should be obtained:

- before handling the personal information of a child under 16 (as recommended by the *Digital Platforms Inquiry*¹²⁸²), or
- only in circumstances where the Act currently requires consent, such as for the collection of sensitive information.

The Discussion Paper also queried whether APP entities should be permitted to assess the capacity of a minor on an *individualised* basis where it would be practical to do so.¹²⁸³ It was acknowledged that 'children have varying levels of maturity, and that an individualised assessment of capacity is consistent with available research on developmental psychology.'¹²⁸⁴

There were mixed views on the merits of the Discussion Paper's proposal with some submitters supporting¹²⁸⁵ and some opposing¹²⁸⁶ it. Some suggested that parental consent may provide limited protection for the child due to a lack of digital literacy on the part of some parents, as well as due to practical concerns.¹²⁸⁷ These practical concerns included where two or more parents or guardians do not agree on the best course of action for their child,¹²⁸⁸ where a child is under State guardianship,¹²⁸⁹ and how an organisation must determine which parent to ask for consent.¹²⁹⁰ Several submitters cautioned against an over-reliance on parental consent as a protective mechanism due to the limits of a consent-based framework of privacy regulation and instead favoured stronger regulation of how children's information may be collected, used or disclosed.¹²⁹¹

An age threshold of 16 years of age was supported by only a small number of submitters.¹²⁹² Generally, submitters considered that an age threshold of 16 could diminish the agency of those under 16 who are capable of thinking and

¹²⁷⁸ *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1 577 UNTS 3 (entered into force 2 September 1990) art 1.

¹²⁷⁹ *Online Safety Act 2021* (Cth) s 5.

¹²⁸⁰ UK ICO, *Age Appropriate Design: A Code of Practice for Online Services*, 'Services covered by this code' (September 2020).

¹²⁸¹ *Data Protection Act 2018* (Ireland) s 29.

¹²⁸² ACCC, *DPI Report* 456, 464-70.

¹²⁸³ *Discussion Paper*, 108.

¹²⁸⁴ *Ibid* 102.

¹²⁸⁵ Submissions to the Discussion Paper: [Australian Council for Children and the Media](#); [ACCC](#); [Australian Communications Consumer Action Network](#).

¹²⁸⁶ Submissions to the Discussion Paper: [New South Wales Council for Civil Liberties](#); [Australian Banking Association](#); [Yourtown](#); [Obesity Policy Coalition](#); [Australian Medical Association](#); [Meta](#); [Medical Insurance Group Australia](#).

¹²⁸⁷ See for example Submissions to the Discussion Paper: [New South Wales Council for Civil Liberties](#); [Google](#); [Yourtown](#).

¹²⁸⁸ Submissions to the Discussion Paper: [Salinger Privacy](#); [Electronic Frontiers Australia](#).

¹²⁸⁹ Submission to the Discussion Paper: [Yourtown](#).

¹²⁹⁰ Submission to the Discussion Paper: [Salinger Privacy](#).

¹²⁹¹ Submissions to the Discussion Paper: [Digital Rights Watch](#); [OAIC](#); [Foundation for Alcohol Research and Education](#); [Obesity Policy Coalition](#); [New South Wales Council for Civil Liberties](#). See relatedly, Lisa Archbold et al, 'Adtech and Children's Rights' (2021) 44(3) *University of New South Wales Law Journal* 857.

¹²⁹² Submissions to the Discussion Paper: [Australian Council for Children and the Media](#); [Association of Heads of Independent Schools Australia](#).

acting for themselves, which could be detrimental to children's privacy and dignity in some education and healthcare settings where parental involvement may be harmful, or that it could discourage children from seeking professional help or guidance.¹²⁹³

Some submitters considered that it would be beneficial to allow individualised assessments of capacity (where practical), so that the differing needs of children at different stages of development can be taken into account.¹²⁹⁴ Others noted that this may be impractical in the online context.¹²⁹⁵ Medical stakeholders stressed that entities in healthcare should continue to be permitted to assess capacity on an individualised basis in accordance with *Gillick*.¹²⁹⁶

Very few submitters considered that parental consent should be required before handling *any* personal information of a child,¹²⁹⁷ as recommended by the *Digital Platforms Inquiry*. Most considered this option to be unworkable as many 'legitimate and routine activities need to happen in a child's life, including education, healthcare and more, without organisations having to stop to ask for a parent's consent for every separate example of personal information handling'.¹²⁹⁸

Some stakeholders considered that existing OAIC guidance¹²⁹⁹ should continue to inform how entities determine the capacity of a child.¹³⁰⁰ The OAIC proposed that it is preferable to maintain the existing approach as the 'APP guidelines steer a middle ground between individualised assessment and practicability'.¹³⁰¹

In light of this feedback, it is considered that existing OAIC guidance on children and young people and capacity¹³⁰² should continue to be relied upon by APP entities. In particular, this guidance provides that:

...An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent.

As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.¹³⁰³

This guidance reflects the recommendations of ALRC Report 108¹³⁰⁴ and has the flexibility to allow for the individualised assessment of capacity where it is reasonable and practicable to do so, which is the most evidence-based way to determine whether a child has the capacity to act on their own behalf.¹³⁰⁵ It also reflects the recommendations of the UN Committee on the Rights of the Child's *General Comment No. 25 on Children's Rights in Relation to the Digital Environment* ('UNCRC General Comment 25'), which provides that states parties 'should respect the evolving capacities of the child' in the digital environment¹³⁰⁶ including in relation to consent for the purposes of privacy law.¹³⁰⁷ Finally, it would not require parent or guardian consent to be obtained prior to handling *any* personal information of a child,¹³⁰⁸ which was not well-supported by submissions.

1293 Submissions to the Discussion Paper: [Salinger Privacy](#); [Avant Mutual](#); [OAIC](#); [ABC](#); [Australian Medical Association](#); [Yourtown](#).

1294 Submissions to the Discussion Paper: [Electronic Frontiers Australia](#); [Castan Centre](#).

1295 Submissions to the Discussion Paper: [Australian Council for Children and the Media](#); [Microsoft](#).

1296 Submissions to the Discussion Paper: [Australian Medical Association](#); [Medical Insurance Group Australia](#); [Avant Mutual](#). See, *Secretary of the Department of Health and Community Services v JWB and SMB* (1992) 175 CLR 189.

1297 Submissions to Discussion Paper: [ACCC](#); [Australian Council for Children and the Media](#).

1298 See relatedly, Submissions to Discussion Paper: [Salinger Privacy](#); [Digital Rights Watch](#); [Microsoft](#); [Office of the Victorian Information Commissioner](#); [ABC](#); [SBS](#). See also, [OAIC](#), 122-3.

1299 OAIC, 'Children and Young People' (Web Page); OAIC, [APP Guidelines \(July 2019\) \[B.59\]–\[B.61\]](#).

1300 Submissions to the Discussion Paper: [OAIC](#); [Australian Banking Association](#).

1301 Submission to the Discussion Paper: [OAIC](#), 123.

1302 OAIC, [APP Guidelines](#) (July 2019) [B.55]–[B.61].

1303 *Ibid* [B.59–B.61].

1304 [ALRC Report 108](#), Recommendation 68-1.

1305 *Ibid*, [68.25]–[68.42], [68.102]–[68.107].

1306 United Nations Committee on the Rights of the Child, [General Comment No. 25 \(2021\) on Children's Rights in Relation to the Digital Environment](#) (2 March 2021) [19]–[21].

1307 *Ibid* [71].

1308 ACCC, [DPI Report](#) 456, 464–70.

The OAIC guidance sets the minimum age for presumption of capacity at 15, which was the age recommended by the ALRC Report 108,¹³⁰⁹ and a more recent research paper.¹³¹⁰

The Act does not currently provide that consent must be given with capacity. It may be beneficial to codify this proposition in the Act, so that the existing OAIC guidance on children and young people¹³¹¹ and capacity¹³¹² is more readily enforceable. A useful model for this codification was recommended by the Castan Centre¹³¹³ and exists in Canada's *Personal Information Protection and Electronic Documents Act*, which provides:

[T]he consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.¹³¹⁴

Existing OAIC guidance could continue to clarify the circumstances where it is reasonable for an APP entity to expect, or presume, that an individual has capacity to consent.¹³¹⁵

Submitters also observed that there are many circumstances where a child may wish to disclose their information *without* requiring the consent of a parent or guardian, including for access to sexual health, domestic violence, mental health, drug and alcohol dependency, homelessness and other community services.¹³¹⁶ Any provision that addresses children's capacity to consent should contain legislated exceptions for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary to their interests, such as where a child is seeking confidential advice, child support services or where it would pose a threat to the health and safety of the child. In this regard, the UNCRC General Comment 25 recommends that the providers of 'preventive or counselling services to children in the digital environment should be exempt from any requirement for a child user to obtain parental consent in order to access such services.'¹³¹⁷

The Discussion Paper queried whether an assumed age of capacity should determine when children should be able to exercise privacy requests independently of their parents, including access, correction, objection or erasure requests.¹³¹⁸ The Castan Centre submitted that this would not be desirable 'as the rationale for the assumed age of consent is to ensure that children are protected from the privacy-invasive activities of third parties, not to diminish their autonomy vis a vis their parents and guardians.'¹³¹⁹ On this basis, such a provision would be of limited utility.

1309 [ALRC Report 108](#), Recommendation 68-1.

1310 Normann Witzleb et al, [Privacy risks and harms for children and other vulnerable groups in the online environment](#) (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 93.

1311 OAIC, [APP Guidelines](#) (July 2019) [B.59]–[B.61]; OAIC, [Children and Young People](#) (Web Page, 2022).

1312 OAIC, [APP Guidelines](#) (July 2019) [B.55]–[B.58].

1313 Submission to the Discussion Paper: [Castan Centre](#), 22.

1314 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 6.1.

1315 See OAIC, [Children and Young People](#) (Web Page, 2022); OAIC, [APP Guidelines](#) (July 2019) [B.55]–[B.61].

1316 Submissions to the Discussion Paper: [Yourtown](#); [Australian Medical Association](#); [Privacy 108](#); [Salinger Privacy](#); [Avant Mutual](#).

1317 United Nations Committee on the Rights of the Child, [General Comment No. 25 \(2021\) on Children's Rights in Relation to the Digital Environment](#) (2 March 2021) [78].

1318 [Discussion Paper](#), 108.

1319 Submission to Discussion Paper: [Castan Centre](#), 21.

16.2 Existing OAIC guidance on children and young people and capacity¹³²⁰ should continue to be relied upon by APP entities.

An entity must decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis. If that is not practical, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise.

The Act should codify the principle that valid consent must be given with capacity. Such a provision could state that ‘the consent of an individual is only valid if it is reasonable to expect that an individual to whom the APP entity’s activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.’*

Exceptions should be provided for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary their interests (including, but not limited to confidential healthcare advice, domestic violence, mental health, drug and alcohol, homelessness or other child support and community services).

*The final wording of any legislative provision will be developed through the legislative drafting process.

16.3 Child appropriate privacy policies and collection notices

The Discussion Paper proposed to require that APP 5 collection notices be clear, current and understandable, ‘in particular for any information addressed specifically to a child.’ The proposal responded to submitters’ concerns that privacy notices are difficult for children to understand, which can hinder their comprehension of online data processes and result in a lack of informed consent.¹³²¹ The proposal would align with Article 12(1) GDPR¹³²² and adopt the recommendation of the ACCC’s *Digital Platforms Inquiry* that the Act be amended to require that notices be written in clear and plain language (particularly if addressed to a child).¹³²³ Submitters to the Discussion Paper broadly supported the proposal to require child-appropriate collection notices.¹³²⁴

The Discussion Paper also recommended that the use of visual and graphical communication methods (including infographics or standardised icons) be encouraged as a method to enhance comprehension, noting that some young people may be less likely to engage with purely written privacy information.¹³²⁵ It was noted that visual and graphical communication could be encouraged in Commissioner-issued guidelines or an APP code. Submitters supported the suggestion that a child-appropriate notice could be delivered using diagrams, cartoons, graphics, video or audio content.¹³²⁶ The OAIC submitted that privacy transparency should educate and empower children and were supportive of measures that would achieve ‘more than mere disclosure of material facts.’¹³²⁷

In light of this support, it is proposed that APP entities be required to ensure that privacy information that is

¹³²⁰ OAIC, [APP Guidelines](#) (July 2019) [B.55]–[B.61].

¹³²¹ Submissions to the Issues Paper: [Castan Centre for Human Rights Law – Monash University](#), 41; [Communications Alliance](#), 8; [Centre for Media Transition, UTS](#), 16; [Obesity Policy Coalition](#), 5–6.

¹³²² GDPR 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’.

¹³²³ ACCC, [DPI Report](#) 461.

¹³²⁴ Submissions to the Discussion Paper: [OAIC](#); [Privacy 108](#); [Australian Council for Children and the Media](#); [Information and Privacy Commission \(NSW\)](#); [Obesity Policy Coalition](#); [New South Wales Council for Civil Liberties](#); [Department of Health \(Cth\)](#); [Meta](#).

¹³²⁵ [Discussion Paper](#), 105. See also Submissions to the Issues Paper: [Reset Australia](#), 8; [Australian Council on Children and the Media](#), 3; [Communications Alliance](#), 8.

¹³²⁶ Submissions to the Discussion Paper: [OAIC](#); [Australian Council for Children and the Media](#).

¹³²⁷ Submission to the Discussion Paper: [OAIC](#), 124.

addressed to a child be child-appropriate. In addition to collection notices, it is proposed that the requirement be extended to privacy policies.

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. 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 meet their obligations. The Basic Online Safety Expectations also contain requirements that certain information, including policies and procedures in relation to safety, be written in plain language.¹³²⁸

Some submitters considered that further practical guidance could be beneficial to ensure that entities are able to meet this requirement when providing notice to children.¹³²⁹ The NSW Council for Civil Liberties submitted that entities should take steps to ensure that the notification is tailored in terms of content, style, mode of delivery and timing in order for it to be effective and appropriate for the variety of ages and abilities of individuals from whom information will be collected.¹³³⁰

OAIC guidance, as well as a Children's Online Privacy Code (Proposal 16.5), could set out more prescriptive requirements on the format, timing and readability of collection notices and privacy policies. This could include prescriptive requirements in relation to:

- whether the information should be written at a particular readability level, depending on the age of likely users¹³³¹
- whether child appropriate information must be displayed in a particular format or at a particular time,¹³³² and
- whether notice must be provided of matters in addition to APP 5.2, including that an online service provides parental controls or allows a parent or guardian to monitor their child's online activity.¹³³³

This could include the use of visual or graphical communication (including infographics or standardised icons). Similar requirements have been introduced in the UK Age Appropriate Design Code¹³³⁴ and Ireland's Fundamentals for a Child-Oriented Approach to Data Processing,¹³³⁵ which encourage entities to use diagrams, cartoons, graphics, video and audio content rather than relying solely on written communications.

16.3 Amend the Privacy Act to require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a child.*

In the context of online services, these requirements should be further specified in a Children's Online Privacy Code, which should provide guidance on the format, timing and readability of collection notices and privacy policies.

*The final wording of any legislative provision will be developed through the legislative drafting process.

1328 Online Safety (Basic Online Safety Expectations) Determination 2022 (Cth) s 17. The *Online Safety Act 2021* (Cth) empowers the eSafety Commissioner to require online service providers to report on the reasonable steps they are taking to comply with the Expectations.

1329 Submissions to the Discussion Paper: [Department of Health \(Cth\)](#), [New South Wales Council for Civil Liberties](#).

1330 Submission to the Discussion Paper: [New South Wales Council for Civil Liberties](#), 27.

1331 Information Commissioner's Office (UK), *Age Appropriate Design: A Code of Practice for Online Services*: [Transparency](#) (September 2020).

1332 Ibid.

1333 Ibid, [Parental controls](#). See also, Submission to the Discussion Paper: [Commissioner for Children and Young People \(South Australia\)](#), 1, who noted that "[C]hildren and young people see risks to their privacy coming from both within their own 'sphere' (family members and schools) as well as from outside their 'sphere' (governments and commercial interests)." Some of the most common breaches of children's privacy and trust can come from those who children should be able to trust the most: parents and schools."

1334 UK ICO, *Age Appropriate Design: A Code of Practice for Online Services*: [Transparency](#) (September 2020).

1335 Data Protection Commission (Ireland), [The Fundamentals for a Child-Oriented Approach to Data Processing](#) (December 2021) 29-30.

16.4 The Best Interests of the Child

The Discussion Paper proposed that APP entities should have regard to ‘whether the collection, use or disclosure of the personal information is in the best interests of the child’ in assessing whether personal information handling is ‘fair and reasonable in the circumstances’.¹³³⁶

This proposal was well supported by submissions¹³³⁷ and it was considered that a stricter test for the handling of children’s personal information would be appropriate.¹³³⁸ It was argued that adoption of the principle of the best interests of the child would allow for children’s rights of ‘access to information, learning and expression’ to be balanced ‘with the protections for safety and privacy’.¹³³⁹

The concept of the best interests of the child derives from the United Nations Convention on the Rights of the Child¹³⁴⁰ and has been adopted as a primary consideration in both the UK Age Appropriate Design Code and the Irish Data Protection Commission’s Fundamentals for a Child-Oriented Approach to Data Processing.¹³⁴¹ In the privacy law context, 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.¹³⁴² Europe’s Article 29 Data Protection Working Party has further noted that in certain circumstances, the best interests of the child will necessitate a deviation from the protection of privacy, for example, 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.¹³⁴³

In some legal contexts, the consideration of the best interests of the child necessitates detailed inquiry into a particular child’s circumstances and needs.¹³⁴⁴ This may not always be practical in the context of online services who offer services to large cohorts of users (including children) at a distance. In this regard, the UK Age Appropriate Design Code notes that entities should consider the needs of ‘child users’ and how to best support those needs in the design of an online service.¹³⁴⁵ The UNCRC General Comment 25 acknowledges that the best interests of the child is a dynamic concept that requires an assessment appropriate to the specific context, but suggests that states parties ‘ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration’.¹³⁴⁶ It is considered that a similar standard to that set by the UK Age Appropriate Design Code should apply in the Australian context so that online services are required to consider the best interests of ‘child users’ generally in the design of their services, and are not required to embark on an intrusive analysis of a particular child user’s online activities, characteristics and circumstances. This should be clarified in any explanatory material that accompanies the reforms, and further consideration will be given to this issue as part of the implementation of the Review.

The AMA argued that this proposal may have unintended consequences for medical research, as there may be ‘no benefit to a [child] personally for their health information to be collected, used or disclosed for medical research’.¹³⁴⁷ In this regard, 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 that entities must account for the best interests of the child as a *primary consideration* where any conflict arises.¹³⁴⁸ The UK ICO further notes that it is unlikely that the commercial interests of an organisation will outweigh a child’s right to privacy.¹³⁴⁹

¹³³⁶ Discussion Paper, 89, 105-7.

¹³³⁷ Submissions to the Discussion Paper: OAIC; Australian Council for Children and the Media; Salinger Privacy; Electronic Frontiers Australia; Department of Health (Cth); Castan Centre; Commissioner for Children and Young People (South Australia); Digital Rights Watch; Obesity Policy Coalition; Foundation for Alcohol Research and Education; Yourtown; Guardian Australia; DIGI.

¹³³⁸ Submission to the Discussion Paper: Guardian Australia.

¹³³⁹ Submissions to the Discussion Paper: Yourtown, 4. See relatedly, Commissioner for Children and Young People (South Australia); Information Commissioner’s Office (UK), *Age Appropriate Design: A Code of Practice for Online Services: Best interests of the child* (September 2020).

¹³⁴⁰ United Nations Convention on the Rights of the Child, art 3. See also, United Nations Committee on the Rights of the Child, *General Comment No. 25 on Children’s Rights in Relation to the Digital Environment* (2 March 2021) 2-3.

¹³⁴¹ Information Commissioner’s Office (UK), *Age Appropriate Design: A Code of Practice for Online Services, ‘Best interests of the child’* (September 2020); Data Protection Commission (Ireland), *The Fundamentals for a Child-Oriented Approach to Data Processing* (December 2021).

¹³⁴² Information Commissioner’s Office (UK), *Age Appropriate Design: A Code of Practice for Online Services, ‘Best interests of the child’* (September 2020); United Nations Committee on the Rights of the Child, *General Comment No 14: The right of the child to have his or her best interests taken as a primary consideration* (29 May 2013) 4. See relatedly, *California Age-Appropriate Design Code Act* (2022) 1.81.47 Cal Civil Code §1798.99.31(b)(1).

¹³⁴³ 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.

¹³⁴⁴ See e.g. *Family Law Act 1975* (Cth) s 60CC.

¹³⁴⁵ UK ICO, *Age Appropriate Design: A Code of Practice for Online Services: Best interests of the child* (September 2020).

¹³⁴⁶ United Nations Committee on the Rights of the Child, *General Comment No. 25 [2021] on Children’s Rights in Relation to the Digital Environment* (2 March 2021) 2-3.

¹³⁴⁷ Submission to the Discussion Paper: Australian Medical Association.

¹³⁴⁸ UK ICO, *Age Appropriate Design: A Code of Practice for Online Services: Best interests of the child* (September 2020).

¹³⁴⁹ Ibid.

16.4 Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances (see Proposal 12.1).

16.5 Prohibited collections, uses and disclosures

The Discussion Paper did not specifically propose to prohibit the handling of children's personal information in high risk contexts, however it invited feedback on whether specific acts or practices should be prohibited.¹³⁵⁰ It noted that any prohibitions would need to be appropriately targeted to avoid proscribing socially beneficial or legitimate practices.¹³⁵¹

Several submissions to the Discussion Paper considered that prohibitions should be recognised in the Privacy Act, including:

- the handling of children's personal information for the purposes of commercial profiling, behavioural advertising, service personalisation or forms of 'digital consumer manipulation'¹³⁵²
- the disclosure of a child's personal information to a third party which exposes the child to potential safety or privacy risks,¹³⁵³ and
- the sale of a child's personal information.¹³⁵⁴

The OAIC considered that the profiling of children online and the personalisation of their experiences in order to target them with behavioural advertising or other content can increase risks and cause harms to children.¹³⁵⁵ Submitters cited Europe's proposed *Digital Services Act*¹³⁵⁶ and the UNCRC General Comment 25¹³⁵⁷ as examples of international instruments that have proposed to prohibit harmful forms of commercial targeted advertising or profiling.¹³⁵⁸ Ireland's Fundamentals for a Child-Oriented Approach to Data Processing also states that 'organisations should not profile children, engage in automated decision-making concerning children, or otherwise use their personal data, for advertising/marketing purposes, unless they can clearly demonstrate how and why it is in the best interests of children to do so.'¹³⁵⁹

Some submitters noted that certain forms of non-commercial targeted marketing may not be harmful, such as campaigns directed at children to raise awareness of Kids Helpline or healthy eating.¹³⁶⁰ Yourtown submitted that any reference to targeted marketing under the Act should exclude the use of data for education and information sharing in relation to essential support and help services, such as Kids Helpline.¹³⁶¹ The South Australian Commissioner for Children and Young People submitted that it is important for the Act to 'appropriately protect children's privacy in a way that does not limit other rights or access to opportunities or benefits either online or offline' and stressed that this would be particularly important when considering the scope of prohibited practices or 'privacy by default' settings.¹³⁶²

¹³⁵⁰ [Discussion Paper](#), 97.

¹³⁵¹ *Ibid.* The Discussion Paper noted as an example that '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.'

¹³⁵² Submissions to the Discussion Paper: [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 9; [Castan Centre](#), 19; [Obesity Policy Coalition](#), 10; [Foundation for Alcohol Research and Education](#), 14.

¹³⁵³ Submission to the Discussion Paper: [Australian Council on Children and the Media](#), 14.

¹³⁵⁴ *Ibid.*

¹³⁵⁵ Submission to the Discussion Paper: [OAIC](#), 106-7.

¹³⁵⁶ Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services ([Digital Services Act](#)) and amending Directive 2000/31/EC, Amendment 500: 'Targeting or amplification techniques that process, reveal or infer personal data of minors or personal data referred to in Article 9(1) of Regulation (EU) 2016/679 for the purpose of displaying advertisements are prohibited.'

¹³⁵⁷ United Nations Committee on the Rights of the Child, [General Comment No. 25 \(2021\) on Children's Rights in Relation to the Digital Environment](#) (2 March 2021), 7 [42]: 'States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children.'

¹³⁵⁸ Submission to the Discussion Paper: [OAIC](#), 107; [Foundation for Alcohol Research and Education](#), 5.

¹³⁵⁹ Data Protection Commission (Ireland), [The Fundamentals for a Child-Oriented Approach to Data Processing](#) (December 2021) 57.

¹³⁶⁰ Submissions to the Discussion Paper: [Yourtown](#); [Salinger Privacy](#).

¹³⁶¹ Submission to the Discussion Paper: [Yourtown](#).

¹³⁶² Submission to the Discussion Paper: [Commissioner for Children and Young People \(South Australia\)](#), 4.

Chapter 20 of this Report proposes to prohibit:

- direct marketing to a child unless the personal information used for the direct marketing was collected directly from the child and the direct marketing is in the child's best interests.
- targeting to a child, with an exception for targeting that is in the child's best interests.
- trading in the personal information of children.

The exceptions for the best interests of the child are crucial to ensure that targeted marketing for essential child support, counselling and community services can continue and that children's rights to participation online are not unduly limited.¹³⁶³ The scope and framing of these exceptions will continue to be considered as part of the implementation of the Review.

16.6 Children's Online Privacy Code

Several children's privacy codes have been developed internationally, including in the UK,¹³⁶⁴ Ireland¹³⁶⁵ and California.¹³⁶⁶ Submissions to the Review have expressed support for the development of a children's online privacy code, modelled on the UK Age Appropriate Design Code.¹³⁶⁷ In its submission to the Issues Paper, the Castan Centre suggested that a code modelled on the UK Age Appropriate Design Code would address 'children's desire for increased transparency, accessibility and flexibility in their dealings with online service providers'.¹³⁶⁸

A children's online privacy code would have the benefit of clarifying the principles-based requirements of the Act in more prescriptive terms, and would provide guidance on how the best interests of the child should be upheld in the design of online services. For example, 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.¹³⁶⁹ It encourages entities to implement 'high privacy' settings by default unless the entity can demonstrate a compelling reason for a different default setting.¹³⁷⁰ 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
- 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
- users should have the option to change settings permanently or just for the current use, and
- nudge techniques to lead or encourage children to provide unnecessary personal data or to turn off privacy protections should not be used.

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 may collect only the minimum amount of personal data needed to provide elements of a service in which a child is actively and knowingly engaged.¹³⁷¹ In addition to recommending default settings and limits to detrimental uses of children's data, the UK Age Appropriate Design Code introduces standards in relation to parental controls,¹³⁷² child-appropriate privacy information and privacy rights,¹³⁷³ and a standard for establishing (with a level of certainty that is appropriate to the risks) the age range of individual users, in order to provide appropriate protections.¹³⁷⁴

¹³⁶³ Ibid.

¹³⁶⁴ UK ICO, [Age Appropriate Design: A Code of Practice for Online Services](#) (September 2020).

¹³⁶⁵ Data Protection Commission (Ireland), [The Fundamentals for a Child-Oriented Approach to Data Processing](#) (December 2021).

¹³⁶⁶ [California Age-Appropriate Design Code Act](#) [2022] 1.81.47 Cal Civil Code.

¹³⁶⁷ 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](#), 3, [ABC](#), 5–6; [Deloitte](#), 24. Submissions to the Discussion Paper: [Meta](#), [DIGI](#). See relatedly, Submission to the Discussion Paper: [Google](#).

¹³⁶⁸ Submission to the Issues Paper: [Castan Centre for Human Rights Law – Monash University](#), 43.

¹³⁶⁹ Information Commissioner's Office (UK), [Age Appropriate Design: A Code of Practice for Online Services](#) (September 2020).

¹³⁷⁰ Ibid.

¹³⁷¹ Ibid.

¹³⁷² UK ICO, [Age Appropriate Design: A Code of Practice for Online Services: Parental controls](#) (September 2020).

¹³⁷³ Ibid, [Transparency](#) and [Online tools](#).

¹³⁷⁴ Ibid, [Age appropriate application](#).

The OP Bill proposed that an Online Privacy Code ('OP Code') be developed which would have included requirements as to how social media services, data brokerage services and large online platforms handle personal information. The Code would have also required stricter requirements to be in place for social media services, including a requirement to take all reasonable steps to verify the age of individuals who use social media services.¹³⁷⁵

The Discussion Paper sought feedback on whether other sectors, aside from social media, pose privacy risks to children which warrant the enhanced protections of a children's privacy code. The Castan Centre considered that the following contexts could benefit from enhanced requirements set out in a children's privacy code:

- educational technology/learning analytics¹³⁷⁶
- behavioural advertising activities directed at children, and
- other activities involving the intentional tracking, monitoring, profiling or targeting of children.¹³⁷⁷

It is considered that the scope of a children's online privacy code should be aligned with that of the UK Age Appropriate Design Code so that it applies to online services 'that are likely to be accessed by children.'¹³⁷⁸ The UK ICO has noted that the Age Appropriate Design Code applies to 'apps, programs, connected toys and devices, search engines, social media platforms, streaming services, online games, news or educational websites and websites offering other goods or services to users over the internet' and is 'not restricted to services specifically directed at children.'¹³⁷⁹ The Age Appropriate Design Code exempts certain entities including services provided by public authorities, 'traditional voice telephony services', and preventative or counselling services.¹³⁸⁰

Adopting this scope for an Australian online children's privacy code would enable the code developer to draw from the experience of the UK ICO when developing the code, and would promote standardisation for regulated entities that operate internationally. It would also ensure that children are protected in contexts beyond social media, including when using educational technology¹³⁸¹ and internet of things (IoT) devices.¹³⁸²

Online safety codes are also currently being developed under the Online Safety Act.¹³⁸³ It would be important for the code developer to consider the relationship between these and the children's online privacy code, to ensure that requirements are consistent.

Submissions to the OP Bill considered that the privacy-intrusive nature of age verification would greatly outweigh its benefits and would lead to increased collection of personal information from individuals, including children.¹³⁸⁴ It was suggested by some submitters that the broader concept of 'age assurance' techniques be considered,¹³⁸⁵ which would be less privacy intrusive, and could better allow for risk based measures including technical measures.¹³⁸⁶ In this regard, the UK Age Appropriate Design Code provides a balanced model which could guide the development of the Code in the Australian context:

Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead.¹³⁸⁷

1375 Exposure Draft, Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth).

1376 See also, Submission to the Discussion Paper: [Commissioner for Children and Young People \(South Australia\)](#).

1377 Submission to the Discussion Paper: [Castan Centre](#), 21.

1378 UK ICO, [Age Appropriate Design: A Code of Practice for Online Services: Services covered by this code](#) (September 2020).

1379 Ibid.

1380 Ibid, see subsection titled: 'What types of online services are not relevant ISS?'

1381 Conor Duffy and John Stewart, 'Investigation reveals tracking by EdTech of millions of Australian school students during COVID lockdowns', [ABC News](#) (online, 25 May 2022).

1382 UK ICO, [Age Appropriate Design: A Code of Practice for Online Services: Connected toys and devices](#) (September 2020).

1383 [Online Safety Act 2021](#) (Cth); eSafety Commissioner, 'Industry codes' (Web Page).

1384 See e.g. Submissions to the OP Bill: [elevenM](#); [Snap Inc](#); [Alannah & Madeline Foundation](#); [Australian Association of National Advertisers](#); [Google](#); [Meta](#); [DIGI](#); [Business Council of Australia](#); [Communications Alliance](#); [IoT Alliance Australia](#); [IGEA](#); [Electronic Frontiers Australia](#); [Reset Australia](#); [Australian Privacy Foundation](#); [Yourtown](#); [Dr Katharine Kemp](#); [Salinger Privacy](#); [New South Wales Council for Civil Liberties](#); [Office of the Victorian Information Commissioner](#); [Association for Data-driven Marketing & Advertising \(ADMA\)](#).

1385 See for example Submissions to the OP Bill: [elevenM](#); [Snap Inc](#); [Alannah & Madeline Foundation](#); [Google](#); [Meta](#); [DIGI](#). Submissions to the Discussion Paper: [Snap Inc](#); [Google](#); [Meta](#).

1386 UK ICO, [Age Appropriate Design: A Code of Practice for Online Services: Age appropriate application](#) (September 2020).

1387 Ibid.

The code developer could also have regard to the Office of the eSafety Commissioner's consultations on if, and how, a mandatory age verification mechanism (or similar) could practically be achieved in Australia. While the roadmap which eSafety is developing is considering the narrower context of access to online pornography the findings may be applicable to the use of age assurance measures across a range of online harms.¹³⁸⁸

Submissions to the OP Bill also proposed that the code developer should be required to consult with children and child-welfare experts.¹³⁸⁹ Other submitters argued that it would be difficult to find a suitable industry code developer to represent the range of sectors that would be regulated,¹³⁹⁰ or that the OAIC should be appointed as the code developer instead of adopting an industry-led self-regulation model.¹³⁹¹

The UK Data Protection Act, in appointing the UK Information Commissioner's Office as the code developer, required the ICO to consult with 'children, parents, persons who appear to the Commissioner to represent the interests of children, child development experts and trade associations'.¹³⁹² A similar statutory requirement to consult with children and other affected parties should be included in the implementation of these reforms.

The eSafety Commissioner should also be consulted, in light of the intersection of privacy and safety matters in the digital environment. This would assist in ensuring regulatory consistency and avoiding duplication.

Proposal 5.1 of this report is that the Act be amended to allow the IC to make an APP code on the direction or approval of the AttorneyGeneral 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. If implemented, this proposal could be used for the selection of a code developer in the children's privacy context.

1388 Office of the eSafety Commissioner, [Age verification roadmap consultations: Round 1](#) (Report, May 2022); [Age verification roadmap consultations: Round 2](#) (Report, October 2022).

1389 Submissions to the OP Bill: [UNICEF](#); [Dr Jonathon Hutchinson](#), [Dr Justine Humphry and Dr Olga Boichak](#); [Australian Human Rights Commission](#); [Castan Centre](#); [Yourtown](#); [Alannah & Madeline Foundation](#); [Reset Australia](#).

1390 Submissions to the OP Bill: [DIGI](#); [Australian Banking Association](#); [Tech Council of Australia](#); [FreeTV Australia](#); [Virgin Australia Group](#).

1391 Submissions to the OP Bill: [CHOICE](#); [Reset Australia](#); [Graham Greenleaf](#), [UNSW Sydney](#); [Dr Michael Douglas](#); [Australian Council on Children and the Media](#); [Office of the Victorian Information Commissioner](#); [The Australia Institute – Centre for Responsible Technology](#); [Dr Katharine Kemp](#); [Alannah & Madeline Foundation](#).

1392 *Data Protection Act 2018* (UK), s 123.

16.5 Introduce a Children’s Online Privacy Code that applies to online services that are ‘likely to be accessed by children’. To the extent possible, the scope of an Australian children’s online privacy code could align with the scope of the UK Age Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services.

The code developer should be required to consult broadly with children, parents, child development experts, child-welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted.

The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service, including:

- **whether, in the context of online services that are likely to be accessed by children, specific requirements are needed for assessing capacity**
- **whether certain collections, uses and disclosures of children’s personal information should be limited**
- **which default privacy settings should be in place for children that use online services**
- **whether entities should be required to ‘establish age with a level of certainty that is appropriate to the risks’ or apply the standards in the Children’s Code to all users instead¹³⁹³**
- **how privacy information (including collection notices and privacy policies) and tools that enable children to exercise privacy rights (including erasure requests) should be designed to improve accessibility for children, and**
- **if parental controls are provided, how to balance the protection of the child with a child’s right to autonomy and privacy from their parents in certain circumstances.**

¹³⁹³ UK ICO, [Age Appropriate Design: A Code of Practice for Online Services: Age appropriate application](#) (September 2020).

17. People experiencing vulnerability

The ACCC's DPI Report drew attention to potential harms arising from a range of problematic data practices, noting that vulnerable consumers faced particular risks.¹³⁹⁴ It stated that 'certain groups of consumers may lack the technical, critical and social skills to engage with the internet in a safe and beneficial manner,' and that some practices – including targeting based on identified or inferred vulnerabilities – magnify the harm vulnerable consumers face.¹³⁹⁵ Some submissions to the Issues Paper said that further consideration should be given to additional or different privacy protections for individuals with vulnerabilities, including adults experiencing temporary or permanent incapacity for reasons such as disability, illness and injury.¹³⁹⁶

The Discussion Paper considered whether the Act recognises third parties to make decisions on behalf of another person. It did not make any specific proposals in relation to privacy protections for people experiencing vulnerability in light of provisions in the lapsed OP Bill which proposed that an OP Code would specify how requirements under the Act should apply to individuals physically or legally incapable of giving consent.

Submissions in response to the Discussion Paper generally supported improving privacy protection of vulnerable individuals, but raised concerns in relation to:

- what is meant by vulnerability¹³⁹⁷
- how to identify vulnerability¹³⁹⁸
- the risk that individuals would be required to disclose further personal and sensitive information to benefit from additional protections,¹³⁹⁹ and
- issues pertaining to capacity and consent for people experiencing vulnerability.¹⁴⁰⁰

17.1 Protections for people experiencing vulnerability

Feedback to the Review highlighted that improved privacy protections for all individuals through a number of the proposals in this Report will address many of the issues faced by people experiencing vulnerability. The Foundation for Alcohol Research and Education submitted that the proposals in the Discussion Paper 'that will ensure companies take more of a privacy by design approach and incorporate measures to reduce privacy harms, will provide overarching protections that also act to protect 'vulnerable individuals''.¹⁴⁰¹

A paper prepared for the OAIC by Monash University and elevenM Consulting indicates that 'the best way to secure the privacy of vulnerable adults online is through strong baseline protections for all adults, combined with flexible obligations to take greater care or apply additional protections or provide greater support where vulnerabilities are disclosed or detected.'¹⁴⁰² Digital Rights Watch submitted that robust privacy protections for *everyone* would go a long way to protect children and vulnerable people.¹⁴⁰³ elevenM submitted that certain Discussion Paper proposals 'based on standards of reasonableness scale effectively to afford higher standards of protection towards younger children and more vulnerable individuals.'¹⁴⁰⁴

1394 ACCC, [DPI report](#) 25, 447. See also research cited by [Uniting Church in Australia, Synod of Victoria and Tasmania](#), that people with cognitive disabilities are among the most vulnerable to privacy threats such as cyberbullying and financial and sexual exploitation: Submission to Discussion Paper, 4.

1395 ACCC, [DPI report](#) 447 - 448.

1396 Submissions to the Issues Paper: [Law Institute of Victoria](#), 9; [Legal Aid Queensland](#), 7; [Guardian Australia](#), 15; [Salinger Privacy](#), 23.

1397 Submissions to the Discussion Paper: [Foundation for Alcohol Research and Education](#), 17; [EWON](#), 2 (submission endorsed by [Energy and Water Ombudsman SA](#), [Energy and Water Ombudsman \[Victoria\]](#) and [Energy and Water Ombudsman Queensland](#)); [Woolworths Group](#), 11; [Retail Drinks Australia](#), 5; [Social Services Portfolio](#), 26. See also Submissions to the Discussion Paper: [Castan Centre](#), 23-24; [Australian Privacy Foundation](#), 11; Cf [Australian Retail Credit Association](#), 11 (who did not support additional or different privacy protections).

1398 Submission to the Discussion Paper: [Social Services Portfolio](#), 26; [OAIC](#), 126.

1399 Submissions to the Discussion Paper: [Foundation for Alcohol Research and Education](#), 17; [Calabash Solutions](#), 16; [Obesity Policy Coalition](#), 13; [OAIC](#), 126.

1400 Submissions to the Discussion Paper: [Law Council of Australia](#), 15; [Social Services Portfolio](#), 26; [Retail Drinks Australia](#), 6; [EWON](#), 2; [Lived Experience Australia](#), 4; [Ramsay Health Care Australia](#), 8.

1401 Submission to the Discussion Paper: [Foundation for Alcohol Research and Education](#), 17.

1402 Normann Witzleb et al, [Privacy risks and harms for children and other vulnerable groups in the online environment](#) (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 180, noting that additional requirements could be considered where individuals are at risk that their specific privacy needs are not met by these general protections.

1403 Submission to the Discussion Paper: [Digital Rights Watch](#), 15, who submitted that such protections should include the creation of a federal right to privacy.

1404 Submission to the Discussion Paper: [elevenM](#), 38. It cited Discussion Paper proposals 10.1 and 10.2 (fair and reasonableness requirements), 11.1 (restricted and prohibited practices), and 12.1 (pro privacy default settings). A number of other submitters also cited the 'fair and reasonable test' as a positive example of such a measure: Submissions to the Discussion Paper: [Foundation for Alcohol Research and Education](#), 17; [Castan Centre](#), 23; [Australian Communications Consumer Action Network](#), 11; [Salinger Privacy](#), 21. Cf Submission to the Discussion Paper: [Commonwealth Bank of Australia](#) which queried how 'fair and reasonable' factors might apply to proactive measures entities may take to protect vulnerable consumers, 3.

17.1.1 Application of general privacy protections to people experiencing vulnerability

The general application of proposals in this Report would uplift privacy protections for all individuals including people experiencing vulnerability. Where an entity is aware that its customers or individuals affected by its information-handling practices may be experiencing vulnerability, this may be factored into the entity's compliance with the requirement. This may be relevant particularly in relation to the proposals requiring entities to:

- ensure their information-handling is fair and reasonable; and
- conduct Privacy Impact Assessments for high-risk practices.

Fair and reasonable

In Chapter 12 it is proposed that the assessment of the fairness and reasonableness of information handling be guided by certain legislated factors, including 'the risk of unjustified adverse impacts or harm.' While the 'fair and reasonable test' would be assessed objectively, where an entity is aware that it is likely to be handling information of people experiencing vulnerability, or is engaging in activities which could have a significant effect on people experiencing certain vulnerabilities, those circumstances will be relevant to whether the entity's information handling objectively satisfies the fair and reasonable test. Any information the APP entity has, or ought to have, about the likely vulnerabilities of their users would be relevant in determining whether a collection, use or disclosure is fair and reasonable in the circumstances.¹⁴⁰⁵

Privacy Impact Assessments

As noted in Chapter 13, it is proposed that APP entities conduct a Privacy Impact Assessment (PIA) prior to commencing a high privacy risk activity. Such activities include those likely to have a significant impact on the privacy of individuals, in line with existing requirements for Australian Government agencies.¹⁴⁰⁶ According to the OAIC guidance the impact on the privacy of individuals 'may vary based on their individual circumstances, so you should consider whether some individuals may be more significantly impacted than others.'¹⁴⁰⁷ A list of factors indicate when a project may be high risk, including: 'handling personal information of individuals with particular needs.'¹⁴⁰⁸ Given the breadth of vulnerability factors that may cause a person to be more susceptible to harm, it is proposed that an entity conduct a PIA before commencing an activity where the entity is aware, or ought to be aware, that an individual (or group of individuals) is experiencing vulnerability and the activity might have a significant effect on that individual (or cohort).

17.1.2 When is an individual vulnerable?

Supporting APP entities to identify when a person might be experiencing vulnerability would assist them in determining how best to comply with their obligations under the Act. However, vulnerability is currently not defined in the Act or OAIC guidance.¹⁴⁰⁹

Submitters considered the definition of vulnerability expressed in the Discussion Paper ('individuals with vulnerabilities, including adults experiencing temporary or permanent incapacity for reasons such as disability, illness and injury') was insufficient. The Foundation for Alcohol Research and Education considered that the definition was too limited, within the context of digital marketing practices, and would do little to address the ways in which data is processed to target and create vulnerability.¹⁴¹⁰ Stakeholders submitted that vulnerability must be viewed as multifaceted, not confined to mental or physical capacity,¹⁴¹¹ nor a fixed trait associated with a specific group or identifiable threshold.¹⁴¹²

¹⁴⁰⁵ Normann Witzleb et al, [Privacy risks and harms for children and other vulnerable groups in the online environment](#) (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 180. This was proposed as one of several additional factors for inclusion in the OP code.

¹⁴⁰⁶ Privacy [Australian Government Agencies – Governance] APP Code 2017 (Cth) cl 12. Privacy Act s 33D.

¹⁴⁰⁷ OAIC, [When do agencies need to conduct a privacy impact assessment?](#) (Web Page, 14 September 2020).

¹⁴⁰⁸ Ibid.

¹⁴⁰⁹ Normann Witzleb et al, [Privacy risks and harms for children and other vulnerable groups in the online environment](#) (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020). The paper states that the Act 'does not make explicit reference to vulnerable groups and their particular needs for protection. Likewise, the APP Guidelines do not make any special provision for vulnerable groups', 139.

¹⁴¹⁰ Submission to the Discussion Paper, [Foundation for Alcohol Research and Education](#), 17.

¹⁴¹¹ Submission to the Discussion Paper: [Energy and Water Ombudsman NSW](#), 2 which submitted that it was critical that the significant vulnerability experienced due to family violence be included.

¹⁴¹² Submission to the Discussion Paper: [Social Services Portfolio](#), 26; [OAIC](#), 126 and [Castan Centre](#), 24 - both citing Normann Witzleb et al, [Privacy risks and harms for children and other vulnerable groups in the online environment](#) (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020).

Given the varied and intersecting ways in which a person can experience vulnerability, submitters proposed that factors should be used to identify individuals who *may* be at higher risk of harm from interferences with their personal information, rather than attempting to define vulnerability as a particular state.¹⁴¹³ The OAIC endorsed viewing vulnerability as ‘a heightened susceptibility to harm’ which can be influenced by individual characteristics and situational factors.¹⁴¹⁴

The Banking Code of Practice and the General Insurance Code of Practice, which set standards for dealing with customers including those experiencing vulnerability, identifies factors which may indicate a person is at higher risk of vulnerability. They also encourage customers to self-identify as vulnerable so that they can be provided with additional support. However, submitters to the Review emphasised that the privacy of vulnerable individuals must be protected without measures enabling or encouraging the disclosure of additional personal information.¹⁴¹⁵

It is proposed that factors should be used to identify individuals who *may* be at higher risk of harm from interferences with their personal information. As a person can move in and out of vulnerability, it would be more appropriate to refer to ‘people experiencing vulnerability’ than ‘vulnerable groups’ or ‘vulnerable individuals’. However, requiring individuals to self-identify in relation to their vulnerability is not proposed given its potential to create additional privacy risks.

This approach was recommended in the Monash University and elevenM Consulting paper and is modelled on the approach taken in the banking and insurance industries, and by the eSafety Commissioner.¹⁴¹⁶

1413 Submission to the Discussion Paper [Social Services Portfolio](#), 26; [Castan Centre](#), citing Normann Witzleb et al, [Privacy risks and harms for children and other vulnerable groups in the online environment](#) (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 24. See also Submission to the Discussion Paper: [Australian Privacy Foundation](#), 11, which proposed that the Act contain ‘indicators of vulnerability’.

1414 Submission to the Discussion Paper: [OAIC](#), 126, referencing Normann Witzleb et al, [Privacy risks and harms for children and other vulnerable groups in the online environment](#) (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020). See also Submission to the Discussion paper: [Castan Centre](#), 23; [Australian Privacy Foundation](#), 11.

1415 Submission to the Discussion Paper: [Obesity Policy Coalition](#), 13; [Foundation for Alcohol Research and Education](#), 17.

1416 Normann Witzleb et al, [Privacy risks and harms for children and other vulnerable groups in the online environment](#) (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) Recommendation 22: The Code should adopt a factor-based definition of vulnerability that relies on a non-exhaustive list of risk factors, modelled on approaches adopted by the eSafety Commissioner, in the Banking Code of Practice and the General Insurance Code of Practice 2020. We support this also as an economy-wide measure’, 19.

The Banking Code of Practice ¹⁴¹⁷	2020 General Insurance Code of Practice ¹⁴¹⁸
<p>We are committed to taking extra care with customers who are experiencing vulnerability, including:</p> <ul style="list-style-type: none"> a) age-related impairment; b) cognitive impairment; c) elder abuse; d) family or domestic violence; e) financial abuse; f) mental illness; g) serious illness; or h) any other personal, or financial, circumstance causing significant detriment. <p>We may become aware of your circumstances only if you tell us about them.</p> <p>We will train our staff to act with sensitivity, respect and compassion if you appear to be in a vulnerable situation.</p> <p>If you tell us about your personal or financial circumstance, we will work with you to identify a suitable way for you to access and undertake your banking.</p>	<p>We are committed to taking extra care with customers who experience vulnerability. We recognise that a person's vulnerabilities can give rise to unique needs, and that their needs can change over time and in response to particular situations.</p> <p>A person's vulnerability may be due to a range of factors such as:</p> <ul style="list-style-type: none"> a) age; b) disability; c) mental health conditions; d) physical health conditions; e) family violence; f) language barriers; g) literacy barriers; h) cultural background; i) Aboriginal or Torres Strait Islander status; j) remote location; or k) financial distress. <p>We encourage you to tell us about your vulnerability so that we can work with you to arrange support — otherwise, there is a risk that we may not find out about it.</p>

The eSafety Commissioner uses a multidimensional or '*intersectional*' lens to understand risk, stating, '[t]his approach recognises that some people may be more at risk of experiencing online abuse if they are vulnerable, due to the presence of other factors in their lives. These may relate to gender, age, race, religion, disability, sexuality, cultural background or geographic location. These factors can apply at an individual, social or systemic level and may impact an individual's ability to recognise online risks, use preventative measures to protect themselves from harm, or seek help.'¹⁴¹⁹

Proposal – factors which indicate vulnerability

OAIC guidance should include a non-exhaustive list of both individual characteristics and situational factors, which can alert an APP entity to the potential that an individual may be at a greater risk of privacy harms. This would assist entities to take proactive steps to minimise risks.

Not all individuals to whom one or more of the factors apply will be experiencing vulnerability; the proposed approach is intended to reduce the prospect that a person will be subject to adverse treatment, or impeded in accessing products and services, because of their membership of a particular group.¹⁴²⁰

¹⁴¹⁷ Australian Banking Association, [Banking Code of Practice](#) (October 5 2021) Chapter 14, 22 [38]–[41].

¹⁴¹⁸ Insurance Council of Australia, [General Insurance Code of Practice](#) (5 October 2021) Part 9, 31. 91]–[93]. This part applies to Retail Insurance Products only.

¹⁴¹⁹ eSafety Commissioner, [Protecting voices at risk online](#) 1.

¹⁴²⁰ This concern was raised in Submission to the Discussion Paper: [Social Services Portfolio](#), 26; see also Normann Witzleb et al, [Privacy risks and harms for children and other vulnerable groups in the online environment](#) (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 149.

Although several submitters called for a definition of vulnerability to be included within the Act¹⁴²¹ including it in guidance would enable it to be developed in consultation with stakeholders and allow for greater flexibility and responsiveness to emerging risk factors. It would also enable a clearer articulation of the intersectionality of risk.¹⁴²²

17.1 Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.

17.2 Capacity and consent

The Act enables individuals to make certain decisions and permits decisions to be made by third parties on behalf of an individual by nomination or where there is some other recognised legal arrangement for substituted decision-making. In its Report 108 the ALRC considered that it was not appropriate for the Act to include a mechanism for assessing capacity as such assessments are complex and better dealt with in specialised legislation.¹⁴²³

17.2.1 Third parties acting on behalf of an individual

The Discussion Paper endorsed the ALRC's view that no changes are required to the Act to explicitly recognise third parties acting with consent or legal authority.¹⁴²⁴ The OAIC agreed with this position, submitting that entities may implement their own procedures to enable an individual to nominate a third party to act on their behalf.¹⁴²⁵ The Social Services Portfolio also considered that it is not necessary for the Act to specifically provide for an individual to nominate a person to act on their behalf. At the same time, it sought further guidance on what steps entities should take to ensure nominations, authorities and consents provided by vulnerable people are valid.¹⁴²⁶

Submitters also sought further clarity and guidance on recognition of guardians and third parties,¹⁴²⁷ the third-party nomination process and record keeping requirements,¹⁴²⁸ and in relation to access of information on behalf of individuals without capacity.¹⁴²⁹ Other submitters highlighted complexities of third parties representing people experiencing vulnerability, such as in family violence situations where the third party may be contributing to the represented individual's vulnerable state.¹⁴³⁰

17.2.2 Notice requirements

APP 5 requires an APP entity to provide notice to an individual regarding collection of their personal information. The Monash University and elevenM Consulting paper proposed that if an individual is being supported or represented in their decision making, notice should also be required to be provided to the supporter or decision maker.¹⁴³¹ Arguably such an obligation already applies under APP 5, in that notifying a third party who is involved in an individual's decision-making where the APP entity is aware of their involvement would likely be reasonable in those circumstances.

1421 Submissions to the Discussion Paper: [Australian Privacy Foundation](#), 11; [Castan Centre](#), 23; [Retail Drinks Australia](#), 5.

1422 The government recognises the importance of implementing policies using an intersectional and diversity lens: see, Department of Social Services, [Australia's Disability Strategy 2021 – 2031](#) (December 2021) 36.

1423 [Discussion Paper](#), 110, [ALRC Report 108](#), [70.49]–[7.52].

1424 [Discussion Paper](#), 110.

1425 Submission to the Discussion Paper: [OAIC](#), 126–127.

1426 Submission to the Discussion Paper: [Social Services Portfolio](#), 26.

1427 Submission to the Discussion Paper: [Lived Experience Australia](#), who support specific reference in the Act to Advance Directives, 4.

1428 Submission to the Discussion Paper: [Retail Drinks Australia](#), 6.

1429 Submission to the Discussion Paper: [Ramsay Health Care Australia](#), 8.

1430 Submission to the Discussion Paper: [EWON](#), 2, Attachment 1.

1431 Normann Witzleb et al, [Privacy risks and harms for children and other vulnerable groups in the online environment](#) (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 178.

A number of submitters also highlighted the importance of individuals being able to understand the information in privacy notices in order to provide informed consent.¹⁴³² The Benevolent Society and the Uniting Church in Australia noted the importance of making reasonable efforts to assist people with disabilities or impairments to understand what privacy notices and policies mean, and the implications of giving consent.¹⁴³³ For people with a communication disability, a conversation using shared communication methods was considered critical to ensure understanding and to gain informed consent.¹⁴³⁴

Some submitters thought that privacy notices should be easily readable, understandable and accessible,¹⁴³⁵ particularly for those with disabilities¹⁴³⁶ and should take into account 'the needs, capabilities and behaviours of the reader,'¹⁴³⁷ which would 'recognise the wide variety of ways in which readers may be hindered in their ability to access, consume and understand a notice.'¹⁴³⁸

Submitters considered that privacy notices may need to be provided in languages other than English and in Easy Read and other accessible formats as individuals may be from culturally and linguistically diverse backgrounds or living with disabilities that impact their ability to read and understand such notices.¹⁴³⁹ Professor Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise submitted that notices should also be machine readable.¹⁴⁴⁰

Castan Centre submitted that the Act should provide that consent is valid only if 'it is reasonable to expect that individuals to whom an organisation's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure, to which they are consenting'.¹⁴⁴¹

17.2.3 Proposals relevant to capacity and consent for people experiencing vulnerability

Supporting a person experiencing vulnerability to make privacy decisions may include providing additional or different resources, or it may involve assistance from third parties.¹⁴⁴² In the last decade there have been significant developments in understanding how to promote the rights of people with disabilities and reduced decision-making capacity.¹⁴⁴³ This work is continuing. The Disability Royal Commission held a roundtable on 31 May 2022 to discuss a national policy and legislative framework for supported decision-making and guardianship, and has prepared proposals for reform.¹⁴⁴⁴

It is not necessary to amend the Act to provide for assessment of capacity or to recognise third parties acting with consent or legal authority. Nor should the Act give specific additional authority to informal representatives; the ALRC cautioned that doing so would expose individuals to an unacceptable risk of invasion of their privacy.¹⁴⁴⁵ The ALRC did, however, recommend that guidance be published on 'practices and procedures allowing for the involvement of third parties, with the consent of an individual, to assist an individual to make and communicate privacy decisions.'¹⁴⁴⁶

In Chapter 11 it is proposed that consent be defined to require that it must be voluntary, informed, current, specific, and unambiguous. Chapter 16 further proposes that the Act be amended to clarify that the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organisation's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal

1432 For example, Submissions to the Discussion Paper: [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 4-5; [Benevolent Society](#), 3-4; [Kimberlee Weatherall, Tom Manousaridis, Melanie Trezise](#), 15-18. See also Chapter 11. A key finding of the Normann Witzleb et al, [Privacy risks and harms for children and other vulnerable groups in the online environment](#) (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) was that the best way to improve consent process for people who have limited capacity to provide consent is to improve the transparency and accessibility of privacy notices/policies and to reduce their complexity, 175.

1433 Submissions to the Discussion Paper: [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 4-5; [Benevolent Society](#), 4.

1434 Submission to the Discussion Paper: [Benevolent Society](#), 4.

1435 Submissions to the Discussion Paper: [elevenM](#), 25; [Benevolent Society](#), 3; [Social Services Portfolio](#), 19; [Law Council of Australia](#), 12; [Kimberlee Weatherall, Tom Manousaridis, Melanie Trezise](#) 15, 17 - who submitted implementing Web Content Accessibility Guidelines 2.0 (WCAG) would help ensure notices are readable by people with a disability. See, relatedly, Normann Witzleb et al, [Privacy risks and harms for children and other vulnerable groups in the online environment](#) (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 182-3.

1436 Submission to the Issues Paper: [OAIC](#), 74.

1437 Submission to the Discussion Paper: [elevenM](#), 25.

1438 Ibid.

1439 Submissions to the Discussion Paper: [Benevolent Society](#), 3; [Law Council of Australia](#), 12; [Kimberlee Weatherall, Tom Manousaridis, Melanie Trezise](#) 17.

1440 Submission to the Discussion Paper: [Kimberlee Weatherall, Tom Manousaridis, Melanie Trezise](#) 15, 17.

1441 Submission to the Discussion Paper: [Castan Centre](#), 24.

1442 OAIC, [APP Guidelines](#) (July 2019) [B.57].

1443 Notably, ALRC, [Equality, Capacity and Disability in Commonwealth Laws](#) [Report No 124, 24 November 2014] (ALRC Report 124).

1444 *Royal Commission into Violence, Abuse, Neglect and Exploitation of People with a Disability*, ([Roundtable Supported decision-making and guardianship: proposals for reform](#), 16 May 2022).

1445 [ALRC Report 108](#), 2336 [70.6].

1446 [ALRC Report 108](#), 2371 [70.116], Recommendation 70-3(a), 2374.

information to which they are consenting. Such a provision would ensure that where vulnerability is identified, consent will only be valid where it is reasonable to expect that individual understands what they are consenting to. These proposals would allow for substituted or supported decision-making while also enabling entities to consider the validity of consent in circumstances where vulnerability is identified, such as family and domestic violence contexts.

A number of submitters indicated that if pro-privacy settings are enabled by default, this would protect the privacy needs of the most vulnerable users.¹⁴⁴⁷ It was considered that this would be particularly beneficial for people who find navigating settings and control options difficult, including those with limited digital capacity or some people with a disability.¹⁴⁴⁸

In Chapter 11 it is proposed that online privacy settings should reflect the privacy by default framework of the Act, and that APP entities be required to ensure that any privacy settings are clear and easily accessible for service users. In addition, the proposal in Chapter 10 to introduce a requirement in APP 5 that collection notices be 'understandable' and that 'appropriate accessibility measures be in place' would enhance the ability of people experiencing vulnerability to provide valid consent when making privacy decisions.

This approach is consistent with the *Disability Discrimination Act 1992* (Cth) (DDA) which makes it unlawful for a person who provides goods or services or makes facilities available, to discriminate against another person on the grounds of that person's disability in the terms or conditions on which those goods or services are made available, or in the manner in which those goods and services are made available.¹⁴⁴⁹ The DDA provides an exemption from non-discrimination provisions if avoiding the discrimination would impose an unjustifiable hardship,¹⁴⁵⁰ which involves assessing all the relevant circumstances of the particular case. In assessing what 'appropriate accessibility measures' would be, all relevant circumstances would be taken into account, including the entity's resources and the amount of expenditure that would be required.

Update OIAC guidance on capacity and consent for people experiencing vulnerability

OIAC guidance should also be updated to clarify that APP 5 requires that notice be provided to a third party involved in an individual's decision making where an entity is aware of the third parties' involvement and also to reflect recent developments in supported decision making. This should provide greater clarity on when and how third parties who give decision-making support should be recognised, and what steps entities should take to ensure that authorities, nominations and consents are valid. The guidance should be developed in consultation with affected groups.

17.2 OIAC guidance on capacity and consent should be updated to reflect developments in supported decision-making.

Targeting which exploits vulnerability

A number of stakeholders proposed that the Act should explicitly prohibit the collection, use or disclosure of information to exploit vulnerabilities through profiling and targeted advertising.¹⁴⁵¹ FARE submitted that prohibiting the collection, use or disclosure of sensitive information (such as information related to a person's physical or mental health and wellbeing) for marketing purposes would reduce the risk of companies exploiting or creating vulnerabilities.¹⁴⁵² Chapter 20 proposes that targeting based on sensitive information should be prohibited and that targeting should have to satisfy the fair and reasonable test. These proposals are addressed in part at preventing targeting from exploiting vulnerability.

¹⁴⁴⁷ Submission to the Discussion Paper: [Foundation for Alcohol Research and Education](#), 17; [eleven M](#), 37; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 4; [Salinger Privacy](#), 30; [Castan Centre](#), 20; [Australian Communications Consumer Action Network](#), 12. [Optus](#) submitted that the preferable approach was providing easily accessible privacy settings, Submission to Discussion Paper: 21.

¹⁴⁴⁸ Submissions to the Discussion Paper: [Australian Communications Consumer Action Network](#), 12; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 4.

¹⁴⁴⁹ [Disability Discrimination Act 1992](#) (Cth) s 24.

¹⁴⁵⁰ *Ibid* s 11.

¹⁴⁵¹ Submissions to the Discussion Paper: [Obesity Policy Coalition](#), 13; [Foundation for Alcohol Research and Education](#), 17; [Castan Centre](#), 25. See also Submissions to the Discussion Paper: [UNSW Allens Hub](#), [Deakin CSRI and IEEE SSIT](#), 9; [Office of the Victorian Information Commissioner](#), 6.

¹⁴⁵² Submission to the Discussion Paper: [Foundation for Alcohol Research and Education](#), 17.

Individuals experiencing financial abuse

In its submission the Australian Banking Association (ABA) stated that it has obligations to provide extra care with customers who are experiencing vulnerability, but expressed concerns that there are limited circumstances in which it is able to use or disclose personal information for these purposes, without express and informed consent. Citing a similar provision in the UK Data Protection Act, it recommended

an amendment to the Privacy Act that permits ‘good faith’ disclosure of information to law enforcement or adult safeguarding authorities in circumstances when an individual’s financial safety may be compromised, without a requirement to obtain express consent from such individuals.¹⁴⁵³

The permitted general situations for the collection use and disclosure personal information are set out in s 16A of the Act. Situations in which information can be used or disclosed for a secondary purpose, without consent, are set out in APP 6.

In its 2019 Report on Elder Abuse, the ALRC recommended that banks and other financial institutions take reasonable steps to prevent the financial abuse of their customers.¹⁴⁵⁴ It recommended that people who report suspected abuse to adult safeguarding agencies be given immunity from certain legal obligations that might otherwise prevent them from reporting abuse.¹⁴⁵⁵ Noting the importance of respecting a person’s autonomy, and that mandatory reporting may be seen as ‘intrusive and patronising’ the ALRC did not recommend that all instances of suspected abuse be reported. Instead, it recommended that the circumstances in which banks should report abuse be clearly set out in an industry guideline.¹⁴⁵⁶

It was submitted that banks may not be able to speak directly to the individual at risk (to discuss concerns and obtain informed consent to share personal information) and in such circumstances may find it challenging to engage with the exceptions and exemptions in the Act.¹⁴⁵⁷ Consumer representatives submitted that clarity is required to ensure that banks can act appropriately in the interests of those customers who may be experiencing financial abuse or may no longer have capacity to consent.¹⁴⁵⁸ They submitted that the government should continue to consult with key stakeholders, including the ABA, consumer groups, Australian Financial Complaints Authority (AFCA), Australian Securities and Investments Commission (ASIC) and the OAIC to:

- identify the key issues faced by vulnerable consumers and the barriers faced by banks in acting appropriately, and
- examine and recommend a potential solution or solutions with a lens to avoiding unintended harms to the consumer.¹⁴⁵⁹

While this issue was raised by financial institutions, consideration should be given to whether changes should apply to other sectors. It is proposed that further consultation should be undertaken to clarify the issues and identify options, and in particular to:

- identify the key privacy related issues which APP entities seeking to safeguard individuals at risk of financial abuse are facing,
- consider whether the ABA’s proposal strikes the right balance between respecting an individual’s privacy and personal autonomy, and protecting people from financial abuse, and
- determine whether these concerns could be addressed other than by amendment to the Act, for example: new OAIC guidance or other action by government or stakeholders.

17.3 Further consultation should be undertaken to clarify the issues and identify options to ensure that financial institutions can act appropriately in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent.

¹⁴⁵³ Submission to the Discussion Paper: [Australian Banking Association](#), 22.

¹⁴⁵⁴ ALRC, *Elder Abuse – A National Legal Response* ([Report No 131](#) May 2017) [ALRC Report 131], 295 [9.2], 303 [9.36].

¹⁴⁵⁵ [ALRC Report 131](#), 307 [9.54]

¹⁴⁵⁶ [ALRC Report 131](#), 308 [9.58]–[9.59], quoting the Submission of State Trustees Victoria.

¹⁴⁵⁷ Submissions to the Discussion Paper: [Australian Banking Association](#), 22; [Australian Banking Association, Financial Rights Legal Centre, Consumer Action Law Centre, Economic Abuse Reference Group, COTA Australia, WEstjustice](#), 1–2.

¹⁴⁵⁸ Submission to the Discussion Paper: [Australian Banking Association, Financial Rights Legal Centre, Consumer Action Law Centre, Economic Abuse Reference Group, COTA Australia, WEstjustice](#), 2.

¹⁴⁵⁹ *Ibid.*

18. Rights of the individual

The Discussion Paper put forward proposals for individuals to have new rights in relation to their personal information that are aimed at providing individuals with greater transparency and control. Similar rights are recognised in data protection frameworks overseas, including under the GDPR as ‘data subject rights’.¹⁴⁶⁰

Currently under the Act, individuals are provided limited transparency and control over their personal information through privacy notices (APP 5), privacy policies (APP 1.3), requirements for entities to implement practices, procedures and systems to deal with complaints and inquiries (APP 1.2), and some access rights (APP 12). The destruction requirement in APP 11 is expressed as an obligation on an entity to destroy personal information, but does not provide an individual with the ability to insist on earlier destruction.

In light of stakeholder feedback which reflects community expectations that individuals should have greater transparency and control over their personal information,¹⁴⁶¹ the following rights should be expressly recognised in the Act, subject to specific exceptions for certain rights, and general exceptions to all of the rights.

Rights directed at improving transparency

- Right to access and explanation – a right to know what personal information is held, where it came from, and what is being done with it (including meaningful information about how automated decisions using an individual’s personal information are made).
- Right to object to the collection, use and disclosure of personal information – a right to challenge whether an APP entity’s handling of information complies with the Act.

Rights directed at giving individuals more control over their information

- Right to erasure – a right to have information deleted.
- Right to correction – a right to require that information be accurate, up-to-date, complete, relevant and not misleading.
- Right to de-index certain search results – a narrow right to have internet search results about an individual de-indexed in specific circumstances.

18.1 Right to portability to develop as part of CDR

The Discussion Paper did not propose introducing a right to portability¹⁴⁶² in the Act on the basis that Australia is implementing data portability on a sectoral basis through the Consumer Data Right (CDR).¹⁴⁶³ The vast majority of submitters did not disagree with this position. However, Privacy 108 submitted that giving individuals portability rights in relation to their personal information under the Act as part of a human rights approach would apply a different and complementary lens to securing the most advantageous commercial services, which is the policy objective supported by the CDR.¹⁴⁶⁴ The Australian Privacy Foundation opposed portability noting concerns about the risks to privacy from the CDR.¹⁴⁶⁵

The CDR currently allows sharing of consumer data in the banking sector, with the energy and telecommunications sectors to follow. While coverage is currently limited, it is envisaged that the CDR will be expanded economy-wide in coming years.¹⁴⁶⁶ Having regard to the lack of stakeholder disagreement to the Discussion Paper’s proposed approach, the CDR remains the appropriate sphere to develop this right. However, implementation of new rights for individuals in the Act would need to align with CDR into the future.¹⁴⁶⁷

¹⁴⁶⁰ In addition to European countries, individual rights are also available, with some variations, in Canada (*Personal Information Protection and Electronic Documents Act*, SC 2000, c 5), Japan (*The Act on the Protection of Personal Information*), Singapore (*Personal Data Protection Act 2012*), and California (*California Consumer Privacy Act of 2018*).

¹⁴⁶¹ See for example Submissions to the Discussion Paper: [elevenM](#), 50-53, citing the former UK Information Commissioner; [Privacy 108](#), 26-27; [Experian](#), 17; [Calabash Solutions](#), 16-17.

¹⁴⁶² Data portability is the ability for consumers to move their data between entities and platforms.

¹⁴⁶³ [Discussion Paper](#), 114.

¹⁴⁶⁴ Submission to the Discussion Paper: [Privacy 108](#), 26.

¹⁴⁶⁵ Submission to the Discussion Paper: [Australian Privacy Foundation](#), 12; Australian Privacy Foundation, [Submission to Exposure draft 29 March 2019 Competition and Consumer \(Consumer Data\) Rules 2019](#) (10 May 2019) 4.

¹⁴⁶⁶ Australian Government, Consumer Data Right, [Rollout](#) (Web Page).

¹⁴⁶⁷ Submissions to the Discussion Paper: [Deloitte Australia](#), 30-31.

18.2 Rationale for Rights of the Individual

Personal information is necessary for many activities of APP entities. The Act allows for this while ensuring that '[n]o-one shall be subjected to arbitrary or unlawful interference with his privacy'¹⁴⁶⁸ by establishing a framework which balances the interests of entities in carrying out their functions or activities with the protection of privacy of individuals.¹⁴⁶⁹ Protecting individuals' privacy depends to a large extent on individuals' ability to exercise control in relation to their personal information.

The DPI Report recognised that lack of transparency about what an entity does with an individual's information places them at a significant disadvantage and denies them the ability to make an informed decision about the collection and use of their data.¹⁴⁷⁰ The Act seeks to achieve transparency through the current obligations for APP entities to have a privacy policy, to provide notice of collection, to provide individuals with access to their personal information and an avenue to correct that information.¹⁴⁷¹ Individuals can exert control by providing or withholding consent to information-handling and by seeking access to personal information held by an entity or correction of their personal information.

The DPI Report recommended that a right to erasure be considered as a means of improving the bargaining power imbalance between digital platforms and consumers.¹⁴⁷² Submitters to the Review echoed this view, highlighting that consumers exercising their rights and possibly choosing to engage with entities with better privacy protections would incentivise entities to adopt data practices more in line with consumer expectations.¹⁴⁷³

The Review sought feedback on enhancing the rights which individuals currently have in relation to their personal information.¹⁴⁷⁴ The proposals in the Discussion Paper were well received in principle by a broad range of submitters¹⁴⁷⁵ principally on the grounds they would increase transparency and control for individuals.¹⁴⁷⁶ Submitters also urged caution in their application, on the basis that enhanced rights could impose an unreasonable regulatory burden for businesses,¹⁴⁷⁷ conflict with other legal obligations,¹⁴⁷⁸ disrupt activities undertaken in the public interest,¹⁴⁷⁹ or push the scales too far in favour of the individual such that individuals would be dictating the activities of APP entities.¹⁴⁸⁰

Submitters highlighted that individuals must be able to understand when they can exercise their rights, and distinctions between rights.¹⁴⁸¹ Strict compliance may not always achieve the outcome the individual actually seeks, particularly if the individual wishes to continue to access a service, or the right unreasonably conflicts with the interests of other consumers or the entity.¹⁴⁸² As such, entities and individuals should work together to determine the best way to address individuals' concerns. This could include finding the best right, or combination of rights, to achieve the desired outcome.

This chapter deals with each right in turn. It then sets out the exceptions which would apply to these rights, and concludes with a discussion about how APP entities would comply with the rights. Some of these proposals extend on the proposals in the Discussion Paper. Accordingly, they may need to be refined through further consultation.

1468 ICCPR Article 17; [Explanatory Memorandum](#), Privacy Bill 1988 [Cth] 2, 7.

1469 Privacy Act s 2A(b).

1470 ACCC, [DPI report](#) 419.

1471 Privacy Act sch 1, APP 1, APP 5, APP 12 and APP 13.

1472 ACCC, [DPI report](#) 401, 471.

1473 Ibid 471; Consumer Policy Research Centre, [Submission to the ACCC Digital Platforms Inquiry](#) (February 2019) 8-9.

1474 [Issues Paper](#) 51-53; [Discussion Paper](#) 111-123, 140-143.

1475 See for example Submissions to the Discussion Paper: [Office of the Victorian Information Commissioner \(OVIC\)](#), 6-7; [ACCC](#), 6; [UNSW Allens Hub](#), [Deakin CSRI and IEEE SSIT](#), 9; [Australian Institute of Health and Welfare](#), 7-8; [Obesity Policy Coalition](#), 13-14, 16; [Salinger Privacy](#), 30-31; [elevenM](#), 41-43; [Google](#), 4-5; [Meta](#), 7; [Electronic Frontiers](#), 15; [Woolworths](#), 11; [ACT | The App Association](#), 4-5; [European Commission](#), 5.

1476 See Submissions to the Discussion Paper: [OVIC](#), 6-7; [ACCC](#), 6; [elevenM](#), 41-43.

1477 Submissions to the Discussion Paper: [Telstra](#), 17; [Shopping Centre Council of Australia](#), 8; [Microsoft](#), 8; [Optus](#), 23-24; [Retail Drinks Australia](#), 9-10; [SBS](#), 13.

1478 Submissions to the Discussion Paper: [National Archives of Australia](#), 1-2; [Optus](#), 24-25; [Uniting Church in Australia](#), [Synod of Victoria and Tasmania](#), 5-6.

1479 Submissions to the Discussion Paper: [Services Australia](#), 10; [CSIRO](#), 11; [Australian Federal Police \(AFP\)](#), 3; [Garvan Institute of Medical Research and Garvan Research Foundation](#), 8; [SBS](#), 13; [ABC](#), 9; [Pharmaceutical Society of Australia](#), 3.

1480 See for example Submissions to the Discussion Paper: [Meta](#), 38; [IAB](#), 25.

1481 Submissions to the Discussion Paper: [OAIC](#), 132-133; [Privacy 108](#), 30-31; [Response 840424239](#), 3-4.

1482 See for example Submissions to the Discussion Paper: [Optus](#), 23-24; [Chartered Accountants Australia and New Zealand \(Chartered Accountants ANZ\)](#), 4; [Social Services Portfolio](#), 27.

18.3 Right to access and explanation

A right to access and explanation would provide transparency so an individual could make informed decisions about their personal information, including whether to exercise other rights.

18.3.1 Current access rights

Under APP 12, an entity must provide an individual with personal information the entity holds about them on request. This right is subject to exceptions which mirror the *Freedom of Information Act 1982* (Cth) (FOI Act) for agencies and the exceptions listed in APP 12.3 for organisations. APP 12.5 provides that where the entity cannot give access in the manner requested, it 'must 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'. APP 12.7 provides that agencies must not charge for an access request and APP 12.8 provides that organisations must not apply an excessive charge. APP 12.9 provides that where a request is refused, the refusal must be explained to the individual.

18.3.2 Discussion Paper proposals about access rights

The Discussion Paper proposed three reforms to APP 12:

- (1) Require APP entities to identify the source of personal information they collect indirectly if requested by the individual.
- (2) Create an additional ground for refusing access where it would prejudice external dispute resolution.
- (3) Enable APP entities to consult with and provide the individual with access to their personal information in an alternative manner, and require entities to provide a general summary on request.

The first and third proposals were directed at improving transparency, particularly in relation to third party collections¹⁴⁸³ and to assist APP entities in complying with access requests. They received strong support from privacy advocates,¹⁴⁸⁴ and were broadly supported by some industry and government submitters.¹⁴⁸⁵ Several submitters emphasised the need for exceptions, largely focused on technical difficulties with compliance.¹⁴⁸⁶ Submitters supported the ability to provide access in a more flexible way, believing it could lead to more specific requests, and avoid voluminous material which a consumer needs to understand for themselves.¹⁴⁸⁷ The second proposal was largely viewed as a positive reform,¹⁴⁸⁸ and is discussed again under exceptions later in this chapter.

Transparency through explanation

Although there was support for the Discussion Paper proposals, submissions highlighted these proposals would not provide individuals with an understanding of *how* their information is being used or disclosed. Submitters noted that individuals do not understand or have a limited understanding of what is being done with their information, including why they are receiving certain marketing.¹⁴⁸⁹ According to Deloitte's Privacy Index, 71 per cent of consumers did not fully understand how their personal information would be used after they gave consent.¹⁴⁹⁰ This could be because the notice was misleading or inadequate and the consequences of uses and collections concealed.¹⁴⁹¹

Chapter 10 of this Report proposes an express requirement that collection notices be clear, up-to-date, concise and understandable. This proposal would address some of the deficiencies of current collection notices and therefore may decrease the need for individuals to seek an explanation under this proposed right. However, even effective notices may not ensure individuals will have the relevant knowledge to exercise their rights where it may have been

¹⁴⁸³ And in light of the [Discussion Paper](#) proposal to remove the right in APP 7.6 to request not to receive direct marketing. This proposal has been replaced by the Targeting proposals in Chapter 20 of this report.

¹⁴⁸⁴ Submissions to the Discussion Paper: [elevenM](#), 50-52; [NSW Council for Civil Liberties](#), 33-34; [Privacy 108](#), 33; [Obesity Policy Coalition](#), 16.

¹⁴⁸⁵ See for example Submissions to the Discussion Paper: [Meta](#), 45; [Australian Department of Health](#), 14.

¹⁴⁸⁶ See for example Submissions to the Discussion Paper: [Telstra](#), 22; [Shopping Centre Council of Australia](#), 9; [Snap Inc.](#), 7.

¹⁴⁸⁷ Submissions to the Discussion Paper: [Illion](#), 3; [Financial Rights Legal Centre and Financial Counselling Australia](#), 17-18.

¹⁴⁸⁸ See for example Submissions to the Discussion Paper: [NSW Council for Civil Liberties](#), 33; [elevenM](#), 52; [Australian Collectors & Debt Buyers Association](#), 9.

¹⁴⁸⁹ Submissions to the Discussion Paper: [Obesity Policy Coalition](#), 16; [Public Health Association of Australia](#), 11.

¹⁴⁹⁰ Submission to the Discussion Paper: [Deloitte Australia](#), 15.

¹⁴⁹¹ Submission to the Discussion Paper: [Dr Katharine Kemp, UNSW Sydney](#), 10. APP 5.1 requires that entities must only take such steps (if any) as are reasonable in the circumstances to provide a collection notice.

provided some time ago, may not be sufficiently tailored to an individual, or may not have been provided at all. As one individual submitter noted, in order to exercise rights, an individual must know, understand and remember what the APP entity is doing with their data and when to initiate a request.¹⁴⁹² The OAIC submitted that in order for the right to object to be an valuable tool, it was essential for individuals to have the information necessary for them to understand specific collections, uses and disclosures to which they could make an objection and the consequences of exercising that right.¹⁴⁹³ The European Commission submitted that knowledge of what is being done with an individual's data 'is essential, as only such information will enable the individual to have a measure of control over his/her data, detect unlawful processing and exercise effective redress'.¹⁴⁹⁴ The right to access and explanation is therefore a vital right to support the effective exercise of the other rights.

A broader right of explanation would address this gap. The GDPR and data protection laws in Canada, Singapore and California all require that individuals be provided with an explanation of how an entity uses, and to whom it discloses, personal information.¹⁴⁹⁵

Jurisdiction and law	Provision
EU/UK - <i>GDPR and UK GDPR</i>	<p>Article 15(1): Individuals have the right to confirm whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data and the following information:</p> <ul style="list-style-type: none"> (a) the purposes of the processing (b) the categories of personal data concerned (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, [including overseas transfers] ... (g) where the personal data are not collected from the data subject, any available information as to their source (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
Canada - <i>Personal Information Protection and Electronic Documents Act 2000</i>	<p>Principle 4.9.1 - Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.</p>
Japan - The Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2020)	<p>Article 27(2) - A personal information handling business operator shall, when requested by a principal to get informed of a utilization purpose of retained personal data that can identify the principal, inform the said principal thereof without delay...</p>

¹⁴⁹² Submission to the Discussion Paper: [Response 840424239](#), 3-4.

¹⁴⁹³ Submission to the Discussion Paper: [OAIC](#), 132.

¹⁴⁹⁴ Submission to the Discussion Paper: [European Commission](#), 4.

¹⁴⁹⁵ GDPR art 15; *Personal Information Protection and Electronic Documents Act 2000* (Canada) sch 1, Principle 9; *Personal Data Protection Act 2012* (Singapore) s 21; *Cal. Civ. Code* (California) § 1798.110.

Singapore - Personal Data Protection Act 2012	Section 21(1): ...on request of an individual, an organisation shall, as soon as reasonably possible, provide the individual with — a) personal data about the individual that is in the possession or under the control of the organisation; b) information about the ways in which the personal data referred to in paragraph (a) has been or may have been used or disclosed by the organisation within a year before the date of the request.
California - California Consumer Privacy Act of 2018	Cal. Civ. Code § 1798.110: (a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following: <ol style="list-style-type: none"> (1) The categories of personal information it has collected about that consumer. (2) The categories of sources from which the personal information is collected. (3) The business or commercial purpose for collecting or selling personal information. (4) The categories of third parties with whom the business shares personal information. (5) The specific pieces of personal information it has collected about that consumer.

New technologies and evolving uses of personal information make the need for an explanation all the more important. Individuals may not appreciate the capabilities of AI or assisted decision-making technologies, or how those technologies can be used to determine access to services. The importance of meaningful information about these new technologies to individuals whose personal information is used to make decisions which significantly affect them is discussed in detail in Chapter 19.

Adequacy of a response

Submitters expressed concern about how APP entities would respond to the proposed access requests.¹⁴⁹⁶ Telstra was concerned that a response could prove onerous and produce a product which would often be of limited utility to the individual.¹⁴⁹⁷ The Australian Privacy Foundation did not support proposal (3) in the Discussion Paper, arguing that it could provide a loophole for APP entities to comply by providing a lesser explanation in the place of access.¹⁴⁹⁸ illion submitted that the ability to consult on the manner in which information is supplied should not be limited and specificity should be encouraged in order to find the most efficient response available.¹⁴⁹⁹

The objective of responding to an access and explanation request would be to inform the individual as far as is reasonable about what is being done with their information. It should include sufficient detail to put the individual in a position to exercise other rights should they choose, or to furnish a complaint to the OAIC should they have concerns about the APP entity's compliance with the Act.

An explanation should inform the individual about what personal information is held and what the APP entity does with it rather than necessarily the substance of the information. For example, where the personal information may

¹⁴⁹⁶ See for example Submissions to the Discussion Paper: [Financial Rights Legal Centre and Financial Counselling Australia](#), 17; [Australian Privacy Foundation](#), 14; [Murdoch Children's Research Institute](#), 8.

¹⁴⁹⁷ Submission to the Discussion Paper: [Telstra](#), 3.

¹⁴⁹⁸ Submission to the Discussion Paper: [Australian Privacy Foundation](#), 14.

¹⁴⁹⁹ Submission to the Discussion Paper: [illion](#), 3.

require expertise to understand (e.g. medical information)¹⁵⁰⁰ then it may not be reasonable to explain the information as that should be done in a consultation with the individual's doctor. It may also not always be reasonable to provide an explanation of all technical data, because it may be unlikely to reduce operational costs while proving unhelpful by risking a misunderstanding between the individual and the entity.¹⁵⁰¹ Rather an explanation needs to suit its context. An APP entity should be required to explain with sufficient specificity in the circumstances what the information is and detail how it came to hold the information and what it is doing with it.

Charge for providing access and form of request

APP 12.7 provides that agencies must not charge for an access request and APP 12.8 provides that organisations must not charge individuals to make a request and any charge for responding to a request must 'not be excessive'. The Review does not propose agencies should be able to charge for responses, but has considered the appropriate charge for organisations.

Experian submitted that access plays an important role in engendering trust in the privacy protection framework, but it must be balanced against costs, time and resources which could outweigh the privacy benefits to consumers. It considered that a nominal cost could help deter unduly burdensome requests.¹⁵⁰² The Australian Privacy Foundation considered that the current ability for an organisation to impose a charge can act as a barrier to individuals exercising their right of access.¹⁵⁰³

The UK Government's recent consultation on the UK GDPR sought feedback on whether to introduce a nominal fee for the exercise of access requests under the UK Data Protection Act. In the 23 June 2022 response, the UK Government resolved not to introduce a nominal fee, referring to the potential to disadvantage vulnerable people in society and encouraging organisations to implement appropriate processes and infrastructure to respond to subject access requests.¹⁵⁰⁴

A lesser 'nominal fee' may be an improvement on the current charge which is 'not excessive'. Introducing a nominal charge for requests which require an organisation to incur some costs and produce a product may be appropriate.

These charges should be waived for vulnerable people. As with current charges, no fee should apply to the making of a request and fees should not apply where the response is merely a summary or explanation of activities in response to an ordinary inquiry. Consideration could be given to specifying the nominal fee in regulations.

The Australian Privacy Foundation submitted that lack of clarity about how an access request can be made can also act as a barrier to the operation of APP 12.¹⁵⁰⁵ The OAIC could provide a template for requests in their guidance and the process for making an access and explanation request should be set out clearly in an APP entity's Privacy Policy.

Specific exception for commercially sensitive decision-making processes

APP 12.3(j) has an exception to providing access where doing so 'would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process'. It is not proposed that this exemption would be removed. Calabash Solutions considered that this exception risks privacy harms if it is relied on to exclude providing access to inferred personal information.¹⁵⁰⁶ However, the proposal to include inferences in the definition of 'collection' in Chapter 4 should clarify that the right of access also applies to inferences. For example, personal information in the form of inferences generated through commercially sensitive algorithms would not be exempt from the right to access and explanation. This would include information used for decision-making by those algorithms and how the inferences were generated, even though the intellectual property in the computer code making up the algorithm itself would be excluded. Specific OAIC guidance on this issue may be beneficial given recent technological changes.

1500 Submissions to the Discussion Paper: [MIGA](#), 7; [Australian Medical Association](#), 14.

1501 Submission to the Discussion Paper: [Telstra](#), 22-23.

1502 Submission to the Discussion Paper: [Experian](#), 22.

1503 Submission to the Discussion Paper: [Australian Privacy Foundation](#), 14.

1504 Department for Digital, Media, Culture & Sport (UK), [Data: a new direction - government response to consultation](#) [23 June 2022].

1505 Submission to the Discussion Paper: [Australian Privacy Foundation](#), 14.

1506 Submission to the Discussion Paper: [Calabash Solutions](#), 20.

18.1 Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features:

- (a) an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act)**
- (b) an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual**
- (c) an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual**
- (d) the entity may consult with the individual about the format for responding to a request, and the format should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information**
- (e) an organisation may charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual.**

Note: exemptions to this right are set out below

Note: The right to an explanation in the context of automated decisions will be further enhanced through proposal 19.3, discussed in Chapter 19.

18.4 Right to object

The Discussion Paper proposed that an individual should be able to 'object or withdraw their consent at any time to the collection, use or disclosure of their personal information'. That proposal had two parts, withdrawal of consent and 'objection'. Withdrawal of consent is discussed in Chapter 11 in the context of consent. The right to object is discussed in this section.

The proposed right to object would be modelled on the corresponding right in the GDPR. The GDPR's right to object enables individuals to request that entities no longer process personal data in certain circumstances.¹⁵⁰⁷ 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'¹⁵⁰⁸ and the entity cannot demonstrate a 'compelling reason' to continue processing.¹⁵⁰⁹ 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.¹⁵¹⁰ Accordingly, outside of the context of direct marketing, it operates more like a right to question or challenge requiring the entity to justify their information handling practices.

The proposed right to object would operate in a similar way, in that it would give an individual the right to question or challenge an APP entity in relation to its handling of personal information against the requirements of the Act. It would require an APP entity to review its information-handling in light of the objection and provide a response to the objection. For example, an individual could challenge an entity that a particular collection is not reasonably necessary and/or not fair and reasonable. The APP entity would be required to satisfy itself that it *is* in all the circumstances, or

¹⁵⁰⁷ GDPR art 21.

¹⁵⁰⁸ Ibid art 6(1)(e)-(f).

¹⁵⁰⁹ UK ICO, [Right to Object](#) (Web Page, October 2022).

¹⁵¹⁰ Ibid.

change its practices. It would then need to provide a simple, understandable response to the individual about why it says the practice is compliant with the entity's obligations under the Act. The effect of a successful objection may be that the APP entity agrees to further minimise collection, collect a different type of information or modify the way in which it uses or discloses certain information. Alternatively, it could assist the individual to decide how it wishes to engage further with the entity, such as deciding not to use its services anymore, or to make a complaint to the OAIC. OAIC guidance, in particular guidance about the fair and reasonable test (discussed in Chapter 12), would assist APP entities in responding to an objection.

The Digital Law Association supported a right to object in principle but did not support the proposal in the Discussion Paper on the basis that an individual would not know what information is being used for what purpose, and therefore would not know to what they may need to object.¹⁵¹¹ The right to access and explanation would address this concern by providing the means by which an individual may obtain the information necessary to effectively exercise their right to object.

Salinger Privacy considered that the language of 'objection' would confuse both individuals and organisations as there was 'little point suggesting to individuals that they have a general right to 'object' to activities over which, in reality, they have little or no control'.¹⁵¹² However, the ordinary meaning of the word 'object' does not convey that an objection will always be accepted, and there is benefit in using similar language to that used for the comparable right under the GDPR.

18.4.1 Objection to data practices which are terms of service

Meta and the Business Council of Australia considered there needed to be an exception for where individuals provide their personal information in exchange for a service. These submitters were concerned that a right to object may force entities to alter their business models.¹⁵¹³

The Business Council of Australia submitted in the context of loyalty schemes that '[the] government cannot reasonably expect businesses to provide benefits to consumers if consumers cease to provide access to the personal information required to fuel insights and innovation to their continued benefit'.¹⁵¹⁴ The concern is that the right should not extend to an individual obtaining the benefit of a service while using an objection to avoid the personal information collection and advertising model which underpins the service. However, the proposed right to object would not enable individuals to require entities to do or not do something with their personal information. It would simply enable individuals to challenge how the entity is handling their personal information.

The submissions above illuminate the intersection of privacy and consumer laws in relation to entities' data handling practices. Where collection and use of an individual's personal information forms part of the bargain between a business and a consumer, the Australian Consumer Law applies to the entity's data handling practices. This overlap was considered in the Discussion Paper where it cited examples of business' data handling found to infringe the ACL.¹⁵¹⁵ However, the existence of a commercial arrangement does not exclude the entity's obligations under the Privacy Act including the proposal in Chapter 12 that to collect, use and disclose personal information it must be done fairly and reasonably.

18.2 Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons.

Note: general exemptions to this right are set out below

1511 Submission to the Discussion Paper: [Digital Law Association](#), 14-15.

1512 Submission to the Discussion Paper: [Salinger Privacy](#), 31.

1513 Submissions to the Discussion Paper: [Meta](#), 38; [Business Council of Australia](#), 2.

1514 Submission to the Discussion Paper: [Business Council of Australia](#), 8.

1515 [Discussion Paper](#), 212.

18.5 Right to erasure

The Discussion Paper proposed a right of erasure on a number of bases. These bases can be divided into circumstances which equate to a request that an APP entity comply immediately with existing obligations to destroy information (for example by court order or under APP 11.2), or where the request concerns information of a specific nature such as sensitive information or information about a child.

The Discussion Paper proposed a right to request erasure similar to that in the GDPR. The Discussion Paper referred to submissions that supported such a right to give individuals greater control over their information, place them in a stronger bargaining positioning relative to digital platforms and give real meaning to withdrawal of consent.¹⁵¹⁶ The ability to make an erasure request is already available under Australia's CDR¹⁵¹⁷ and My Health Record schemes.¹⁵¹⁸

Deloitte considered that an erasure right would be beneficial in giving greater control to individuals over their personal information and supporting organisations to improve retention and destruction practices.¹⁵¹⁹ Privacy 108 emphasised that a right to erasure could help address the power imbalance between individuals and the entities which hold their information.¹⁵²⁰

The UK Department for Culture, Media & Sport commissioned a report which sought to quantify the economic benefits arising from greater consumer trust and agency. The right to erasure was determined as having a range of benefits including ending harmful use of data, more accurate data and cost savings as part of the EU's GDPR rollout.¹⁵²¹ The Business Council of Australia on the other hand argued that the experience from the GDPR suggests that the costs of establishing appropriate processes and practices to facilitate erasure rights has been in excess of their utility for consumers.¹⁵²²

In the 2018 Deloitte UK report 'A new era for privacy - GDPR 6 months on', 12 per cent of surveyed consumers had used the right to erasure within the first 6 months of the law being introduced, with a further 18 per cent indicating that they may use this right in the future.¹⁵²³ A right to erasure may require APP entities to consider introducing or improving their data governance capabilities. However, Australian businesses could learn from the experience of businesses in the EU and thereby reduce the costs of establishing new systems. The upfront costs of establishing procedures would be balanced against a continuing dividend of consumer trust and agency.

Submitters to the Discussion Paper considered that the proposed right to erasure was broader than the GDPR model in the sense that it proposed a right for categories of information outright (sensitive information and children's information) rather than limiting it to where the entity can no longer lawfully process the information no matter its type.¹⁵²⁴ Submitters considered that an Australian right to erasure should be modelled on and interoperable with the GDPR version.¹⁵²⁵

In light of submitter feedback and other reforms in this Report, an Australian right to erasure should not be limited by reference to specific categories of information. Specific protections for sensitive information and children's information are proposed in Chapters 11 and 12. A right to erasure should be able to be exercised in relation to any information. However, the right would be limited to where the information should be destroyed for example by court order or under APP 11.2 as it is no longer needed.

In this respect, the right would effectively be an extension of APP 11.2 by requiring the entity to destroy the information upon request of the individual, rather than at the time the entity considers this is required. A right to erasure could be a complementary step to a successful challenge under the right to object or a withdrawal of consent. For example, if an individual discovered through the right to access and explanation that an entity has more information than the individual is comfortable with, the individual could decide to discontinue using that entity's services and ask the entity to delete their personal information as part of the right to erasure (as opposed to deletion in the ordinary course of the reasonable steps the entity would take to comply with APP 11.1).

1516 Submissions to the Issues Paper: [Australian Department of Health](#), 10; [CAIDE and MLS](#), 8; [Centre for Media Transition](#), 18–19; [Consumer Policy Research Centre](#), 9–10; [Oracle](#), 15. See also ACCC, [DPI Report](#), 471.

1517 [Competition and Consumer \(Consumer Data Right\) Rules 2020](#) (Cth) sub-div 4.3.4.

1518 [My Health Records Act 2012](#) (Cth) s 17(3) s 51.

1519 Submission to the Discussion Paper: [Deloitte Australia](#), 32.

1520 Submission to the Discussion Paper: [Privacy 108](#), 26–27.

1521 Submission to the Discussion Paper: [The Australia Institute - Centre for Responsible Technology](#), 9, referring to: London Economics (2017), [Research and analysis to quantify the benefits arising from personal data rights under the GDPR: Report to the Department for Culture, Media & Sport](#).

1522 Submission to the Discussion Paper: [Business Council of Australia](#), 8.

1523 Deloitte UK, [A new era for privacy - GDPR 6 months on](#), 2018, 14.

1524 Submission to the Discussion Paper: [BSA | The Software Alliance](#), 13; [SBS](#), 13.

1525 Submissions to the Discussion Paper: [BSA | The Software Alliance](#), 13; [DIGI](#), 20.

18.5.1 Specific law enforcement exception in the case of erasure

The right to erasure will need to be carefully considered in the context of the general exceptions set out at the end of this chapter. In particular a large number and broad range of submitters were concerned about how erasure might affect APP entities' activities in the public interest.¹⁵²⁶ There should be further engagement with stakeholders on the detail of exceptions prior to the legislative provisions being finalised.

The Australian Federal Police and the Victorian and Tasmanian Synod of the Uniting Church in Australia expressed particular concerns about the effect of the right to erasure for law enforcement and the potential for exploitation of the right to conceal criminal activity.¹⁵²⁷ The current law enforcement exception to access in 12.3(h) relies on a 'reason to suspect unlawful activity'. In the context of erasure, it is possible that there would be circumstances where there was, as yet, no reason to suspect unlawful activity at the time the right to erasure was exercised. Criminal actors may thereby be able to erase evidence of their activities before they come to the attention of a law enforcement body or before an APP entity has reason to suspect anything. The AFP submitted it is difficult for APP entities to know what might be required for law enforcement ahead of time. While training and guidance from law enforcement and the OAIC may assist in this regard, the AFP considered some types of personal information may warrant special treatment under any right to erasure, including:¹⁵²⁸

- joint personal information
- metadata
- financial records, and
- rental or property records.

The AFP suggested that these types of information could be quarantined rather than erased as an option to comply with the right.¹⁵²⁹ This approach has merit. Applying the right to erasure to require quarantine of information in the above categories would operate to ensure such information is available to law enforcement if required but would still restrict the entity's own use of the information. The quarantine exception would not be a requirement to retain information; entities would not need to hold information longer than they normally would in line with their normal destruction processes.

18.5.2 Response to an erasure request

Some submitters considered that de-identifying or quarantining information should be sufficient to 'erase' any type of information.¹⁵³⁰ Other submitters were concerned about being required to delete valuable de-identified data which they otherwise could continue to use.¹⁵³¹ The Australian Government Social Services Portfolio submission supported erasure where the data was no longer required for service delivery, provided it did not interfere with their ability to use de-identified datasets.¹⁵³²

The Shopping Centre Council of Australia was concerned about being required to identify an individual whose information has been de-identified in order to comply with an erasure request. This scenario may be counter to the policy rationale for the reform by increasing rather than decreasing held personal information.¹⁵³³

A right of erasure should not undermine other aspects of the regime established under the Act and therefore would not apply retrospectively to information that was already de-identified. However, if an erasure request were made where personal information had been de-identified, the entity would need to erase the personal information if the de-identified information was re-identified.

1526 See for example Submissions to the Discussion Paper: [ACCC](#), 11; [Office of the Information Commissioner Queensland](#), 3; [Murdoch Children's Research Institute](#), 7-8; [Privacy 108](#), 27; [Business Council of Australia](#), 8; [Digital Law Association](#), 15.

1527 Submissions to the Discussion Paper: [AFP](#), 3-4; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 6.

1528 Submission to the Discussion Paper: [AFP](#), 4.

1529 Ibid.

1530 Submissions to the Discussion Paper: [Australian Banking Association](#), 24; [Australian Information Industry Association](#), 4; [ABC](#), 9.

1531 Submissions to the Discussion Paper: [CSIRO](#), 11; [Insurance Council of Australia](#), 13; [ARCA](#), 12.

1532 Submission to the Discussion Paper: [Social Services Portfolio](#), 27-28.

1533 Submissions to the Discussion Paper: [Shopping Centre Council of Australia](#), 8.

The Fundraising Institute Australia and Public Fundraising Regulatory Association submitted that erasing personal information from databases would defeat the efforts to maintain accurate information on donor preferences, such that an individual's data may be collected again after they had requested erasure.¹⁵³⁴ An individual should therefore be presented with a choice. If the individual wants all their information erased, the APP entity should explain the consequences of that, including that their information may be collected again in the future. The APP entity could instead offer to keep the erasure request on record in the event their information was re-identified for any reason. However, if the individual does not want the entity to keep a record of them, the entity would need to ensure its security systems will protect the de-identified information from re-identification into the future. Security obligations on APP entities would also require them to ensure that bad actors do not abuse the system by making erasure requests and falsely claiming to be the individual concerned.¹⁵³⁵

18.5.3 Notifying third parties of an erasure request

The OAIC submitted the right to erasure should extend to information which is no longer 'held' by an entity in the sense that it should require the entity to notify others who may hold that personal information of the erasure request. Such an obligation would be similar to Article 19 of the GDPR which requires third party notification unless this proves impossible or involves disproportionate effort.¹⁵³⁶

A right to erasure should require third party notification, but this should be limited to where an APP entity has received personal information from a source other than the individual or an APP entity has disclosed personal information to another entity. In both cases, the APP entity has handled personal information in ways which warrant additional action in relation to an erasure request, unless that action is impossible or involves disproportionate effort.

18.3 Introduce a right to erasure with the following features:

- (a) An individual may seek to exercise the right to erasure for any of their personal information.**
- (b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.**
- (c) In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.**

Note: general exemptions to this right are set out below

18.6 Right to correction

APP 13 provides that where an individual requests correction of information, if the APP entity is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading having regard to a purpose for which the information is held, the entity must take reasonable steps to correct the information.

¹⁵³⁴ Submission to the Discussion Paper: [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 8. [Garvan Institute of Medical Research and Garvan Research Foundation](#), at 8, agreed with this submission.

¹⁵³⁵ Submission to the Discussion Paper: [OAIC](#), 144.

¹⁵³⁶ Ibid 143-144.

The Discussion Paper did not put forward any proposals in relation to APP 13, but asked whether generally available publications over which an APP entity has control should be required to be corrected under APP 13.¹⁵³⁷

The OAIC submitted that APP entities should be required to comply with APP 13 for personal information it has published online to provide individuals with greater control over their personal information and 'mitigate the risk of harm that may arise from incorrect information being widely available online'.¹⁵³⁸

The Australian Medical Association and the Association of Australian Medical Research Institutes were concerned about the impracticality of extending correction requests to information in published journals, including such information as author names or qualifications, especially where that data may now exist in multiple locations.¹⁵³⁹

APP entities do not 'hold' personal information under the Privacy Act unless the entity maintains possession and control of a 'record' containing the information. A 'record' does not include a 'generally available publication', which is defined in the Act as a publication which is generally available to members of the public. Prior to the age of the internet, it would have been very difficult to have any control over paper-based publications that had been made publicly available. However, today, many publications are available online. An entity which maintains a webpage can still have control over what is published on that webpage notwithstanding that it is available to members of the public. Misleading or inaccurate personal information online can cause harm to individuals and that information can be corrected by the entity in control of a website at its source.

However, there will be times where the public interest in freedom of expression or academic research does not favour a correction of an online publication.¹⁵⁴⁰ The entity would instead assess the request in light of the general public interest exceptions discussed later in this chapter.

18.4 Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control.

18.7 Right to de-index internet search results

The OAIC submitted that there would be substantial public interest in introducing a sub-category of erasure for the de-indexing of search results for indexed links that are 'inadequate, irrelevant or no longer relevant, or excessive'.¹⁵⁴¹ A number of other submitters agreed.¹⁵⁴²

This right already exists in the EU. The heading of 'Right to erasure' in Article 17 of the GDPR contains in brackets the words '(right to be forgotten)'. The 'Right to be Forgotten' arose out of the 2014 decision of the Court of Justice of the European Union in *Google Spain SL v Costeja González*¹⁵⁴³ as an extension of the rights in the predecessor privacy regulation to the GDPR (Directive 95/46). The test established by that case is that where a search is made on the basis of a person's name and links to webpages are presented in the search results, the webpages can be de-indexed from the results on that search 'because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine'.¹⁵⁴⁴ This applies even where the information on web pages is published lawfully by third parties and contains true information relating to the individual making the de-indexing request.¹⁵⁴⁵

¹⁵³⁷ [Discussion Paper](#), 143.

¹⁵³⁸ Submission to the Discussion Paper: [OAIC](#), 161.

¹⁵³⁹ Submissions to the Discussion Paper: [Australian Medical Association](#), 13; [AAMRI](#), 5.

¹⁵⁴⁰ Such as a newspaper article or academic journal.

¹⁵⁴¹ Submissions to the Discussion Paper: [OAIC](#), 138.

¹⁵⁴² Submissions to the Discussion Paper: [Privacy 108](#), 27; [NSW Council for Civil Liberties](#), 20-30; [UWA Law School Students: Sophie Archibald, Samantha Hopson, Sarah Jones, Gar-Hou Tran and Emma Young](#), 1;

¹⁵⁴³ Judgment of 13 May 2014, *Google Spain SL v Costeja González*, C-121/12, EU:C:2014:317.

¹⁵⁴⁴ *Google Spain SL v Costeja González*, at [94].

¹⁵⁴⁵ *Ibid.*

When a request is made to a search engine it is only the search result which is removed. The content remains at its source on the internet. The right regulates the ease of access to personal information through a search engine, not its removal from the internet.

Information on a search engine can be accessed within seconds of conducting a search of a person's name and that content may be embarrassing, harmful, inaccurate or irrelevant. In the absence of a right to de-index that material, individuals may be required to engage in costly and lengthy court action, most likely under defamation law, to control the information.¹⁵⁴⁶ The OAIC submitted that there was a strong case for a right to de-index, particularly where attempts to remove the information at its source is not feasible, such as where the source is offshore, anonymous or ignores takedown requests. Reporting on the right in the EU indicates that it is a relatively fast and cost-effective way for individuals to self-manage their personal information, with over 92 per cent of European de-indexing requests targeting personal or sensitive information resulting in successful de-indexation with a median time of 6 days.¹⁵⁴⁷

The OAIC submitted that the regulatory burden for search engines would be eased in Australia having regard to the existing systems established to comply with the right to be forgotten in Europe by the large search engines who will be affected.¹⁵⁴⁸

A right to de-index internet search results could be introduced on similar grounds as apply under the GDPR. That is, information which is excessive in volume (revealing too much about an individual), inaccurate, out-of-date in light of the time that has elapsed, incomplete, irrelevant (i.e. not relating to the person but potentially capable of impacting the person's reputation by association), or misleading. This test would reflect the test in *Google Spain SL v Costeja González*¹⁵⁴⁹ adapted for the Act.¹⁵⁵⁰ This test would capture information such as criminal charges when the individual was a minor, or historical media reports which do not represent the current circumstances of the individual.¹⁵⁵¹ Such a right would extend to all sensitive information and all information about a child unless an exception applies having regard to the special sensitivities of these types of information. The information should specifically apply to excessive information, meaning information which would reveal too much about an individual in all the circumstances, such as all their personal details or identification documents. The same exceptions to the other rights of the individual would apply to a right to de-index search results.

18.7.1 Volume of requests

Google publishes online a constantly updated Transparency Report of the requests made to delist content under EU Privacy law. Since *Google Spain*, Google has received over 1.32 million requests to delist over 5.16 million URLs. As at December 2022, Google had delisted just under 50 per cent of URLs requested.¹⁵⁵² Google's reasons for not delisting may include the existence of alternative solutions, technical reasons, or duplicate URLs. Google does not delist information which is 'strongly in the public interest' including when relating to professional life, past crime, political office, public life, self-authored content, government documents, or journalism.¹⁵⁵³

When first implemented, the right to be forgotten resulted in an initial burst of URL removal requests of over 100,000 per month for the first three months in 2014 which ultimately settled to around 47,000 per month from 2015 to 2019.¹⁵⁵⁴

Google is the overwhelmingly dominant search engine in Australia.¹⁵⁵⁵ Using the UK as a comparator¹⁵⁵⁶ and adjusting for population size,¹⁵⁵⁷ the Review estimates from Google's figures that Australia would have been responsible for at least 58,000 requests to de-list over 250,000 URLs in the eight-year period 2014 to 2022.

¹⁵⁴⁶ Submission to the Discussion Paper: [OAIC](#), 138.

¹⁵⁴⁷ *Ibid* 139.

¹⁵⁴⁸ *Ibid* 138.

¹⁵⁴⁹ Judgment of 13 May 2014, *Google Spain SL v Costeja González*, C-121/12, EU:C:2014:317.

¹⁵⁵⁰ The change in the language is for consistency with similar existing wording in APP 13 (Right to Correction).

¹⁵⁵¹ Such as the circumstances of Mr Costeja González in *Google Spain SL v Costeja González*, C-121/12, EU:C:2014:317.

¹⁵⁵² Google, *Transparency Report*, '[Requests to delist content under European privacy law](#)' (Web Page, 14 December 2022).

¹⁵⁵³ Google, *Transparency Report Help Centre*, '[European privacy requests Search removals FAQs: What are some common scenarios where you do not delist pages?](#)' (Web Page, 2022).

¹⁵⁵⁴ Bertram, Theo et al. (Google, Inc.), '[Five Years of the Right to be Forgotten](#)', 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), November 11–15, 2019, London, United Kingdom, (New York, 2019) 5.

¹⁵⁵⁵ ACCC, [DPI Report](#), 95.

¹⁵⁵⁶ Google, *Transparency Report*, '[Requests to delist content under European privacy law](#)' (Web Page, 14 December 2022).

¹⁵⁵⁷ Using Australia Bureau of Statistics for Australia's population as at 31 March 2022 : <https://www.abs.gov.au/>; and World Bank data for the United Kingdom: <https://data.worldbank.org/indicator/SP.POP.TOTL?locations=GB>.

18.7.2 Responsibility for adjudicating requests

Google expressed concerns that the right to be forgotten in the EU requires it to answer complex, important questions about whether there is public interest in information remaining available in search results and balancing personal privacy against publishing rights.¹⁵⁵⁸ Google submitted that these complex decisions should be made by an appropriate and independent judicial or regulatory authority that is in a better position to assess the broader context of the right.¹⁵⁵⁹

Requiring the OAIC to assess all de-listing requests would be an unacceptable burden on public funds. Instead, the search engine could assess a request, and where complex public interest questions were involved, the search engine could refer the request to the OAIC for assessment on a fee-for-service basis. The OAIC should be able to refuse a referral if it considers that the request does not raise issues requiring assessment by the OAIC. OAIC guidance on factors relevant to the public interest general exception to the rights considered further below would assist Google and other search engines respond to requests to de-list search results. Inevitably, the OAIC will require further resources to provide guidance and assist individuals who exercise this right.

18.7.3 Jurisdictional limits

Deloitte Australia noted that the 2019 decision of the *Google LLP v CNIL* introduced a jurisdictional limit on the scope of the right to erasure for search engines within Europe.¹⁵⁶⁰ This means that the right cannot be used to de-index search results on all of a search engine's domain name extensions, but only those which are associated with a European jurisdiction (e.g. google.fr), notwithstanding that an Australian domain (google.com.au) or American domain (google.com) can be accessed from European territory.¹⁵⁶¹ It is desirable to avoid any confusion about jurisdictional limits at the outset.¹⁵⁶²

The court in *Google LLC v CNIL* considered that a search engine should use measures which 'effectively prevent or, at the very least, seriously discourage an internet user' within the EU gaining access to search results on other domains not subject to de-indexing of offending search results.¹⁵⁶³ This means a search engine must take measures to discourage searches which defeat de-indexing. Such measures may include making parallel de-indexing available under the GDPR and Australian law and defaulting a search engine to the local country domain. Google already adopts the latter measure.

18.5 Introduce a right to de-index online search results containing personal information which is:

- i. sensitive information [e.g. medical history]
- ii. information about a child
- iii. excessively detailed [e.g. home address and personal phone number]
- iv. inaccurate, out-of-date, incomplete, irrelevant, or misleading

The search engine may refer a suitable request to the OAIC for a fee.

The right should be jurisdictionally limited to Australia.

¹⁵⁵⁸ Submission to the Issues Paper: [Google](#), 9.

¹⁵⁵⁹ *Ibid*, 10.

¹⁵⁶⁰ Submission to the Discussion Paper: [Deloitte Australia](#), 35. Judgment of 24 September 2019, *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, EU:C:2019:772.

¹⁵⁶¹ *Google LLC v CNIL*, at [37] and [73].

¹⁵⁶² Submission to the Discussion Paper: [Deloitte Australia](#), 35.

¹⁵⁶³ *Google LLC v CNIL*, at [73].

18.8 General exceptions to the rights of the individual

All the rights of the individual should be subject to exceptions which may be categorised as falling under one of the following three general exceptions:¹⁵⁶⁴

1. Competing public interests
2. Required or authorised by law and legal relationships
3. Technically infeasible or abuse of process

Common general exceptions are features of overseas jurisdictions with multiple rights. The GDPR contains general exceptions for the right to erasure with more specific exceptions otherwise left to national legislation.¹⁵⁶⁵ The UK lists exceptions to GDPR Rights in the Schedules to the UK Data Protection Act. The majority of these exceptions, such as freedom of expression,¹⁵⁶⁶ research,¹⁵⁶⁷ and health data,¹⁵⁶⁸ are expressed to apply to all rights. Within these exceptions, there are some specific sub-exceptions, for example 'serious harm' in the case of health data for the right of access.¹⁵⁶⁹ General exceptions with specific sub-exceptions relevant to specific rights where appropriate could be adopted in the Act, subject to further consultation on the precise content of each general exception.

18.8.1 Exceptions for competing public interests

Exceptions to the rights of the individual where there are competing public interests would apply where the public interest in a particular activity outweighed the public interest in protecting privacy. In such cases, the rights should be proportionately limited in scope. An evaluative exercise would be required when balancing the interests. Rights should always continue to operate to the extent the balancing does not weigh against it.¹⁵⁷⁰

Freedom of expression

Submitters were concerned that the right to erasure could have negative impacts on the freedom of expression.¹⁵⁷¹ There was a fear that the right to erasure could be used to censor or control information contrary to the public interest in freedom of expression. The Discussion Paper considered that an exception to the right to erasure could be modelled on the public interest test in the FOI Act with factors that could guide decisions about what was in the public interest:¹⁵⁷²

- promotion of the objects of the Act
- informing the public, or enabling debate on a matter of public importance
- constituting an unreasonable limitation on the expression of a legitimate view or opinion, or
- inhibiting the handling of personal information for archival, research or statistical purposes, journalistic purposes; or for academic, artistic or literary expression in the public interest.

The OAIC's submission agreed with this approach, and considered an evaluative exercise could be informed by OAIC guidance.¹⁵⁷³ While most valuable for the right to erasure, an exception for freedom of expression based on the FOI Act test could be recognised as part of a public interest exception which could potentially apply to other rights, if relevant.¹⁵⁷⁴

¹⁵⁶⁴ See for example Submissions to the Discussion Paper: [Office of the Information Commissioner Queensland](#), 3.; [SBS](#), 14; [NSW Council for Civil Liberties](#), 4.

¹⁵⁶⁵ See EU GDPR art 23.

¹⁵⁶⁶ *Data Protection Act 2018* (UK) (DPA) sch 2, Pt 5

¹⁵⁶⁷ *Ibid* sch 2, Pt 6

¹⁵⁶⁸ *Ibid* sch 3, Pt 2

¹⁵⁶⁹ *Ibid* sch 3, Pt 2, para 5.

¹⁵⁷⁰ This is the reverse of how the balancing act would work in the ALRC Report 123 statutory tort model. In the statutory tort discussed in Chapter 27, unless the balancing exercise favours privacy, the cause of action would not be made out.

¹⁵⁷¹ Submissions to the Discussion Paper: [NSW Council for Civil Liberties](#), 29; [Meta](#), 40; [Privacy 108](#), 27; [elevenM](#), 44; [ABC](#), 9.

¹⁵⁷² [Discussion Paper](#), 121.

¹⁵⁷³ Submission to the Discussion Paper: [OAIC](#), 141-142.

¹⁵⁷⁴ For example, there may be freedom of expression dimensions to the rights to correction (not correcting an article as it is a public record), objection (the objected to activity serves the public interest in the context of the fair and reasonable test), or the right to de-list.

Law enforcement

The public interest in law enforcement is recognised as an exception to the current right of access. That exception applies where an entity has reason to suspect that unlawful activity, or misconduct of a serious nature, has been, is being or may be engaged in, and giving access would likely prejudice the taking of appropriate action, or access would prejudice enforcement by enforcement bodies.¹⁵⁷⁵ Submitters considered that law enforcement exceptions should apply to erasure,¹⁵⁷⁶ and the OAIC considered it should apply to both erasure and objection.¹⁵⁷⁷ A law enforcement exception modelled on the current exception for access could be adopted as a general exceptions where compliance would impact law enforcement.

Health services, research and national security

Submitters were concerned that the exercise of the rights to object and to erasure could impact the delivery of health care and research.¹⁵⁷⁸ The OAIC considered that the right to object should have clear exceptions, including where objection would inhibit the handling of personal information for archival, research or statistical purposes. It considered that a narrow interpretation of public interest should be adopted to prevent APP entities from rejecting objections on the basis of their own commercial research and statistical purposes.¹⁵⁷⁹

The Act currently recognises exceptions to certain requirements in the Act for collection, use and disclosure of information in some health care situations¹⁵⁸⁰ and human-based research.¹⁵⁸¹ Having regard to the public interest in effective and informed health care and research, consideration should be given to applying health care and research exceptions to the rights of the individual.

The Act also currently recognises certain 'permitted general situations' which cover circumstances relating to national security and missing persons. These circumstances should remain exempt from the rights of the individual.¹⁵⁸²

18.8.2 Required or authorised by law and legal relationships

Where required or authorised by law, or compliance would be unlawful

Submitters were concerned about situations where the exercise of a right could be contrary to law, or could conflict with collection, use, disclosure, or retention of information which is required or authorised by law.¹⁵⁸³ The rights of the individual should not displace other regulatory regimes. For example, the rights should not displace obligations such as those in the *Archives Act 1983* (Cth) for Commonwealth records,¹⁵⁸⁴ the *Corporations Act 2001* (Cth) for business records,¹⁵⁸⁵ or the *Telecommunications (Interception and Access) Amendment (Data Retention) Act* (Cth)¹⁵⁸⁶ for specific data. This exception would also operate to ensure compliance with current or reasonably anticipated orders of a court or tribunal or other competent authority with power to require documents or information.¹⁵⁸⁷

Legal relationships and legal and related proceedings

Many submitters were concerned about erasure in the context of the performance of a contract.¹⁵⁸⁸ Information required to perform contractual or other like obligations should be able to be retained and those activities continued unless the exercise of the right in effect seeks to terminate the contract or legal relations. In either case, the rights of erasure or objection could operate to require that only strictly necessary information be retained.

¹⁵⁷⁵ APP 12.3(h) and (i). There is also a law enforcement exception in s 16A which creates a 'permitted general situation' which duplicates APP 12.3(h).

¹⁵⁷⁶ Submissions to the Discussion Paper: [Services Australia](#), 10; [NSW Council for Civil Liberties](#), 29; [Optus](#), 24-25; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 7.

¹⁵⁷⁷ Submission to the Discussion Paper: [OAIC](#), 131, 140-141.

¹⁵⁷⁸ Submissions to the Discussion Paper: [Garvan Institute of Medical Research and Garvan Research Foundation](#), 5, 8; [Murdoch Children's Research Institute](#), 7-8; [Ramsay Health Care Australia](#), 8; [CSIRO](#), 11; [Avant Mutual](#), 13.

¹⁵⁷⁹ Submission to the Discussion Paper: [OAIC](#), 131. See also Submissions to the Discussion Paper: [NSW Council for Civil Liberties](#), 28-29; [Privacy 108](#), 27. Privacy 108 proposed erasure be subject to a successful right to object for public interest reasons; [elevenM](#), 44.

¹⁵⁸⁰ See 'permitted health situations' in s 16B of the Privacy Act.

¹⁵⁸¹ See s 95A, s 16B(2), and s 16B(3) of the Privacy Act.

¹⁵⁸² Submission to the Discussion Paper: [Meta](#), 38; [Optus](#), 25.

¹⁵⁸³ See for example Submissions to the Discussion Paper: [Australian Banking Association](#), 24; [Financial Services Council](#), 9; [National Australia Bank](#), 5.

¹⁵⁸⁴ Submissions to the Discussion Paper: [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 7; [SBS](#), 14; [National Archives of Australia](#), 3-4.

¹⁵⁸⁵ Submission to the Discussion Paper: [Financial Services Council](#), 9.

¹⁵⁸⁶ Submission to the Discussion Paper: [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 8; [Optus](#), 24-25.

¹⁵⁸⁷ Submissions to the Discussion Paper: [Optus](#), 25; [Australian Banking Association](#), 23; [SBS](#), 14; [Social Services Portfolio](#), 28.

¹⁵⁸⁸ See for example Submissions to the Discussion Paper: [SBS](#), 14; [Australian Banking Association](#), 23, 24; [Insurance Council of Australia](#), 12-13; [MIGA](#), 6.

The right to access contains an exception for ‘information [which] relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings’.¹⁵⁸⁹ The rights of the individual should not be exercised so as to interfere with legal processes.

To address concerns about the potential for access rights to undermine the integrity of external dispute resolution schemes, the Discussion Paper proposed an additional exception to allow an organisation to refuse a request for information relating to EDR services where giving access would prejudice a dispute resolution process.¹⁵⁹⁰ Similar access exceptions are recognised in overseas privacy laws, such as Singapore’s *Personal Data Protection Act 2012*.¹⁵⁹¹

18.8.3 Technically infeasible or abuse of process

Technically impossible or infeasible

The Discussion Paper proposed an exception to the right to erasure where it would be ‘technically impractical or impossible’. It also proposed a similar exception in the context of extending the right to access ‘unless it would be impossible or would involve disproportionate effort’.¹⁵⁹² There would be situations where actioning a request for access or erasure would be impossible due to technical limitations in how the information is held or used, or would be unreasonable having regard to the nature of the request and the information involved.

Many submitters supported exceptions for technical limitations.¹⁵⁹³ However, Deloitte Australia submitted that any technically impossible or infeasible exceptions would need to be carefully drafted to ensure that organisations do not design systems to take advantage of the exception.¹⁵⁹⁴ The OAIC considered that the technical impracticality exception in the context of erasure would be part of the reasonableness threshold for a response (discussed further below).¹⁵⁹⁵

Frivolous or vexatious requests

Many submitters were concerned about the cost to APP entities of responding to frivolous or vexatious requests and submitted there should be a corresponding exception.¹⁵⁹⁶ An exception for such requests already exists in relation to access. It is appropriate that such an exception be extended to all rights of the individual.

18.6 Introduce relevant exceptions to all rights of the individual based on the following categories:

- (a) **Competing public interests:** such as where complying with a request would be contrary to public interests, including freedom of expression and law enforcement activities.
- (b) **Relationships with a legal character:** such as where complying with the request would be inconsistent with another law or a contract with the individual.
- (c) **Technical exceptions:** such as where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request.

¹⁵⁸⁹ APP 12.3(d)

¹⁵⁹⁰ [Discussion Paper](#), 142.

¹⁵⁹¹ *Personal Data Protection Act 2012* (Singapore) s 21.

¹⁵⁹² [Discussion Paper](#), 119, 141.

¹⁵⁹³ Submissions to the Discussion Paper: [Federal Chamber of Automotive Industries](#), 24-25; [Optus](#), 24; [Shopping Centre Council of Australia](#), 8; [Microsoft](#), 8; [Meta](#), 40.

¹⁵⁹⁴ Submissions to the Discussion Paper: [Deloitte Australia](#), 35.

¹⁵⁹⁵ Submission to the Discussion Paper: [OAIC](#), 140.

¹⁵⁹⁶ Submissions to the Discussion Paper: [SBS](#), 15; [Optus](#), 23, 25; [Federal Chamber of Automotive Industries](#), 25; [Uniting Church in Australia](#), [Synod of Victoria and Tasmania](#), 8; [OAIC](#), 132, 142.

18.9 Compliance with the rights of the individual

Feedback on the Discussion Paper highlighted the need for APP entities to work with individuals to ensure the effective exercise of their rights. This section proposes a number of principles to assist entities in complying with the rights set out in this chapter, so that individuals are made aware of their rights and how they may be exercised, how an APP entity engages with an individual who has requested to exercise a right, the steps required to respond to a request, and the timeframe for a response.

18.9.1 Informing individuals about their rights

The OAIC recommended that APP entities be required to notify individuals of their ability to request erasure and the right to object.¹⁵⁹⁷ CPA Australia agreed that APP entities should be required to notify individuals of their rights to withdraw consent, where consent is obtained.¹⁵⁹⁸

Entities are currently required to notify individuals at the point of collection that the privacy policy of the APP entity contains information on how to access and seek correction of their personal information. It would be appropriate to extend that obligation to all the rights of the individual. Privacy policies should include relevant information on its procedures for responding to the rights of the individual.

18.7 Individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them.

Privacy policies should set out the APP entity's procedures for responding to the rights of the individual.

18.9.2 Obligation of reasonable assistance

In relation to access requests, the Discussion Paper proposed that APP entities be able to consult with an individual to provide access to the requested information in an alternative manner.¹⁵⁹⁹ This proposal responded to concerns about how to effectively respond to an access request for personal information that is technical in nature and which could result in the provision of information that is incomprehensible to an ordinary person.

The NSW Council for Civil Liberties submitted that a response must meet the needs of both parties and flexibility should not be a way for the APP entity to sidestep responsibilities.¹⁶⁰⁰ elevenM supported measures to enable open dialogue between entities and individuals, including a requirement to help customers understand the nature of the personal information the business holds about them.¹⁶⁰¹ Experian Australia submitted that there should be a mechanism in the right to access for quickly addressing concerns to avoid complaints and clear guidance as to what data needs to be provided or reviewed.¹⁶⁰²

illion submitted the ability for the APP entity to consult with the individual concerned should not be limited to the manner in which the information is supplied but also the specifics of what is required to ensure a more efficient response is available.¹⁶⁰³ Google strongly supported the opportunity for an entity to inform the individual of the consequences of their objection, and flexibility that allows time for entities to respond and for individuals to consider

¹⁵⁹⁷ Submission to the Discussion Paper: [OAIC](#), 132-133.

¹⁵⁹⁸ Submission to the Discussion Paper: [CPA Australia](#), 4.

¹⁵⁹⁹ [Discussion Paper](#), proposal 18.3, 143.

¹⁶⁰⁰ Submission to the Discussion Paper: [NSW Council for Civil Liberties](#), 34.

¹⁶⁰¹ Submission to the Discussion Paper: [elevenM](#), 52.

¹⁶⁰² Submissions to the Discussion Paper: [Experian Australia](#), 22.

¹⁶⁰³ Submissions to the Discussion Paper: [illion](#), 3.

that response before the exercise of their right is confirmed.¹⁶⁰⁴ The OAIC also agreed with this proposal.¹⁶⁰⁵ The Australian Department of Health was also broadly supportive of measures aimed at providing APP entities with a greater degree of flexibility when responding to access requests.¹⁶⁰⁶ Experian Australia noted that subject access requests make up the majority of complaints made to the ICO in the UK and appear to frequently arise due to a mismatch of expectations and practice; individuals may have an expectation that an access request will yield a larger amount of information than that which appear in the organisation's response.¹⁶⁰⁷

The OAIC submitted that there should be an obligation on APP entities to assist individuals to exercise their rights or to give effect to requests in a more limited way rather than outright rejecting the exercise of the right. An overly broad objection may lock an individual out of receiving products or services they would like to receive instead of objecting to a specific practice or aspect of the service.¹⁶⁰⁸ The OAIC recommended a requirement modelled on existing FOI requirements to provide 'reasonable assistance' to individuals to reframe their request and provide them with a reasonable opportunity to revise a request, before the request is refused.¹⁶⁰⁹

An obligation on APP entities to provide reasonable assistance to individuals to exercise their rights would address the imbalance in understanding between the APP entity and the individual, whilst facilitating the relationship between the parties. For example, an individual could object to a particular use which arises from the way in which the individual engages with a service, and rather than ceasing the relationship, the APP entity could erase one set of information but assist the individual to re-engage with the service on a different, mutually agreed basis. Reasonable assistance would enable the individual to exercise their rights, without a technical or legalistic approach to the wording of a request, which may not be in the interests of either party.

18.8 An APP entity must provide *reasonable assistance* to individuals to assist in the exercise of their rights under the Act.

18.9.3 Reasonable steps to respond

The proposed right to object in the Discussion Paper envisaged a requirement to take reasonable steps to comply, similar to the requirement which applies to a correction request under APP 13.

Microsoft encouraged flexibility for APP entities in responding to requests, including, if appropriate, self-service portals for access rights.¹⁶¹⁰ Reasonable steps does not always mean more work or detail. The Uniting Church expressed concerns that refusing a right of the individual on the basis of suspicion of criminal activity may 'tip off' the individual suspected of a crime if the APP entity was required to provide an explanation.¹⁶¹¹ Such a response may not be reasonable. Retail Drinks Australia submitted that the rights of the individual should not overburden business with administrative requirements when responding to requests for the deletion of trivial data such that the burden of the inconvenience, time and cost of meeting that obligation would be excessive compared with the relevant impact to an individual's privacy.¹⁶¹²

The steps an APP entity takes in responding to the exercise of a right should be governed by what is reasonable having regard to all the circumstances, consistent with existing reasonableness tests in the APPs and the CDR. The OAIC thought the following considerations for a reasonable steps test for the right of erasure could be included in guidance:¹⁶¹³

- the amount of personal information – more rigorous steps may be required as the quantity of information increases
- the possible adverse consequences for an individual if their personal information is not properly deleted – more rigorous steps may be required as the risk of adversity increases

¹⁶⁰⁴ Submission to the Discussion Paper: [Google](#), 4.

¹⁶⁰⁵ Submission to the Discussion Paper: [OAIC](#), 14.24

¹⁶⁰⁶ Submission to the Discussion Paper: [Australian Department of Health](#), 14.

¹⁶⁰⁷ Submission to the Discussion Paper: [Experian Australia](#), 22.

¹⁶⁰⁸ Submission to the Discussion Paper: [OAIC](#), 133.

¹⁶⁰⁹ Ibid.

¹⁶¹⁰ Submission to the Discussion Paper: [Microsoft](#), 8.

¹⁶¹¹ Submission to the Discussion Paper: [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 6.

¹⁶¹² Submission to the Discussion Paper: [Retail Drinks Australia](#), 9.

¹⁶¹³ Submission to the Discussion Paper: [OAIC](#), 139-140.

- the practicality, including time and cost involved – although an APP entity would not be excused from deleting personal information by reason only that it would be inconvenient, time-consuming or impose some cost to do so.
- the technical capabilities of an APP entity
- a proportionality test that measures whether the burden or expense of erasure would be disproportionate to the risks to the consumer's privacy or community expectations in each case.

The OAIC considered the reasonable steps tests would be supported by an APP entity's obligation under APP 1 to implement practices, procedures and processes to give effect to the rights of the individual.¹⁶¹⁴ The OAIC also considered a 'reasonable steps' test was the appropriate test for the right to object.¹⁶¹⁵

If introduced, the controller-processor distinction would determine which entity was the controller with the obligation to respond to the exercise of the rights of the individual (see Chapter 22). The Discussion Paper proposal to make this distinction received support from submitters.¹⁶¹⁶ Where a request was made to a processor, it should be referred to the controller and the individual informed that the controller is responsible for responding.

Restriction in use pending determination of a request

Article 18 of the GDPR contains a right to restriction of processing while an individual right, such as an objection, is being considered. As the Discussion Paper did not make any proposal in relation to restricting use or disclosure of information after the exercise of a right, most submitters did not address this issue.

However, Avant Mutual expressed concern about any requirement to cease using, collecting or disclosing personal information while considering an objection on the basis that it would be onerous and unworkable in the healthcare context where continued collection and disclosure may be required for ongoing care.¹⁶¹⁷ Restriction in use following the exercise of a right should be addressed as part of the reasonable steps an APP entity must take. In some circumstances (especially if the individual has requested it) the reasonable steps test may entail restricting use or disclosure while the request is considered.

Compliance for legacy datasets

Some submitters were concerned about information collected in legacy datasets which were not designed with the rights of the individual in mind and may make compliance difficult and costly, or impossible.

Deloitte Australia submitted that legacy IT operations may not be capable of supporting the erasure of specific data points from backups and that development of specifically defined requirements to assist organisations would be beneficial.¹⁶¹⁸ Retail Drinks Australia submitted that the workload required to identify, map, and then develop internal processes for the rights of the individual would be a significant multi-year process for larger organisations with large legacy, or decentralised approaches to datasets. Retail Drinks Australia recommended a grace period of at least two years to comply.¹⁶¹⁹

The National Australia Bank submitted that the practice of 'putting the data beyond use' should be sufficient to satisfy an erasure request.¹⁶²⁰ UK ICO guidance includes in certain contexts permitting back-up data which cannot otherwise be erased being put 'beyond use' such that it is no longer accessed and is replaced in due course in line with an established schedule.¹⁶²¹

Legacy IT systems of many APP entities may not be designed with privacy in mind. It may therefore be appropriate to have a suitable implementation period before these obligations commence.

No application to de-identified or aggregated data

Shopping Centre Council of Australia sought guidance on how a right to erasure would apply to aggregated de-identified data given that an individual would need to be re-identified to comply with the right. Re-identification could expose the individual to new privacy risks and would impose financial costs on the entity.¹⁶²² Experian expressed similar concerns.¹⁶²³ The Australian Banking Association submitted that individual rights should not apply to information to the extent it has been de-identified.¹⁶²⁴

¹⁶¹⁴ Submission to the Discussion Paper: [OAIC](#), 140.

¹⁶¹⁵ Ibid, 130-131.

¹⁶¹⁶ Submissions to the Discussion Paper: [Telstra](#), 4; [BSA | The Software Alliance](#), 13; [ACT | The App Association](#); 4-5 [Australian Information Industry Association](#), 4.

¹⁶¹⁷ Submission to the Discussion Paper: [Avant Mutual](#), 12-13.

¹⁶¹⁸ Submission to the Discussion Paper: [Deloitte Australia](#), 36.

¹⁶¹⁹ Submission to the Discussion Paper: [Retail Drinks Australia](#), 8.

¹⁶²⁰ Submission to the Discussion Paper: [National Australia Bank](#), 5.

¹⁶²¹ UK ICO, guidance, 'Right to Erasure', ['Do we have to erase personal data from backup systems?' \(Web Page\)](#).

¹⁶²² Submission to the Discussion Paper: [Shopping Centre Council of Australia](#), 8.

¹⁶²³ Submission to the Discussion Paper: [Experian Australia](#), 17.

¹⁶²⁴ Submission to the Discussion Paper: [Australian Banking Association](#), 24.

As discussed in Chapter 4, deidentified information should attract certain protections under the Act but it is not considered that the rights of the individual should apply to such information. However, having regard to the contextual nature of de-identification, APP entities would need to take care to ensure that if de-identified information is re-identified following an erasure request or an objection, that the security systems they have in place are sufficient to prevent re-identification into the future, or that the request is actioned at such time.

No fee to exercise the rights

Experian submitted that organisations should be entitled to charge for reasonable costs of responding to erasure requests. It cited costs incurred by an entity to verify a requester's identity to prevent fraud in the exercise of the right.¹⁶²⁵ However, other than where an organisation is required to undertake work and produce 'a product' in response to a request for access and explanation, individuals should not be charged to exercise any of the rights of the individual.

18.9 An APP entity must take reasonable steps to respond to an exercise of a right of the individual. Refusal of a request should be accompanied by an explanation for the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC.

18.9.4 Timeframes for responding

Submitters generally agreed that a response to the exercise of a right must be within a reasonable period.¹⁶²⁶ Some submitters preferred a base time period of one month.¹⁶²⁷ The National Australia Bank suggested 90 days.¹⁶²⁸

Under the existing rights to access and request the correction of personal information, an agency must respond to the request within 30 days after the request is made, or if the entity is an organisation, within a reasonable period after the request is made. The Act recognises that a one-size fits all timeframe may not be appropriate for all organisations, but the explanatory memorandum explained that a reasonable period will not usually exceed 30 days.¹⁶²⁹

The OAIC and elevenM preferred that the current formulation for timeframes in APP 12, with a distinction between agencies and organisations, should apply to the rights to erasure and objection.¹⁶³⁰ The Australian Banking Association supported a response within a reasonable period having regard to the complexity of the request, the volume and sensitivity of the information, and the extent to which an APP entity must work with other entities.¹⁶³¹

Deloitte Australia submitted that, based on its survey of organisations across 11 countries (including Australia), only 30 per cent of entities were able to respond to data subject requests received within one month and 37 per cent were either unable to keep up with the volume or only able to respond to a few within one month.¹⁶³² Financial Rights Legal Centre and Financial Counselling Australia researched the privacy practices of general insurers and found that most participants received a response to an APP 12 access request fairly quickly, but others experienced delays of over one month to over three months. Some individuals did not receive confirmation of their requests and others experienced delay in receiving confirmation.¹⁶³³

This Report recommends APP entities be required to acknowledge receipt of a request to exercise a right within a reasonable time after the request is made. In line with submissions, an agency should respond to the request within 30 days of the request being made. However, an agency may respond in a longer timeframe provided they can justify

¹⁶²⁵ Submission to the Discussion Paper: [Experian Australia](#), 17.

¹⁶²⁶ See for example Submissions to the Discussion Paper: [NSW Council for Civil Liberties](#), 30; [Australian Banking Association](#), 25; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 6; [OAIC](#), 134, 143; [Retail Drinks Australia](#), 9.

¹⁶²⁷ Submissions to the Discussion Paper: [OAIC](#), 134; [Privacy 108](#), 28; [elevenM](#), 45.

¹⁶²⁸ Submission to the Discussion Paper: [National Australia Bank](#), 5.

¹⁶²⁹ Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 87.

¹⁶³⁰ Submissions to the Discussion Paper: [elevenM](#), 45; [OAIC](#), 133, 143;

¹⁶³¹ Submission to the Discussion Paper: [Australian Banking Association](#), 25.

¹⁶³² Submission to the Discussion Paper: [Deloitte Australia](#), 34.

¹⁶³³ Submission to the Discussion Paper: [Financial Rights Legal Centre and Financial Counselling Australia](#), 18.

this is necessary and reasonable. This is to reflect that the proposed new rights might take longer to process than the existing access and correction rights. An organisation should respond within a reasonable period. Entities should communicate this timeframe to the individual when they acknowledge receipt of the request.

18.10 An organisation must acknowledge receipt of a request to exercise a right of the Individual within a reasonable time and provide a timeframe for responding.

An agency and organisation must respond to a request to exercise a right within a reasonable timeframe. In the case of an agency, the default position should be that a reasonable timeframe is within 30 days, unless a longer period can be justified.

19. Automated decision-making

The safe and responsible development and deployment of new and emerging technologies, including ADM, presents significant opportunities for enhancing productivity and facilitating economic growth, and improving outcomes for Australians across health, environment, defence and national security.¹⁶³⁴ While the Act does not expressly regulate the use of personal information in ADM systems, submissions to the Review highlighted privacy implications arising out of ADM.¹⁶³⁵ In particular, submitters raised concerns about the transparency and integrity of decisions made using ADM.¹⁶³⁶ Ensuring Australia's regulatory settings which apply to new and emerging technologies, including ADM, are fit for purpose in the digital age is crucial to promote public trust and confidence in the adoption of these technologies.¹⁶³⁷ The Discussion Paper sought feedback on proposals to increase transparency about the use of ADM, which would assist with enhancing individuals' confidence in the uptake of ADM in a variety of contexts.

19.1 What is ADM?

ADM refers to the deployment of technology to automate a decision-making process. ADM systems can be used to assist or replace the judgment of human decision-makers.¹⁶³⁸ ADM systems range from systems that apply simple business rules to those that use sophisticated algorithms to make discretionary decisions. This extends from the use of a simple rules-based formula to affirm if someone meets objective criteria, to the use of AI, where a computer learns from text, images or sounds to predict and take independent action, including making decisions, rather than being programmed to execute a decision-making process in a specified way.¹⁶³⁹ ADM systems offer the potential to increase the efficiency, accuracy and consistency of decisions, but these systems also raise complex ethical and legal issues.¹⁶⁴⁰

19.1.1 Impacts of ADM systems

The use of ADM systems is increasing across government and the private sector.¹⁶⁴¹ CrowdStrike submitted that AI has the opportunity to drive positive social outcomes and create the opportunity for innovation in a variety of industries including medicine and education.¹⁶⁴² The OAIC noted that ADM has the potential to create significant opportunities and efficiencies for society, but these benefits will only be fully enabled if the risks are appropriately mitigated.¹⁶⁴³ ADM systems offer the potential to increase the efficiency, accuracy and consistency of decisions.¹⁶⁴⁴

Information which relates to individuals can be used to train, test or deploy ADM systems. ADM can pose risks to individuals when systems are 'trained' using historical data that is affected by prejudice, such as through the under-representation of minorities in data-sets¹⁶⁴⁵ or when systems are not designed to take into account the unique circumstances of an individual.¹⁶⁴⁶ This can result in algorithmic bias which can lead to unfair treatment and discrimination.¹⁶⁴⁷ For example, if a system used to make home loan decisions was trained on many years of human decisions that were prejudiced against female loan applicants, the historical bias might be 'hidden' in the training data, but the system will continue to apply this disadvantage to female loan applicants, even if there is no longer any underlying prejudice or other improper motivation in the design of the system.¹⁶⁴⁸

¹⁶³⁴ Australian Government, [Positing Australia as a leader in digital economy regulation](#) (Issues Paper, March 2022) 1.

¹⁶³⁵ 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](#), 39-40; [OAIC](#), 46, 4; [Office of the Information Commissioner Queensland](#), 3; [Reset Australia](#), 7; [Salinger Privacy](#), 34-35.

¹⁶³⁶ Submissions to the Issues Paper: [CAIDE and MLS](#), 3; [Shaun Chung and Rohan Shukla](#), 7; [Consumer Policy Research Centre](#), 13; [Dr John Zerilli](#), 2. Submissions to the Discussion Paper: [Centre for AI and Digital Ethics](#), 8; [Consumer Policy Research Centre](#), 8-9; [Data Synergies](#); [Deloitte](#), 41; [elevenM](#), 49; [Calabash Solutions](#), 19; [Professor Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 20; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 9-10; [Office of the Victorian Information Commissioner](#), 8; [OAIC](#), 153.

¹⁶³⁷ Australian Government, [Positing Australia as a leader in digital economy regulation](#) (Issues Paper, March 2022) 1.

¹⁶³⁸ Information and Privacy Commission New South Wales, [Automated decision-making, digital government and preserving information access rights – for agencies](#) (September 2020) 1.

¹⁶³⁹ Australian Government, [Positing Australia as a leader in digital economy regulation](#) (Issues Paper, March 2022) 3.

¹⁶⁴⁰ AHRC, [Human Rights and Technology](#) (Final Report, 2021).

¹⁶⁴¹ OAIC, [Submission to AHRC Human Rights and Technology Inquiry Issues Paper](#) (Web Page, 19 October 2018); Australian Government, [Positing Australia as a leader in digital economy regulation](#) (Issues Paper, March 2022); Submissions to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 8; [Office of the Information Commissioner Queensland](#), 3.

¹⁶⁴² Submission to the Discussion Paper: [CrowdStrike](#), 4.

¹⁶⁴³ Submission to the Discussion Paper: [OAIC](#), 153.

¹⁶⁴⁴ AHRC, [Human Rights and Technology](#) (Final Report, 2021).

¹⁶⁴⁵ Ibid 107; Submissions to the Discussion Paper: [Professor Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 18-19; [NSW Council for Civil Liberties](#), 31.

¹⁶⁴⁶ Submission to the Discussion Paper: [European Commission](#).

¹⁶⁴⁷ Submission to the Discussion Paper: [Consumer Policy Research Centre](#), 8-9; AHRC, [Human Rights and Technology](#) (Final Report, 2021) 107.

¹⁶⁴⁸ AHRC, [Human Rights and Technology](#) (Final Report, 2021) 107.

UNSW Allens Hub, Deakin CSRI and IEEE SSIT submitted that privacy risks arise because ADM systems encourage greater data collection, sharing and combining.¹⁶⁴⁹ The OAIC's submission to the AHRC Issues Paper noted that privacy risks may include collating data from a wide variety of different sources, inferential decision-making based on data which may not be accurate, limited transparency around decision-making and retaining data for a longer period of time.¹⁶⁵⁰ The Office of the Information Commissioner Queensland suggested the significant impacts ADM can have on an individual's privacy and other rights warrants legislated, enforceable protections.¹⁶⁵¹

19.2 International approaches to regulating ADM in data protection laws

19.2.1 European Union

The GDPR includes specific obligations for the use of personal data to make decisions based solely on automated processing, including profiling, which produces legal or similarly significant effects.¹⁶⁵² If a human is involved in the decision making process, it will not be a decision based solely on automated processing.¹⁶⁵³ However, the human involvement needs to be meaningful and substantial.¹⁶⁵⁴ The GDPR requires that individuals be given prior notice of the use of personal data in ADM.¹⁶⁵⁵ It also requires that individuals have a right to access information about the existence of solely ADM producing legal or similarly significant effects, and 'meaningful information about the logic involved, as well as the significance and the envisaged consequences' of such processing to the individual.¹⁶⁵⁶ 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.¹⁶⁵⁷ Organisations must also carry out Data Protection Impact Assessments if processing of personal data is likely to result in high risk to individuals.¹⁶⁵⁸

19.2.2 United States

The *California Privacy Rights Act*, which comes into effect in 2023 will give consumers the right to opt-out of the use of ADM technology. Consumers will be able to request 'meaningful information about the logic involved in decision making processes, as well as a description of the likely outcome for the process with respect to the consumer'. These requirements are not limited to decisions that have a legal or similarly significant effect. The Virginia Consumer Data Protection Act, which comes into effect in 2023, will give individuals the ability to opt out of having their personal data processed for the purpose of profiling in furtherance of decisions that produce a legal or similarly significant effect concerning the consumer.

¹⁶⁴⁹ Submission to the Discussion Paper: [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 10.

¹⁶⁵⁰ OAIC, [Submission to AHRC Human Rights and Technology Inquiry Issues Paper](#) (Web Page, 19 October 2018);

¹⁶⁵¹ Submission to the Discussion Paper: [Office of the Information Commissioner Queensland](#), 4.

¹⁶⁵² GDPR art 22.

¹⁶⁵³ UK ICO, [Rights related to automated decision making including profiling](#) (Web Page).

¹⁶⁵⁴ Ibid.

¹⁶⁵⁵ GDPR arts 13(2)(f), 14(2)(g).

¹⁶⁵⁶ Ibid arts 13(2)(f), 14(2)(g), 15(1)(h).

¹⁶⁵⁷ Ibid art 22.

¹⁶⁵⁸ Ibid art 35.

19.3 Discussion Paper proposal

The Discussion Paper sought feedback on a proposal to require privacy policies to include information on whether personal information would be used in ADM which has a legal, or similarly significant effect on people's rights. A number of submitters expressed support for the proposal,¹⁶⁵⁹ with some suggesting the proposal would promote transparency.¹⁶⁶⁰ However, submitters generally considered that the proposal did not go far enough¹⁶⁶¹ and that privacy law should do more to address the harms associated with ADM.¹⁶⁶²

19.3.1 Solely automated processing

Some submitters sought clarification about whether the definition of ADM would align with the definition used in the GDPR, which applies to solely automated decisions.¹⁶⁶³ The UK ICO notes that for a decision to fall outside the scope of being a 'solely' automated decision, 'human involvement has to be active and not just a token gesture'.¹⁶⁶⁴ It further notes that the question is whether a human reviews the decision before it is applied and has discretion to alter it, or whether they are simply applying the decision taken by the automated system.¹⁶⁶⁵

Woolworths suggested the proposal should clarify that decision making is only 'automated' where it occurs without human intervention and that without this clarification the proposal risks becoming uncertain and unduly broad.¹⁶⁶⁶ elevenM suggested human oversight has only limited effectiveness in preventing or managing harms arising from ADM. Graham Greenleaf and Katharine Kemp recommended that any proposal in relation to ADM should capture decisions based significantly rather than solely on automated processing.¹⁶⁶⁷ Some submitters suggested the proposal should be amended to clarify that it only applies to the use of personal information relating to an identifiable individual.¹⁶⁶⁸

19.3.2 Legal or similarly significant effect

Submitters suggested the term 'legal or similarly significant effect' was uncertain.¹⁶⁶⁹ UK ICO guidance states that a decision produces 'legal effects' if it affects an individual's legal status or legal rights, such as the ability to access a social security benefit.¹⁶⁷⁰ A decision has a 'similarly significant effect' to a legal decision if it has an equivalent impact on an individual's circumstances, behaviour or choices, such as the automatic refusal of an online credit application.¹⁶⁷¹ The Article 29 EU Data Protection Working Party Guidelines on automated individual decision-making provides examples of automated decision-making with a similarly significant effect, including differential pricing resulting in prohibitively high prices that effectively bar someone from certain goods or services, or reducing a customer's credit card limit based on analysis of other customers.¹⁶⁷²

¹⁶⁵⁹ Submissions to the Discussion Paper: [Department of Health \(Cth\)](#), 14; [Deloitte](#), 41; [Calabash Solutions](#), 19; [Office of the Victorian Information Commissioner](#), 8; [OAIC](#), 154; [Information and Privacy Commission NSW](#), 4; [Castan Centre](#), 33; [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 9; [Meta](#), 44; [CHOICE](#), 16; [Australian Banking Association](#), 26; [DIGI](#), 22; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 12; [ACMA](#), 4; [Woolworths Group](#), 13.

¹⁶⁶⁰ Submissions to the Discussion Paper: [Calabash Solutions](#), 19; [Office of the Victorian Information Commissioner](#), 8; [Information and Privacy Commission NSW](#), 4.

¹⁶⁶¹ Submissions to the Discussion Paper: [Centre for AI and Digital Ethics](#), 8; [Consumer Policy Research Centre](#), 8-9; [Deloitte](#), 41; [elevenM](#), 48; [Australian Communications Consumer Action Network](#), 15; [Calabash Solutions](#), 19; [Professor Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 20; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 10; [OAIC](#), 154-155; [Office of the Information Commissioner Queensland](#), 4; [NSW Council for Civil Liberties](#), 31-32; [CHOICE](#), 15; [Australian Privacy Foundation](#), 13; [Privacy 108](#), 32; [Salinger Privacy](#), 38; [Graham Greenleaf](#), 5-6; [Dr Katharine Kemp](#), 19; [Department of Health Western Australia](#), 11; [Electronic Frontiers Australia](#), 13; [Financial Rights Legal Centre and Financial Counselling Australia](#), 17; [Digital Rights Watch](#), 21-22.

¹⁶⁶² Submissions to the Discussion Paper: [Digital Rights Watch](#), 22; see also: [Consumer Policy Research Centre](#), 8-9; [Australian Communications Consumer Action Network](#), 15.

¹⁶⁶³ Submissions to the Discussion Paper: [Australian Banking Association](#), 26; [Australian Financial Markets Association](#), 8;

¹⁶⁶⁴ UK ICO, [What does the UK GDPR say about automated decision-making and profiling?](#) (Web Page).

¹⁶⁶⁵ Ibid.

¹⁶⁶⁶ Submission to the Discussion Paper: [Woolworths Group](#), 13.

¹⁶⁶⁷ Submissions to the Discussion Paper: [Graham Greenleaf](#), 5-6; [Dr Katharine Kemp](#), [UNSW Sydney](#), 19.

¹⁶⁶⁸ Submissions to the Discussion Paper: [Woolworths Group](#), 13; [Ai Group](#), 11;

¹⁶⁶⁹ Submissions to the Discussion Paper: [Experian](#), 21; [ACMA](#), 4; [Woolworths Group](#), 13; [Ai Group](#), 11; [Business Council of Australia](#), 11.

¹⁶⁷⁰ UK ICO, [What does the UK GDPR say about automated decision-making and profiling?](#) (Web Page).

¹⁶⁷¹ Ibid.

¹⁶⁷² Article 29 Data Protection Working Party, [Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679](#), Adopted on 3 October 2017, 22.

A large number of submitters supported including a non-exhaustive list of examples of decisions with legal or similarly significant effect.¹⁶⁷³ The OAIC noted that United States legislation has sought to provide additional clarification on the scope of this term.¹⁶⁷⁴ The Virginia Consumer Data Protection Act provides a non-exhaustive list of significant effects, which includes denial of consequential services or support, such as financial and lending services, housing, insurance, education enrolment, criminal justice, employment opportunities and health care services, or access to basic necessities, such as food and water.¹⁶⁷⁵

The Law Council of Australia suggested these examples should be supplied in a form that would allow it to be focused on the technology of the day and to be updated on a regular basis.¹⁶⁷⁶ The Castan Centre recommended removing the word 'similarly' and suggested it added confusion and could limit an individual's rights.¹⁶⁷⁷ The submission further suggested that 'introducing a threshold of significance elevated to a standard akin to a legal right may create barriers to justice for vulnerable individuals'.¹⁶⁷⁸

Proposal – prior notification of the use of personal information in ADM systems

In response to submitter feedback, it is proposed that entities be required to include information on whether personal information will be used in ADM which has a legal, or similarly significant effect on an individual's rights in the entity's privacy policy. OAIC guidance should be developed on the types of decisions with a legal or similarly significant effect on an individual's rights. This could extend to providing a non-exhaustive list of examples of decisions in guidance. The obligation should extend to decisions that are substantially automated, rather than being restricted to decisions that are solely automated. As noted in the Discussion Paper, few decisions are made without any level of human intervention, and if the proposal was restricted to solely automated decisions, entities could potentially bypass requirements by including a negligible level of human involvement.¹⁶⁷⁹ This would align with the interpretation of the GDPR regulation of 'solely automated decisions' which applies to ADM if human involvement is 'fabricated' rather than 'meaningful'.¹⁶⁸⁰ Guidance should be provided to entities to clarify the meaning of 'substantially automated', which should not capture decisions where a human decision-maker has genuine oversight of a decision, reviews a decision before it is applied and has discretion to alter the decision. Consultation will be required to ensure the parameters of 'substantially automated' are appropriately calibrated.

19.1 Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal, or similarly significant effect on an individual's rights.

19.2 High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act. This should be supplemented by OAIC Guidance.

¹⁶⁷³ Submissions to the Discussion Paper: [Deloitte](#), 41; [Office of the Victorian Information Commissioner](#), 8; [Castan Centre](#), 33; [CHOICE](#), 16; [Australian Banking Association](#), 27; [Experian](#), 21; [Privacy 108](#), 32; [Department of Health Western Australia](#), 11; [Australian Financial Markets Association](#), 8; [Western Union](#), 8; [Law Council of Australia](#), 16.

¹⁶⁷⁴ Submission to the Discussion Paper: [OAIC](#), 156.

¹⁶⁷⁵ *Code of Virginia* ch 53 (*Consumer Data Protection Act*) § 59.1-571; Future of Privacy Forum, [Automated decision-making systems: Considerations for state policymakers](#) (Web Page, May 2021).

¹⁶⁷⁶ Submission to the Discussion Paper: [Law Council of Australia](#), 16.

¹⁶⁷⁷ Submission to the Discussion Paper: [Castan Centre](#), 32-33.

¹⁶⁷⁸ *Ibid.*

¹⁶⁷⁹ 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 to the Issues Paper: [OAIC](#), 94, which submitted that the OPC of Canada explicitly recommended against the use of 'solely' in Bill C-11 (*Consumer Privacy Protection Act* and the *Personal Information and Data Protection Tribunal Act* (2020)) (Canada)).

¹⁶⁸⁰ Article 29 Data Protection Working Party, [Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679](#), Adopted on 3 October 2017, 20-21.

19.3.3 Additional protections

Submissions suggested expanding the proposal to include a right to opt-out of ADM,¹⁶⁸¹ a right to review¹⁶⁸² or right to challenge decisions made using ADM,¹⁶⁸³ a right to explanation,¹⁶⁸⁴ no go zones¹⁶⁸⁵ and additional organisational accountability requirements such as Privacy Impact Assessments or more detailed privacy policies.¹⁶⁸⁶ Submissions suggested that informing individuals of the fact that ADM is happening does little to equip individuals with the ability to seek redress where harms arise.¹⁶⁸⁷

The Department of Industry, Science and Resources is considering how regulatory settings and systems can maximise the opportunities of AI and ADM through its consultation.¹⁶⁸⁸ It is seeking feedback on a proposal to require impact assessments to be undertaken if there is a medium or high risk of adverse impacts from an AI or ADM application. The proposed requirement would be mandatory for Commonwealth agencies, and voluntary for private sector organisations.

The AHRC report considered, but did not recommend a right to explanation, and noted that generally, decisions made by non-government entities do not carry a legal entitlement to reasons. The OAIC suggested the Discussion Paper proposal could be supplemented with a requirement to provide a more technical explanation of the ADM process on request. This could include information about the types of personal information being used, how that information is weighted and information about how any ratings given to an individual relates to other information or decisions.¹⁶⁸⁹

elevenM suggested individuals should be given meaningful information about the decision-making logic involved, as well as the significance and the consequences for the individual, consistent with the GDPR. The European Commission submitted that a right to explanation should include information about the underlying logic of decisions. This suggestion aligns with the views of Australians on AI technology in the OAIC Australian Community Attitudes to Privacy Survey (2020 ACAP survey) results, which showed 84 per cent of respondents believed individuals should have a right to know if a decision affecting them is made using AI technology, and 78 per cent believed individuals should be told what factors and personal information are considered by the algorithm and how these factors are weighted.¹⁶⁹⁰

Proposal – right to meaningful information

In response to submitter concerns about the limited utility of the Discussion Paper proposal, it is proposed that entities be required to also provide individuals with meaningful information about how automated decisions with a legal or similarly significant effect on an individual's rights are made. Information provided through privacy notices or privacy policies could include general information about the types of personal information that would be used and how the information would be weighted. Information provided to individuals on request could be more tailored to the specific individual and include an explanation of how a decision was reached. Proposals 18.7-18.9 regarding responding to requests to exercise rights of the individual would apply to requests for meaningful information on automated decisions with legal or similarly significant effect on an individual's rights.

1681 Submissions to the Discussion Paper: [elevenM](#), 48-49; [Professor Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 20; [NSW Council for Civil Liberties](#), 32.

1682 Submissions to the Discussion Paper: [elevenM](#), 48-49; [Australian Communications Consumer Action Network](#), 15; [NSW Council for Civil Liberties](#), 32; [European Commission](#); [Salinger Privacy](#), 38; [Electronic Frontiers Australia](#), 13; [Financial Rights Legal Centre and Financial Counselling Australia](#), 17; [Digital Rights Watch](#), 22.

1683 Submissions to the Discussion Paper: [elevenM](#), 48-49; [European Commission](#); [CHOICE](#), 15; [Financial Rights Legal Centre and Financial Counselling Australia](#), 17.

1684 Submissions to the Discussion Paper: [Deloitte](#), 41; [elevenM](#), 48-49; [Australian Communications Consumer Action Network](#), 15; [OAIC](#), 155; [European Commission](#); [Salinger Privacy](#), 38; [Electronic Frontiers Australia](#), 13; [Digital Rights Watch](#), 22.

1685 Submissions to the Discussion Paper: [CHOICE](#), 15; [Privacy 108](#), 32; [Financial Rights Legal Centre and Financial Counselling Australia](#), 17.

1686 Submissions to the Discussion Paper: [Calabash Solutions](#), 19; [OAIC](#), 155; [Privacy 108](#), 32; [Minderoo Tech & Policy Lab](#), [UWA Law School](#), 13.

1687 Submissions to the Discussion Paper: [elevenM](#), 49-50; [Digital Rights Watch](#), 22.

1688 Australian Government, [Positioning Australia as a leader in digital economy regulation – Automated Decision Making and AI Regulation](#) (Issues Paper, March 2022) 1.

1689 Submission to the Discussion Paper: [OAIC](#), 155.

1690 OAIC, [Australian Community Attitudes to Privacy Survey 2020](#) (2020) 87.

Providing individuals with meaningful information on automated decisions with legal or similarly significant effect would ensure individuals have sufficient understanding about the rationale for automated decisions to enable them to exercise other rights, either under privacy law, such as the right to object, or other frameworks such as administrative or discrimination law. Other current and proposed requirements under the Act would also operate to safeguard the integrity of automated decisions through obligations relating to personal information used in ADM systems. For example, the obligation in APP 10 to take reasonable steps to ensure the accuracy and quality of personal information held by entities and the application of the fair and reasonable test may operate to require entities to monitor their ADM systems for bias where the decisions being made would significantly impact individuals. The right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made should be considered as part of broader work to regulate AI and ADM, including the work being undertaken by the Department of Industry, Science and Resources. A consistent approach across frameworks will be required to ensure the proposal is not duplicative and to reduce the regulatory burden on APP entities.

19.3 Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect.

This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.

20. Direct marketing, targeting and trading

Data has taken on a critical role with the rise of the digital economy.¹⁶⁹¹ A paper by the International Monetary Fund notes that the proliferation of data in the economy presents ‘a tremendous opportunity to boost growth through efficiency and innovation’ but argues there is a trade-off between reaping the commercial and social benefits that can be derived from the collection and dissemination of personal information and respecting an individual’s desire for privacy.¹⁶⁹²

The privacy risks associated with direct marketing have changed significantly since the APPs were introduced. The OAIC’s submission to the Discussion Paper noted that privacy risks have emerged due to the use of high volumes of data, often involving personal information to deliver targeted advertising on websites and apps.¹⁶⁹³ Submitters have highlighted the significant benefits and potential harms that can flow from the use of information to provide personalised content. The ACCC estimated that display advertising expenditure was around \$6.5 billion in Australia in 2020.¹⁶⁹⁴ Entities yield revenue from user engagement with personalised content and advertising, which enables them to provide consumers with access to content or services for free or at a lower cost. However, consumers often underestimate the degree and consequences of the data collection that websites carry out in exchange for providing free digital goods and services.¹⁶⁹⁵

The DPI Report recommended 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’.¹⁶⁹⁶ The report suggested that consumers who prefer to provide their personal information for targeted advertising purposes should be required to actively make this selection.¹⁶⁹⁷ The DPI Report also recommended that a ‘Digital Platforms’ Data Practices Code’ be developed to provide consumers the ability to select global opt-outs or opt-ins for the collection of personal information for profiling purposes or sharing personal information with third parties for targeted advertising purposes.¹⁶⁹⁸

The Discussion Paper put forward several proposals in relation to direct marketing and targeted advertising. This chapter sets out stakeholder feedback on those proposals and makes a number of new proposals in light of that feedback. Accordingly, the Report recommends further consultation on these new proposals.

20.1 Current regulation of direct marketing

APP 7 provides that an organisation must not use or disclose personal information that it holds about an individual for the purposes of direct marketing with some exceptions. Direct marketing was included in the Act as a discrete principle rather than as a kind of secondary purpose under APP 6 because of the community interest about the use and disclosure of personal information for the purpose of direct marketing.¹⁶⁹⁹

Organisations are prohibited 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.¹⁷⁰⁰ If an individual would not reasonably expect their personal information to be used or disclosed for direct marketing, or the personal information was collected from a third party, consent must be obtained unless impracticable to do so.¹⁷⁰¹ These provisions reflect the intent that more stringent obligations should apply to organisations that use the information of individuals who are not existing customers.¹⁷⁰²

Organisations must not use or disclose sensitive information for the purpose of direct marketing unless the individual has provided consent.¹⁷⁰³ There are no exceptions to this requirement. In all cases, the organisation must provide simple means by which the individual may easily request not to receive direct marketing from the organisation.

¹⁶⁹¹ International Monetary Fund, *The Economics and Implications of Data: An Integrated Perspective* [Report No 19/16 2019] 1.

¹⁶⁹² Ibid.

¹⁶⁹³ Submissions to the Discussion Paper: OAIC, 98.

¹⁶⁹⁴ ACCC, *Digital Advertising Services Inquiry: Final Report* [Report, 2021] 43.

¹⁶⁹⁵ Federal Trade Commission (United States of America), *A Brief Primer on the Economics of Targeted Advertising* [2020] 9.

¹⁶⁹⁶ ACCC, *DPI Report*, 465.

¹⁶⁹⁷ Ibid 468.

¹⁶⁹⁸ Ibid 481.

¹⁶⁹⁹ Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 81.

¹⁷⁰⁰ Privacy Act sch 1 APP 7.2.

¹⁷⁰¹ Ibid APP 7.3.

¹⁷⁰² Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 81.

¹⁷⁰³ Privacy Act sch 1 APP 7.4

Finally, APP 7 does not apply to the extent that the *Spam Act 2003* (Cth) (Spam Act) or DNCR Act apply.¹⁷⁰⁴ For example, APP 7 would not likely be relevant to direct marketing calls or faxes where the number is listed on the Do Not Call Register, or the call is made by a registered charity.¹⁷⁰⁵ Submissions noted that different definitions of 'direct marketing' apply in these Acts and supported harmonisation of the requirements across the Acts.¹⁷⁰⁶

20.2 Discussion Paper proposals

Direct marketing is not defined in the Privacy 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'.¹⁷⁰⁷ The Discussion Paper presented a broad concept of 'direct marketing' to capture a spectrum of activities including:

- direct communication of marketing material to an individual by using their personal information such as their name and address, and
- displaying online advertisements targeted to individuals based on a profile of their attributes, characteristics or interests, inferred from their online behaviour and other datasets.¹⁷⁰⁸

The Discussion Paper put forward proposals aimed at addressing privacy harms associated with this range of activities.

20.2.1 Provide individuals with more choice and control

Submissions to the Issues Paper raised concerns about the validity of consent to direct marketing where consent sought is expressed in broad terms and bundled with other information handling purposes or is required as a condition of accessing a service.¹⁷⁰⁹ Submitters also suggested that opting out of receiving direct marketing can require complex, time-consuming and repeated actions.¹⁷¹⁰

There is currently no right to opt out of the collection, use or disclosure of personal information for the purpose of direct marketing.¹⁷¹¹ This limits the ability for individuals to exercise control over their personal information for the range of above marketing activities.

The Discussion Paper sought feedback on a proposal to require entities to provide individuals with an unqualified right to object to any collection, use or disclosure of personal information for the purpose of direct marketing. On receiving notice of an objection, an entity would be required to 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.

20.2.2 Provide individuals with greater transparency

Submissions to the Issues Paper also expressed concern about a lack of transparency in relation to profiling and targeted advertising.¹⁷¹² The DPI Report found 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.¹⁷¹³

1704 Ibid APP 7.8

1705 Submission to the Issues Paper: [OAIC](#), 45. See also OAIC, [APP Guidelines](#) (July 2019) [7.9]–[7.12].

1706 Submissions to the Discussion Paper: [Calabash Solutions](#), 18–19; [Commonwealth Bank of Australia](#), 3; [Shopping Centre Council of Australia](#), 9; [Privacy 108](#), 30.

1707 OAIC, [APP Guidelines](#) (July 2019) [7.9].

1708 [Discussion Paper](#), 124.

1709 Submissions to the Issues Paper: [Dr Katharine Kemp](#), 16; [OAIC](#), 77; [Deloitte Australia](#), 11; [Consumer Policy Research Centre](#), 7–9. For broader concerns about requiring consent to the use of personal information to access online services see 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](#), 21; [Law Institute of Victoria](#), 9; [CAIDE and MLS](#), 7; [NSW Council for Civil Liberties](#), 8; [Uniting Church of Australia](#), 3; [Queensland Law Society](#), 5–6

1710 Submissions to the Issues Paper: [Dr Katharine Kemp](#), 19; [Legal Aid Queensland](#), 12; [Privacy 108](#), 12.

1711 Submission to the Issues Paper: [OAIC](#), 55.

1712 Submissions 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.

1713 ACCC, [DPI Report](#), 412.

The Discussion Paper sought feedback on a proposal to require APP entities to include additional information in their privacy policy, including:

- 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.

The Discussion Paper also tested a proposal to require the use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions to be a primary purpose notified to the individual when their personal information is collected. Under this proposal, entities would only be permitted to undertake direct marketing where it was the purpose for the original collection, as notified to the individual. It was considered that this proposal could capture targeted advertising to consumers of goods and services as well as the use of profiling to target individuals with ideological or political messaging.

20.3 Submitter feedback

Stakeholder feedback on the Discussion Paper proposals was mixed. While there was strong support for addressing privacy harms associated with direct marketing and targeting, submitters suggested the proposals should be refined to better achieve the objectives outlined in the Discussion Paper. Feedback from submissions highlighted that any reforms should:

- distinguish direct marketing from targeting personalised content and advertising
- recognise that targeting often uses information that does not meet the threshold of personal information, but the use of such information can still pose privacy risks
- address identified harms while ensuring that beneficial direct marketing and targeted advertising is not adversely impacted
- clarify how any proposed reforms would apply to ad-supported platforms, and
- clarify whether profiling and trading in personal information would be captured by the proposals.

20.3.1 Direct marketing is distinct from targeting

Submissions noted the definition of direct marketing used in the APP Guidelines is difficult for entities to comprehend as it lacks specificity and clarity,¹⁷¹⁴ and suggested it is currently unclear if the definition captures targeted advertising or contextual advertising because it requires *direct communication*.¹⁷¹⁵ Submitters suggested 'direct marketing' is not the most suitable term to accurately reflect the range of activities referred to in the Discussion Paper. Salinger Privacy and ADMA recommended that regulatory responses should distinguish between the more intrusive and covert tracking and profiling activities (across websites, apps and devices) which power targeted personalised content and advertising, and less harmful activities such as a business sending out an email to its existing customer base to notify them of a sale.¹⁷¹⁶ These submissions suggested that direct marketing to a known individual with whom an organisation has a pre-existing relationship should remain lawful provided individuals could opt-out of the direct marketing.¹⁷¹⁷ Submissions also noted that 'direct marketing' does not capture targeted messaging not in the form of 'marketing', which could pose privacy harms, such as the amplification of misinformation, exclusion from opportunities or influencing voter intentions.¹⁷¹⁸

The definition presents challenges when attempting to address online harms resulting from online behavioural advertising and other forms of targeting. This is because the delivery of targeted content does not require direct communication with an individual. In addition, targeting can rely on the collection, use and disclosure of information relating to individuals that may not meet the threshold of personal information. Data Synergies submitted that using audience segments enables 'personalisation', in the sense that a distinct group of users receive advertisements

1714 Submissions to the Discussion Paper: [Australian Association of National Advertisers](#), 6.; [ADMA](#), 28-29; [Google](#), 5; [Snap Inc](#), 7.

1715 Submissions to the Discussion Paper: [Australian Association of National Advertisers](#), 6; [Google](#), 5; [Snap Inc](#), 7.

1716 Submissions to the Discussion Paper: [Salinger Privacy](#), 26; [ADMA](#), 28.

1717 Submissions to the Discussion Paper: [Salinger Privacy](#), 32; [ADMA](#), 28.

1718 Submissions to the Discussion Paper: [Salinger Privacy](#), 32; [elevenM](#), 45.

tailored to their needs, preferences or interests, but the recipient does not need to be personally identified.¹⁷¹⁹ Deloitte noted that uncertainty about whether the current definition of personal information includes technical information, and that de-identified information is not protected under the Act, can also result in limited transparency for these activities (and, particularly, marketing and advertising activities that can involve third parties tracking individuals in a de-identified manner across a range of platforms).¹⁷²⁰

How does targeting work?

Targeting systems are used to promote content in social media feeds, recommend videos, target advertisements and personalise search engine results.¹⁷²¹ Online targeting includes personalised advertising, which enables advertisers to direct advertisements to specific groups of people based on information held about them and content recommendation systems which personalise content to individual users based on information held about them.¹⁷²² Content recommendation systems learn how a user, and similar users, respond to different content and use this information to generate more accurate predictions.¹⁷²³ Content recommendation systems and personalised advertising work together to drive the success of online platforms.¹⁷²⁴ Content recommendation systems encourage users to spend more time on a platform and in the process, users share more data about themselves.¹⁷²⁵ This increases the revenue that can be earned from personalised advertising.¹⁷²⁶

Personalised advertising on platforms allows advertisers to target platform users based on information the platform has collected and inferred about users.¹⁷²⁷ This may include sensitive information, or enable sensitive characteristics to be inferred.¹⁷²⁸ Platforms may also enable advertisers to target their own customers by matching common features held by platforms and advertisers about individuals such as email address or phone numbers.¹⁷²⁹ Advertisers can also target potential customers by using platforms' tracking code on their website to show ads to them when they visit the platform.¹⁷³⁰ Platforms also provide tools for advertisers to target 'lookalikes' of their existing customers based on a measure of each user's similarity to others.¹⁷³¹

Programmatic advertising allows advertisers to target people across the internet outside of platform environments.¹⁷³² Real-time bidding allows advertisers to compete for advertising space on websites in milliseconds.¹⁷³³ When a person visits a website, the website publisher auctions advertising space to multiple advertisers through an auction system for advertising to be directed to that person.¹⁷³⁴ This process involves considering information about the person visiting the website, likely gathered through tracking technologies embedded in websites such as cookies and fingerprinting. Advertisers may attempt to build a more detailed picture of the person by referring to data about the person held by data brokers and others.¹⁷³⁵ Based on this information, they decide how much they think it is worth to advertise to this person, and bid for the advertising space on that basis.

20.3.2 Information used for targeting

Developments in the way data is handled makes it increasingly difficult to draw a clear distinction between personal and non-personal information in the online environment.¹⁷³⁶ Targeting can use a broad range of information about people including their demographic characteristics, interests, location, devices and personality types.¹⁷³⁷ Chris Culnane and Kobi Leins have suggested 'there is a significant incentive for organisations to assert their data is de-identified, since it frees them to use it for secondary purposes without consent, and to on-sell the data locally or internationally'.¹⁷³⁸ Dr Katharine

1719 Submission to the Discussion Paper: [Data Synergies](#), 17.

1720 Submission to the Discussion Paper: [Deloitte Australia](#), 38.

1721 Centre for Data Ethics and Innovation (UK), [Online targeting: Final report and recommendations](#) (2020).

1722 Ibid.

1723 Ibid.

1724 Ibid.

1725 Ibid.

1726 Ibid.

1727 Ibid.

1728 Facebook, [Review your off-Facebook activity](#) (Web Page, 2020).

1729 Centre for Data Ethics and Innovation (UK), [Online targeting: Final report and recommendations](#) (2020).

1730 For example, Google Analytics Conversations, Facebook Pixel.

1731 For example, Google Analytics Conversations, Facebook Pixel.

1732 ACCC, [Digital Advertising Services Inquiry: Final Report](#) (2021) 34.

1733 UK ICO, [Update report into adtech and real time bidding](#) (2019) 5.

1734 Centre for Data Ethics and Innovation (UK), [Online targeting: Final report and recommendations](#) (2020).

1735 Ibid.

1736 Submission to the Issues Paper: [OAIIC](#), 45-46.

1737 Kayleen Manwaring, Katharine Kemp and Rob Nicholls, [\[Mis\]informed Consent in Australia](#) (2021) 88-119.

1738 Chris Culnane and Kobi Leins, 'Misconceptions in Privacy Protection and Regulation' (2019) 36(2) *Law in Context* 49, 50.

Kemp noted that entities often state the information they use has been ‘anonymised’ or ‘de-identified’ such that it is no longer personal information – the implication is that the use of this information poses no risk to the individual and is not governed by the Privacy Act.¹⁷³⁹

Many businesses aim to distinguish, profile and interact with individuals using this information.¹⁷⁴⁰ The OAIC’s submission to the Issues Paper noted that targeting involves increasingly complex methods involving multiple parties using cookies and other identifiers which enables the individual user of a device to be targeted to receive a particular advertisement, offered personalised content or recommendations, sent political messaging, or subjected to automated decisions such as differential pricing.¹⁷⁴¹ Dr Kayleen Manwaring, Dr Katharine Kemp and Dr Rob Nicholls observed that data brokers often market their ability to provide a ‘single customer view’ or a ‘360 view’ of individual customers. They often achieve this by using ‘unique identifiers’ in the absence of a name or email address.¹⁷⁴² However, Chris Culnane and Kobi Leins have argued that the data points that represent an individual’s actions, devices, location etc. are often as effective, if not more effective, at identifying an individual as traditional identifiers.¹⁷⁴³

The UK ICO has recognised that an individual may be identifiable either as a named individual or simply as a unique user of electronic communications and other internet services who may be distinguished from all other users.¹⁷⁴⁴ The point at which an individual is identifiable by a particular service provider as a result of an identifier is highly dependent on the circumstances and the context in which it is used and may depend on the relationship between the individual and the service provider (such as whether the individual has used the service previously and the extent of that engagement).

By creating a user profile, an advertiser can segment users and assign specific interest category labels to that user based on a range of information relating to the individual. The individual will then be presented with advertisements relevant to that label. The information which is used to target individuals with personalised content and advertising could be ‘information which relates to an individual’. However, as set out in Chapter 4, it will only be personal information that is protected under the Act if the person is reasonably identifiable or identified.

The following is an example of how targeted advertising could occur by assigning an audience label using information that relates to a person, but may not be personal information.

An online search service may have access to information such as device identifiers and IP addresses when a person is not signed into an account, which may be linked to other information about the person (such as search history). If the person shows an interest in purchasing a mobile phone plan through their internet activity, the online search service may then place the person in a segment for advertising based on this information. The person is then served advertisements highlighting deals available for mobile phone plans.

Submitters had mixed views about whether reforms should apply to aggregated information. Some submissions suggested that reforms should not apply to marketing that is aggregated and targeted to cohorts of users rather than individuals.¹⁷⁴⁵ Telstra submitted that personal information is aggregated so that it is not reasonably capable of re-identification, it will no longer be personal information and should not be subject to the Act. Equifax submitted that extending reforms to aggregated information would unreasonably limit the business utility of personal information which is not warranted in view of the privacy risk to individuals. Other submitters suggested it was necessary for reforms to extend to aggregated information.¹⁷⁴⁶ Uniting Church submitted that allowing an exemption for aggregation would ‘create a loophole that is likely to be extensively used to target people who have individually objected to targeted marketing’.¹⁷⁴⁷

1739 Kayleen Manwaring, Katharine Kemp and Rob Nicholls, [\[Mis\]informed Consent in Australia](#) (2021) 106.

1740 Ibid 107.

1741 Submission to the Issues Paper: [OAIC](#), 46.

1742 Kayleen Manwaring, Katharine Kemp and Rob Nicholls, [\[Mis\]informed Consent in Australia](#) (2021) 107.

1743 Chris Culnane and Kobi Leins, ‘Misconceptions in Privacy Protection and Regulation’ (2019) 36(2) *Law in Context* 49, 53.

1744 UK ICO, ‘[What are identifiers and related factors?](#)’ (Web Page).

1745 Submissions to the Discussion Paper: [Shopping Centre Council of Australia](#), 9; [Telstra](#), 20-21; [Equifax](#), 15.

1746 Submissions to the Discussion Paper: [Calabash Solutions](#), 19; [Consumer Policy Research Centre](#), 8; [Obesity Policy Coalition](#), 14; [Foundation for Alcohol Research and Education](#), 19-20; [Public Health Association Australia](#), 10.

1747 Submission to the Discussion Paper: [Uniting Church in Australia](#), [Synod of Victoria and Tasmania](#), 9.

Current regulation of targeting

The protections in the Act only apply to personal information. Since the information collected and used in targeting is often not enough to identify an individual (such as information about a user's interests and the websites they visited), an organisation that uses this information may not need to comply with the Act.¹⁷⁴⁸

The Australian Consumer Law (ACL) includes prohibitions against misleading and deceptive conduct, false and misleading claims and certain unfair business practices.¹⁷⁴⁹ The ACCC has brought several cases under the ACL challenging the extent and manner of consumer tracking undertaken by large digital platforms under these provisions.¹⁷⁵⁰ However, the ACL does not specifically regulate targeting and where targeting is not misleading or deceptive, or does not otherwise breach the ACL, the ACCC will not be able to take action.

The Australian advertising industry is largely self-regulated. The *Australian Best Practice Guideline for Online Behavioural Advertising*¹⁷⁵¹ (OBA Guideline) was developed by a group of businesses and industry associations in the online advertising sector. The OBA Guideline applies to the collection and use of 'interest-based advertising' data to serve advertising based on pre-defined interest categories. Interest based advertising data ('IBA data') is defined as data on web browsing activity of an internet-enabled device which allows the device to be added to one or more pre-defined interest categories.¹⁷⁵² The OBA Guideline states that IBA data does not include personal information.

The OBA Guideline does not apply to contextual advertising, which is advertising that is displayed to visitors to webpages based on the content of the webpage being viewed (e.g. if a person views a travel webpage and they are served an advertisement for luggage or travel insurance whilst viewing that webpage). Contextual advertising can also include search engine advertising (e.g. if a user searches travel and the search results display a travel ad).

The OBA Guideline sets out 7 self-regulatory principles:¹⁷⁵³

1. third parties shall not combine IBA data with personal information unless they treat the IBA data as personal information in accordance with the Privacy Act
2. third parties should give clear and comprehensible notice
3. third parties should give users choice with respect to the collection and use of third party IBA purposes
4. entities should maintain appropriate safeguards to protect IBA data and only retain IBA data for as long as necessary
5. categories uniquely designed to target children under 13 will not be created – third party IBA which relies on sensitive market segments (defined consistently with sensitive information under the Privacy Act) should obtain a user's express consent prior to engaging in third party IBA using that information
6. entities should provide information to inform individuals and businesses about IBA
7. signatories to guideline are responsible for self-certifying they comply with the guideline.

A number of organisations are signatories to the OBA Guideline, including Fairfax Digital, Google, Microsoft, NineMSN, realestate.com.au, Sensis Digital Media, Digital Ten and Yahoo!7. The OBA Guideline states that it is 'overseen by the ADDA' – the Australian Digital Advertising Alliance.

20.3.3 Impacts of targeting

The UK Government expert body, the Centre for Data Ethics and Innovation (CDEI Online Targeting Report), examined the impact of targeting in 2020 and identified key elements of platforms' social and political power as including:¹⁷⁵⁴

- observation: platforms observe people's behaviour in environments where they have an expectation of privacy. Knowledge about individuals makes it easier to influence their actions. When people know they are being observed they may behave differently
- influencing perception: platforms have become a major source of news and information – the decisions made by online targeting systems influence the flow of information in society and this affects what people perceive as normal, important and true. This impact is compounded by the fact that people do not know this process is taking place since it does not involve a conscious choice like turning on the TV or picking up a newspaper.

¹⁷⁴⁸ OAIC, [Targeted advertising](#) (Web Page).

¹⁷⁴⁹ *Competition and Consumer Act 2012* (Cth) vol 3, sch 2, ss 18, 29-34, 151-160.

¹⁷⁵⁰ For example, *Australian Competition and Consumer Commission v Google LLC (No 2)* [2021] FCA 367.

¹⁷⁵¹ IAB Australia, [Online Behavioural Advertising Guidelines](#) (2014).

¹⁷⁵² Ibid 7.

¹⁷⁵³ Ibid 10-13.

¹⁷⁵⁴ Centre for Data Ethics and Innovation (UK), [Online targeting: Final report and recommendations](#) (2020).

- **prediction and influence:** organisations using online targeting systems can learn how people react to content and use this knowledge to make increasingly accurate predictions which can be used to influence people's actions and beliefs, as individuals and across populations.

Privacy harms associated with targeting

The effectiveness of targeting lies in its ability to predict people's preferences and behaviours and influence their perceptions, actions and beliefs.¹⁷⁵⁵ While this can bring benefits to both organisations (by showing products to customers most likely to be interested) and individuals (through seeing content that is most relevant to them), it also has the potential for significant harm.

Lack of transparency and control

Submissions to the Review raised concerns about the lack of transparency about what data is being collected for targeting and how it is being used, as well as an absence of effective control over that data.¹⁷⁵⁶ This lack of transparency and control allows user data to be used for targeting in ways that are contrary to consumers' expectations and wishes.¹⁷⁵⁷ The Foundation for Alcohol Research and Education submitted that there is 'little to no transparency' about how data-driven advertising models function to deliver highly personalised and targeted advertising to individuals.¹⁷⁵⁸ Deloitte suggested the specificities of particular marketing activities are not always detailed in privacy notices or privacy policies and as a result consumers are not always made aware of how their data is handled in relation to these activities.¹⁷⁵⁹

In relation to targeting for political campaigning, the UK ICO has noted the importance of being able to communicate with and engage voters, including through digital technologies, as an essential part of democratic life. However, it considers that the 'often invisible' nature of these techniques can affect people's trust and confidence in how their personal data is being used which poses a risk which undermines the democratic process.¹⁷⁶⁰ Submitters to the Review echoed this concern.¹⁷⁶¹

The ACCC's Digital Advertising services inquiry ('Adtech') final report noted that consumer harms can arise from targeted display advertising in situations where consumers are not informed or do not consent to how their data is collected, processed, used, or stored, and also in the case of data breaches.¹⁷⁶² It noted that the increasing amounts of data on individuals resulting from Australians carrying out more of their lives online, is concerning where consumers are unsure how to, or cannot exercise control over their data and how it is used.¹⁷⁶³ The Office of the Victorian Information Commissioner supported amending the Act to give individuals greater control over the use of their information in advertising and to make entities more transparent about the use of individuals' personal information for advertising purposes.¹⁷⁶⁴

The UK Competition and Markets Authority online and digital advertising market study found that:¹⁷⁶⁵

- consumers have some control over their data, but frequently platforms do not give them full control and some do not allow consumers to turn off personalised ads
- consumers are served with personalised advertisements by default and consumers are 'nudged' to make choices that are in the best interest of the platform, and
- consumers must engage with long, complex terms and conditions, and must make several clicks to access settings – consumers rarely engage with these terms and when they do, they spend very little time reading them.

¹⁷⁵⁵ Ibid.

¹⁷⁵⁶ Submissions to the Discussion Paper: [Dr Katharine Kemp, UNSW Sydney](#), 18; [OAIC](#), 147; [Foundation for Alcohol Research and Education](#), 19-20.

¹⁷⁵⁷ [Digital Platform Services Inquiry: Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services](#) (2022) 43.

¹⁷⁵⁸ Submissions to the Discussion Paper: [Foundation for Alcohol Research and Education](#), 20.

¹⁷⁵⁹ Submission to the Discussion Paper: [Deloitte Australia](#), 39.

¹⁷⁶⁰ UK ICO, [Guidance for the use of personal data in political campaigning](#) (Web Page).

¹⁷⁶¹ Submission to the Issues Paper: [Queensland University of Technology, Faculty of Law](#), 18; [Office of the Victorian Information Commissioner](#), 5-6; [Salinger Privacy](#), 12; [Office of the Information Commissioner, Queensland](#), 3; [Digital Rights Watch](#), 5. Submissions to the Discussion Paper: [Internet Association of Australia](#), 3; [Office of the Victorian Information Commissioner](#), 3-4 [elevenM](#), 22-23; [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 2-3; [Castan Centre](#), 13; [Digital Rights Watch](#), 18; [Professor David Lindsay](#), 17.

¹⁷⁶² ACCC, [Digital Advertising Services Inquiry: Final Report](#) (2021), 40.

¹⁷⁶³ Ibid.

¹⁷⁶⁴ Submission to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 8.

¹⁷⁶⁵ Competition and Markets Authority (UK), [Online platforms and digital advertising - Market study final report](#) (2020).

Discrimination, exclusion and manipulation

The OAIC's 2020 ACAP survey found 89 per cent of respondents were uncomfortable or very uncomfortable with online businesses like social media sites targeting advertising based on what they have said and done online.¹⁷⁶⁶ elevenM expressed concern about the creation of detailed behavioural, demographic or interest-based profiles and the tailoring of offers or services to these profiles in ways that might be unfair or adversely impact the individual, such as denial of service or preferential pricing.¹⁷⁶⁷

The CDEI Online Targeting Report highlighted the role which targeting can play in facilitating unlawful discrimination, and cited instances of targeting on Facebook which excluded individuals from housing, employment and financial services advertisements on the basis of their sex, age and ethnicity.¹⁷⁶⁸ It noted comments by the UK Parliament's Joint Select Committee on Human Rights that 'the targeting of content online means that people have no way of knowing how what they see online compares to what others see - and therefore whether they have been discriminated against, and on what basis'.¹⁷⁶⁹

The Digital Services Act (DSA), which will regulate targeted advertising in European Union countries, recognises the particularly serious negative effects which can occur when individuals are presented with advertisements based on targeting techniques optimised to match their interests and potentially appeal to their vulnerabilities.¹⁷⁷⁰ It acknowledges that manipulative techniques can negatively impact entire groups and amplify social harms, for example by contributing to disinformation campaigns or by discriminating against certain groups.¹⁷⁷¹ For this reason, providers of online platforms will be prohibited from presenting advertisements based on profiling, using GDPR special categories of personal data, including by using profiling based on those special categories.¹⁷⁷²

The DSA outlines four categories of systemic risks, including (1) the dissemination of illegal content, (2) the impact on the exercise of fundamental rights (e.g. freedom of expression, media freedom and pluralism, the right to private life, data protection, the right to non-discrimination, the rights of the child and consumer protection), (3) negative effects on democratic processes, civic discourse and electoral processes and (4) negative effects on the protection of public health, minors and serious negative consequences to the person's physical and mental wellbeing, or on gender-based violence.

Submitters expressed concern that targeting impacts democracy by inhibiting informed political debate and restricting voters' ability to make freely informed decisions¹⁷⁷³ and suggested political targeting can be manipulative¹⁷⁷⁴ and exploit individual beliefs and fears.¹⁷⁷⁵ The CDEI Report noted the concern that targeting may contribute to polarisation within society as a result of individuals only seeing information and opinions that mirror their own which may harden their opinions and prevent them from experiencing narratives and ideas which run counter to their own.¹⁷⁷⁶ The ACCC considered that targeting of groups based on highly specific categories can be used to inflame societal tensions.¹⁷⁷⁷

¹⁷⁶⁶ OAIC, [Australian Community Attitudes to Privacy Survey 2020](#) (2020) 29.

¹⁷⁶⁷ Submission to the Discussion Paper: [elevenM](#), 45. See also Submissions to the Discussion Paper [Calabash Solutions](#), 18; [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 23. [Office of the Victorian Information Commissioner](#), 7-8; [Financial Rights Legal Centre and Financial Counselling Australia](#), 16 and Submissions to the Issues Paper: [Office of the Victorian Information Commissioner](#), 2-3; [Salinger Privacy](#), 23.

¹⁷⁶⁸ Centre for Data Ethics and Innovation (UK), [Online targeting: Final report and recommendations](#) (2020).

¹⁷⁶⁹ *Ibid.*

¹⁷⁷⁰ [Digital Services Act 2022](#) (EU) recital 69, art 26.

¹⁷⁷¹ *Ibid.*

¹⁷⁷² *Ibid.*

¹⁷⁷³ Submissions to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 7; [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#); 3; [Castan Centre](#), 13; [Digital Rights Watch](#), 18; [Professor David Lindsay](#), 17; [Reset Australia](#), 3; [DIGI](#), 2; [Michael Douglas, UWA Law School](#), 2.

¹⁷⁷⁴ Submissions to the Discussion Paper: [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#); 3; [Castan Centre](#), 15; [Digital Rights Watch](#), 18; [Professor David Lindsay](#), 17; [Reset Australia](#), 3; [DIGI](#), 2.

¹⁷⁷⁵ Submission to the Discussion Paper: [elevenM](#), 74.

¹⁷⁷⁶ Centre for Data Ethics and Innovation (UK), [Online targeting: Final report and recommendations](#) (2020); Centre for Data Ethics and Innovation (UK) [Landscape Summary: Online Targeting](#) (2020) citing Lisa Maria Neudert and Nahema Marchal [Polarisation and the use of technology in political campaigns and communication](#) European Parliament (2019) 16.

¹⁷⁷⁷ ACCC, [DPI Report](#), 446.

Exploitation of people experiencing vulnerability and children

Targeting can reinforce existing preferences and shape new ones – the risk that targeting poses to autonomy is more significant for people who may be vulnerable.¹⁷⁷⁸ Content recommendation systems may service increasingly extreme content because a person has viewed similar material (e.g. content related to self-harm or eating disorders).¹⁷⁷⁹ Targeting systems that seek to optimise user engagement have been shown to prioritise controversial, shocking or extreme content that produces emotional responses.¹⁷⁸⁰

The ACCC *Digital Platform Services Inquiry Interim Report No. 5 – Regulatory reform* (DPS Interim Report No 5) found that targeting systems have allowed for the more effective targeting of scams, which may result in substantial financial loss.¹⁷⁸¹ This is because the extensive data collected by digital platforms may provide scammers with the tools to target scams to certain vulnerable consumer groups, based on attributes those groups share. It highlighted that, in 2021, Indigenous Australians, older Australians and people from culturally and linguistically diverse communities and people with disability reported record high losses to scams.¹⁷⁸²

The DSA notes that specific groups or persons may be vulnerable or disadvantaged in their use of online services because of their gender, race or ethnic origin, religion or belief, disability, age or sexual orientation. The House of Representatives Select Committee on Social Media and Online Safety observed that content produced online has the capacity to encourage or promote destructive or unhealthy behaviours for vulnerable users. The eSafety Commissioner's submission to the committee pointed to examples of self-harm, suicide and eating disorders as topics which fall under this category.¹⁷⁸³ Harms can also arise through the spread of misinformation, disinformation, or encouraging mistrust in government institutions.¹⁷⁸⁴ These harms may be amplified when promoted through content recommendation systems.

The ACCC's Adtech report noted that ad tech providers and other digital platforms have broad discretions to collect and use consumers' data without consent (or potentially without consumers understanding fully what they consented to when they used a service or made a transaction). This can give rise to consumer harms through the delivery of highly personalised and targeted advertisements to vulnerable consumers, including children, for alcohol, gambling, or unhealthy food and beverages and encouraging user interfaces which encourage addiction and pose risks to personal security and safety of children.¹⁷⁸⁵

A submission by Reset Australia reflecting the views of children and young people to the draft OP Bill cited a young person as stating:

When I started using Instagram more, the platform collected enough data to know I'm a young woman, and began targeting me with fashion, beauty, and fitness content. My feed became flooded with that type of content, and then, I started receiving more dieting and cosmetic procedure videos.¹⁷⁸⁶

The DSA states that when assessing the risks to the rights of the child, providers should consider, for example, how easy it is for minors to understand the design and functioning of the service, as well as how minors can be exposed through their service to content that may impair minors' health, physical, mental and moral development.¹⁷⁸⁷ Such risks may arise, for example, in relation to the design of online interfaces which exploit the weaknesses and inexperience of minors or which may cause addictive behaviour.¹⁷⁸⁸

¹⁷⁷⁸ Centre for Data Ethics and Innovation (UK), [Online targeting: Final report and recommendations](#) (2020) citing Christopher Burr, Nello Cristianini and James Ladyman, 'An analysis of the interaction between intelligent software agents and human users' (2018) 28 *Minds and Machines* 735 and Daniel Susser, Beate Roessler and Helen Nissenbaum 'Online Manipulation: Hidden Influences in a Digital World' (2019) 4 *Georgetown Law Technology Review* 1.

¹⁷⁷⁹ Centre for Data Ethics and Innovation (UK), [Online targeting: Final report and recommendations](#) (2020).

¹⁷⁸⁰ Ibid.

¹⁷⁸¹ ACCC, [Digital Platform Services Inquiry: Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services](#) (2022) 45.

¹⁷⁸² Ibid 48.

¹⁷⁸³ eSafety Commissioner, [Inquiry into Social Media and Online Safety](#) (2022) 26.

¹⁷⁸⁴ House of Representatives Select Committee on Social Media and Online Safety, [Social Media and Online Safety](#) (2022).

¹⁷⁸⁵ ACCC, [Digital Advertising Services Inquiry: Final Report](#) (2021), 40.

¹⁷⁸⁶ Submission to OP Bill: [Reset Australia](#), 2.

¹⁷⁸⁷ ACCC, [Digital Advertising Services Inquiry: Final Report](#) (2021), 40.

¹⁷⁸⁸ Ibid.

Benefits of targeting

Submitters to the Review also highlighted the benefits of targeting. IAB submitted that targeted advertising brings enormous economic benefits to small businesses and Australian consumers.¹⁷⁸⁹ Others noted that targeted advertising is important for businesses in the digital economy because it allows businesses to direct advertising to the customers most likely to purchase their goods and services, and consumers see advertisements for goods and services that are more relevant to their interests.¹⁷⁹⁰ Targeting can lead to lower marketing costs for businesses by reducing wastage of advertisements served to disinterested consumers.¹⁷⁹¹ Under competitive market conditions, some of these cost savings could translate into lower prices for consumers.¹⁷⁹²

Snap Inc. submitted that behavioural advertising is also a critical component of many online platforms' business models.¹⁷⁹³ Targeted advertising allows online platforms to generate revenue which enables entities to provide consumers with access to content or services for free or at a reduced cost.¹⁷⁹⁴ Optus pointed to evidence of the growing importance of personalisation as a point of differentiation in service delivery to meet consumers' expectations,¹⁷⁹⁵ and that consumers are increasingly in favour of more personalised services and expect companies to deliver a more personalised experience and offerings.¹⁷⁹⁶ The ability of targeting to predict where people may be susceptible or vulnerable to particular harms can also be used to prevent them from seeing potentially harmful content.¹⁷⁹⁷

While noting the need for future research into how decisive targeting techniques are in shaping or changing political preferences and voting behaviour, the CDEI Online Targeting Report noted that targeting may increase voter engagement by connecting voters to the issues that matter to them.¹⁷⁹⁸

20.3.4 Viability of ad-supported services

Some submitters raised particular concerns about the impact of proposals affecting targeted advertising on ad-supported platforms.¹⁷⁹⁹ The Interactive Games and Entertainment Association submitted that while ad-supported platforms are free to access, they are not free to develop or maintain – to provide a customisable player experience, game publishers rely on data analysis and tailored advertising.¹⁸⁰⁰ Meta submitted that ad-supported services provide significant value to users and businesses. Nine submitted that media should be permitted to continue to provide media content in exchange for receipt of advertising and that without this value exchange, the public would not have free access to multiple Australian media organisations' content.¹⁸⁰¹ The submission further noted that access to multiple voices is important for a healthy democracy, economy and society.¹⁸⁰²

IAB and Meta submitted that if a consumer objects to their personal information being collected, used or disclosed for targeted advertising it should be possible for entities to no longer offer the service.¹⁸⁰³ This was said to be because an organisation should not have to fundamentally change its business model (which in turn affects the business models of its advertising customers) in order to respond to a consumer objection.¹⁸⁰⁴ Meta suggested that any right to object should explicitly clarify this as it would enable users to 'make an appropriately informed decision as to whether the value they derive from the service outweighs any actual or perceived cost to their privacy from accepting personalised ads'.¹⁸⁰⁵

¹⁷⁸⁹ Submission to the Discussion Paper: [IAB](#), 25.

¹⁷⁹⁰ Submissions to the Discussion Paper: [Australian Collectors and Debt Buyers Association](#), 8; [Experian](#), 18; ACCC, [Digital Advertising Services Inquiry: Final Report](#) (2021), 40.

¹⁷⁹¹ Federal Trade Commission (US), [A Brief Primer on the Economics of Targeted Advertising](#) (2020) 6.

¹⁷⁹² Ibid.

¹⁷⁹³ Submission to the Discussion Paper: [Snap Inc.](#), 7.

¹⁷⁹⁴ Submissions to the Discussion Paper: [Meta](#), 38-39; [IGEA](#), 11; [Nine](#), 14.

¹⁷⁹⁵ Submissions to the Discussion Paper: [Optus](#), 6. McKinsey & Company, [The value of getting personalization right--or wrong--is multiplying](#) (Web Page, 12 November 2021).

¹⁷⁹⁶ Ibid.

¹⁷⁹⁷ Centre for Data Ethics and Innovation (UK), [Online targeting: Final report and recommendations](#) (2020).

¹⁷⁹⁸ Centre for Data Ethics and Innovation (UK), [Landscape Summary: Online Targeting](#) (2019) 37 citing Samuel C Woolley and Philip N Howard, *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (Oxford University Press, 2018) and Kate Connolly, 'Angela Merkel: internet search engines are "distorting perception"' *The Guardian* (28 October 2016).

¹⁷⁹⁹ Submissions to the Discussion Paper: [DIGI](#), 21.

¹⁸⁰⁰ Submissions to the Discussion Paper: [IGEA](#), 11.

¹⁸⁰¹ Submissions to the Discussion Paper: [Nine](#), 13-14.

¹⁸⁰² Ibid.

¹⁸⁰³ Submissions to the Discussion Paper: [Meta](#), 39, [IAB](#), 25.

¹⁸⁰⁴ Submissions to the Discussion Paper: [Meta](#), 39.

¹⁸⁰⁵ Ibid, 41.

Other submitters took the view that the consequences of objecting to use of personal information for advertising must not include that the organisation will cease to provide the same good or service, unless the provision of marketing is the primary good or service provided, and this is clearly identified to the individual.¹⁸⁰⁶ The Foundation for Alcohol Research and Education submitted that the notification of consequences of not consenting should not mislead people to believe that consent to data processing for marketing is required for a service to function optimally (e.g. if a person wishes to use location data for service functioning but does not want their location data used for marketing, this should be enabled).¹⁸⁰⁷ Dr Katharine Kemp submitted that the provision of a free service should not justify an organisation giving itself a 'blank cheque' for advertising purposes.¹⁸⁰⁸

20.3.5 The relationship between targeting, profiling and trading

Targeting systems often rely on profiling, which is defined in the GDPR as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.¹⁸⁰⁹ Profiling can be used to suggest or serve content to users, to determine where, when and how frequently that content should be served, to encourage users towards particular behaviours, or to identify users as belonging to particular groups.¹⁸¹⁰

Experian submitted that not all profiling is intrusive and harmful. Many businesses 'profile' their customer base for the purpose of understanding their customers in an aggregated form.¹⁸¹¹ This is done to understand who is most likely to consume the business' products and services.¹⁸¹² Profiling can also be used for other purposes such as the personalisation of services, predicting the likelihood that certain medical treatments will be successful, to help establish or estimate the age of a user, for child protection, counter terrorism, or the prevention of crime.¹⁸¹³ Telstra suggested personal information collected to create profiles of individuals and groups for the purposes of research, analytics, product development and network assurance should not be captured by reforms.¹⁸¹⁴

Profiles are usually based on an individual's past online behaviour – they can be created using information about an individual's internet activity and inferences about an individual based on this activity. Information is collected, inferred and combined into digital profiles by data brokers, online platforms and other actors within the online advertising ecosystem, often through trading in information about individuals.¹⁸¹⁵ Entities can combine information about individuals from a variety of sources to build more accurate profiles.¹⁸¹⁶ The trade of information relating to individuals can facilitate the building of more detailed profiles.

Data brokerage services

Data brokerage services are organisations whose business model is based on trading in information relating to individuals including personal information and deidentified information. They specialise in the collection of information about individuals from a variety of online and offline sources, which the data broker combines for the purposes of providing services to other firms.¹⁸¹⁷ Data brokers generally do not collect information directly from consumers.¹⁸¹⁸ Information collected and combined by data brokers may include:

- internet search and browsing history
- browsing behaviour, including hovering, scroll speed and clicking
- customer loyalty scheme transaction data
- online and offline purchase histories
- email communications and online chats
- social media data, including posts, comments, connections and profile information
- apps installed and app usage, including frequency and duration of use, and biometric data recorded by the app

¹⁸⁰⁶ Submissions to the Discussion Paper: [Foundation for Alcohol and Research Education](#), 19; [Public Health Association Australia](#), 10; [Obesity Policy Coalition](#), 14.

¹⁸⁰⁷ Submissions to the Discussion Paper: [Foundation for Alcohol and Research Education](#), 19.

¹⁸⁰⁸ Submissions to the Discussion Paper: [Dr Katharine Kemp, UNSW Sydney](#), 18.

¹⁸⁰⁹ GDPR art 4(4).

¹⁸¹⁰ UK ICO, [Profiling](#) (Web Page).

¹⁸¹¹ Submissions to the Discussion Paper: [Experian](#), 18.

¹⁸¹² Ibid.

¹⁸¹³ UK ICO, [Profiling](#) (Web Page); UK ICO, [What is automated decision-making and profiling?](#) (Web Page).

¹⁸¹⁴ Submissions to the Discussion Paper: [Telstra](#), 20.

¹⁸¹⁵ Centre for Data Ethics and Innovation (UK), [Online targeting: Final report and recommendations](#) (2020).

¹⁸¹⁶ Submissions to the Discussion Paper: [Deloitte Australia](#), 5.

¹⁸¹⁷ Kayleen Manwaring, Katharine Kemp and Rob Nicholls, [\[Mis\]informed Consent in Australia](#) (2021) 96.

¹⁸¹⁸ UK ICO, [Investigation into data protection compliance in the direct marketing data broker sector](#) (2020) 12.

- location data, including GPS, WIFI, IP address, Bluetooth;
- consumer survey responses and online 'quiz' or 'personality test' responses,
- internet of things (IoT) logs
- data from wearable devices, such as 'smart watches' and fitness devices
- unique identifiers associated with the consumers' collection of devices
- publicly available census data, electoral rolls, property records and court records, and
- credit information, including loan applications, loan repayment histories, loan defaults.¹⁸¹⁹

This information can be combined to create a highly detailed profile of an individual. Data brokers often market their ability to provide a 'single customer view' or a '360 view' of individual customers.¹⁸²⁰ Data brokers sell information about individuals to a wide range of actors including marketers, insurers and political parties.¹⁸²¹ The consumer profile may include, or permit inferences about, the consumer's age, gender, relationship status, pregnancy, children, income, health issues, financial position, property ownership, purchasing intentions, sexual orientation, sexual activity, drug use, alcohol consumption, psychological biases, political views, religious affiliations, ethnicity, consumption preferences and personality predictions.¹⁸²² In addition to profiling, brokers may create consumer segments or 'audiences' based on attributes, interests and purchasing intentions. Data brokers can trade in personal or deidentified information, however concerns have been raised about the ability for deidentified data to be accurately re-identified.¹⁸²³

Customer loyalty schemes

Customer loyalty schemes collect information about consumers including their demographic data, transaction history, interests, preferences, consumption patterns, buying behaviour and habits. Consumer data is primarily collected, analysed and used to generate consumer insights to retain existing customers and obtain new ones; for business improvement and product development purposes; to personalise products and services; and for targeted advertising. Some schemes generate additional revenue by selling de-identified insight reports to third parties and advertising to their membership on behalf of third parties.¹⁸²⁴ In addition, loyalty schemes may share consumer data with data brokers.¹⁸²⁵ It is estimated that almost 90 per cent of Australian consumers are a member of a customer loyalty scheme.¹⁸²⁶

Combining loyalty program customer data with data from external sources allows loyalty schemes to know more about a member's lifestyle, interests and social attitudes.¹⁸²⁷ The data collected includes metadata such as age, gender and address, and transactional data describing store-visiting and product-buying characteristics, spending patterns and timestamps of when interactions occur. The data can also help loyalty schemes identify a member's preferences, consumption patterns, buying behaviour and habits.¹⁸²⁸

Privacy harms of trading

Trading in personal information can result in harm to individuals when they are not provided with sufficient transparency and control in relation to how their information is shared. The Consumer Policy Research Centre's 2020 Data and Technology Consumer Survey found that 60 per cent of respondents were uncomfortable with companies sharing their personal information with third parties for purposes other than delivering products and services they had signed up for.¹⁸²⁹ A recent CHOICE consumer survey indicated 40 per cent of respondents were not aware that customer loyalty schemes share data with data brokers and 70 per cent said they were concerned or very concerned about the sale of their data.¹⁸³⁰

In 2020, the Federal Court ordered HealthEngine to pay \$2.9 million in penalties for engaging in misleading conduct which included sharing patients' personal information to private health insurance brokers.¹⁸³¹ Between 2014 and

1819 Kayleen Manwaring, Katharine Kemp and Rob Nicholls, *[Mis]informed Consent in Australia* (2021) 96–97; DMA, *GDPR for marketers: profiling* (2018) 6.

1820 Ibid 97.

1821 Digital Rights Watch, *Watchlist: data brokers* (Web Page, 18 October 2018).

1822 Kayleen Manwaring, Katharine Kemp and Rob Nicholls, *[Mis]informed Consent in Australia* (2021) 97.

1823 The Conversation, *'How the shady world of the data industry strips away our freedoms'* (Web Page, 14 August 2020); ACCC, *Customer loyalty schemes: Final report* (2019) 78.

1824 ACCC, *Customer loyalty schemes: Final report* (2019) 51.

1825 Ibid 52, Sue Mitchell *'Woolworths doubles down on data, takes control of Quantum'* *Australian Financial Review* (20 April 2021); Sue Mitchell *'Woolworths hands data sharing contracts to Quantum, Nielsen'* *Australian Financial Review* (4 October 2018).

1826 ACCC, *Customer loyalty schemes: Final report* (2019) 6.

1827 Ibid 48.

1828 Ibid 47.

1829 Submissions to the Discussion Paper: *Consumer Policy Research Centre*, 8; Consumer Policy Research Centre *'2020 Data and Technology Consumer Survey'* (December 2020) 17.

1830 CHOICE, *What are loyalty schemes like Flybuys and Everyday Rewards doing with your data?* (Web Page, 20 December 2021).

1831 ACCC, *HealthEngine to pay \$2.9 million for misleading reviews and patient referrals* (Web Page, 20 August 2020).

2018, HealthEngine shared non-clinical personal information of over 135,000 patients with third party private health insurance brokers without adequately disclosing this to consumers. An investigation by the UK ICO in 2020, which resulted in enforcement action against Experian, found that various credit reference agencies were trading, enriching and enhancing people's personal data without their knowledge. This processing resulted in products which were used by commercial organisations, political parties or charities to find new customers, identify the people most likely to be able to afford goods and services, and build profiles about people.¹⁸³²

Dr Katharine Kemp submitted that the transfer of personal information to third parties in ad tech supply chains 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.¹⁸³³ The Consumer Action Law Centre submitted that entities should be required to clearly state whether information is shared with or sold with third parties.¹⁸³⁴ Other submitters raised concerns that it would be impractical to list all third parties in a privacy policy.¹⁸³⁵

In its Customer Loyalty Scheme final report, the ACCC expressed particular concern about loyalty schemes collecting, using and disclosing consumer data in ways that do not meet consumers' expectations, including:¹⁸³⁶

- seeking broad consents from, and making vague disclosures to, consumers about the collection, use and disclosure of their data
- 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 on behalf of loyalty schemes.

The ACCC recommended that loyalty schemes should continue to take steps to improve the transparency of their data practices and the ability of consumers to control how their data is collected, used and disclosed.¹⁸³⁷ Several customer loyalty schemes made improvements to their information handling practices during the course of the ACCC's review.¹⁸³⁸

A number of submitters suggested that customer loyalty schemes can offer tangible benefits to consumers¹⁸³⁹ and that individuals make a choice as to whether the benefits offered by the scheme are commensurate to the participation in the scheme.¹⁸⁴⁰ The Shopping Centre Council of Australia suggested the primary purpose of customer loyalty schemes is to provide a tailored experience to existing customers and that engagement with a customer loyalty scheme is entirely voluntary and governed by clear and explicit terms and conditions.¹⁸⁴¹ For participating in a loyalty scheme, consumers are offered discounts, rewards, tailored communications and promotions. In exchange, businesses derive value from consumers by collecting data, including personal information about them.¹⁸⁴² However, submissions generally took the view that customer loyalty schemes should not be regulated differently or separately.¹⁸⁴³

Current regulation of trading

The OAIC notes that trading in personal information generally means buying, selling or bartering personal information.¹⁸⁴⁴ APP 3.6 provides that an organisation must collect personal information about an individual only from the individual unless it is unreasonable or impracticable to do so.¹⁸⁴⁵ OAIC guidance states considerations relevant to whether it is unreasonable or impracticable to collect personal information from the individual include whether the individual would reasonably expect personal information about them to be collected directly from them or another source, and whether direct collection would jeopardise the integrity of the purpose of collection or the integrity of the personal information collected.¹⁸⁴⁶ Dr Katharine Kemp has noted the words 'unreasonable' and 'impracticable' are not defined in the Act and have not been considered in the context of trading in personal information.¹⁸⁴⁷

1832 UK ICO, [Investigation into data protection compliance in the direct marketing data broker sector](#) (2020) 2.

1833 Submissions to the Issues Paper: [Dr Katharine Kemp](#), 13.

1834 Submissions to the Discussion Paper: [Consumer Action Law Centre](#), 2.

1835 Submissions to the Discussion Paper: [Insurance Council of Australia](#), 15.

1836 ACCC, [Customer loyalty schemes: Final report](#) (2019) 82.

1837 ACCC, [Customer loyalty schemes: Final report](#) (2019) 84.

1838 [Discussion Paper](#), 126.

1839 Submissions to the Discussion Paper: [Shopping Centre Council of Australia](#), 8; [Telstra](#), 22; [Pharmaceutical Society of Australia](#), 4.

1840 Submissions to the Discussion Paper: [Shopping Centre Council of Australia](#), 8; [Telstra](#), 22.

1841 Submissions to the Discussion Paper: [Shopping Centre Council of Australia](#), 5.

1842 ACCC, [Customer loyalty schemes: Final report](#) (2019) 47.

1843 Submissions to the Discussion Paper: [Foundation for Alcohol Research and Education](#), 21; [Telstra](#), 22; [Obesity Policy Coalition](#), 16; [Calabash Solutions](#), 19; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 9-12; [Consumer Policy Research Centre](#), 8; [CHOICE](#), 15.

1844 OAIC, [Trading in personal information](#) (Web Page).

1845 Privacy Act sch 1 APP 3.6(b).

1846 OAIC, [APP Guidelines](#) (July 2019) [3.65].

1847 Katharine Kemp, [Australia's forgotten privacy principle: why common 'enrichment' of customer data for profiling and targeting is unlawful](#) (2022) 9.

20.4 International approaches to regulating direct marketing, targeting and trading

20.4.1 European Union

Article 21 of the GDPR provides individuals with an absolute right to object to processing of their personal data for direct marketing, including profiling for the purposes of direct marketing.¹⁸⁴⁸ The UK ICO notes that it is an absolute right, which means there are no exemptions or grounds for an entity to refuse.¹⁸⁴⁹ The Irish Data Protection Commission's guidance states that 'direct marketing involves a person being targeted as an individual, and the marketer attempting to promote a product or service, or attempting to get the person to request additional information about a product or service'.¹⁸⁵⁰

The GDPR and ePrivacy Directive¹⁸⁵¹ regulate how entities can target in the EU. The ePrivacy Directive regulates the use of cookies or other tracking technologies, which can be used to create rich profiles on individuals which inform the serving of targeted content. Under the ePrivacy Directive, organisations must obtain consent before installation or use of cookies or other tracking technologies, unless they are necessary for the provision of the electronic communication services.

Under Article 6 of the GDPR, processing of personal data must have a lawful basis. The two relevant bases for targeting are where an individual has provided consent, or 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 which require protection of personal data, in particular where the data subject is a child. All processing of personal data, which includes personal data which have undergone pseudonymisation, must be lawful, fair and transparent.¹⁸⁵²

Where personal data has been collected through cookies or tracking technology for the purposes of targeting, in addition to requiring consent under the ePrivacy Directive before installing or using cookies or tracking technology, consent will likely be required to process this data. The European Data Protection Board considers that legitimate interests in these circumstances is unlikely to be an appropriate legal basis, as the targeting relies on the monitoring of individuals' behaviour across websites and locations using tracking technologies and there is an imbalance between the company's legitimate interest and the protection of users' fundamental rights.¹⁸⁵³ However, the European Data Protection Board considers that legitimate interest is likely to be a valid legal ground in relation to targeting on the basis of data directly provided by the data subjects.¹⁸⁵⁴ For example, information provided by a user on a social media profile such as age, gender, location.

In July 2022, the EU adopted the DSA alongside the Digital Markets Act (DMA). Once formally adopted by the Council of the EU, both Acts will be published in the EU Official Journal and enter into force twenty days after publication. The DSA will be directly applicable across the EU and will apply fifteen months after the entry into force or from 1 January 2024 (whichever comes later). Under the DSA, providers of online platforms must not present advertising based on profiling using personal data when they are aware with reasonable certainty that the recipient of the service is a minor, or using special categories of personal data (as defined in GDPR).¹⁸⁵⁵

The DSA will also require platforms to be transparent about how their content moderation and recommendation systems work in their terms of service and offer users alternative content recommendation systems that are not based on profiling.¹⁸⁵⁶ Platforms must also give users clear information about why they are targeted with an advertisement and how to change their advertisement settings. The DSA also seeks to regulate the use of dark patterns by prohibiting platforms from 'deceiving or nudging recipients of the service' and from 'distorting or impairing the autonomy, decision-making, or choice of the recipients of the service via the structure, design or functionalities of an online interface'.¹⁸⁵⁷ The GDPR does not include specific obligations for trading in personal data. Trading in personal data constitutes processing

1848 GDPR art 21(2) and (3); Submissions to the Discussion Paper: [OAIC](#), 147.

1849 UK ICO, [Right to object](#) (Web Page).

1850 Data Protection Commissioner (Ireland) [Rules for Direct Electronic Marketing](#) (Web Page).

1851 The ePrivacy Directive is a set of legal guidelines which sets out objectives for EU Member States to meet, which aims to "particularise and complement" the provisions of the GDPR with respect to the processing of personal data in the electronic communication sector.

1852 GDPR art 5 and 4(5); GDPR Recital 26.

1853 European Data Protection Board (EU) [Guidelines 8/2020 on the targeting of social media users](#) (2020) 16.

1854 Ibid 14–15.

1855 GDPR art 9. Special category data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (when used for identification purposes) and data concerning health, a person's sex life or sexual orientation.

1856 [Digital Services Act 2022](#) (EU) art 38

1857 Ibid art 25.

under the GDPR, for which organisations need to identify a lawful basis. In the data brokering context, the lawful bases that are generally referred to are consent and legitimate interests.¹⁸⁵⁸ Consent must be freely given, specific, informed and unambiguous. Legitimate interests is likely to be an appropriate basis for processing when organisations are using personal data in ways that individuals would reasonably expect and which have minimal privacy impact, or where there is a compelling justification for the processing.¹⁸⁵⁹ GDPR also requires entities to inform individuals about the collection and use of their personal data. This obligation applies to personal data collected directly from the individual and when it is collected from another source.¹⁸⁶⁰

20.4.2 United Kingdom

The requirements contained in the GDPR are mirrored in the UK GDPR. The Privacy and Electronic Communications Regulations (PECR) implement the ePrivacy Directive and apply to the use of cookies and other tracking technologies. The use of cookies and similar technologies are only permitted if a user has given consent and has been provided with clear information about the purposes for which the information collected is stored and accessed. The UK Government has proposed reforms that would remove the consent requirement for analytics cookies (treating these as ‘strictly necessary’ cookies), and remove the requirement for prior consent for all types of cookies ‘once automated technology is widely available to help users manage online preferences’ (i.e. browser-level global opt-out functionality).

The UK ICO Direct Marketing Detailed Guidance draft direct marketing code of practice states that ‘the GDPR applies to online advertising if you are processing personal data such as an individual’s name, account name or other similar information in the context of online advertising. However, even if you are targeting a particular user without knowing this sort of information, you still need to comply. This is because you are ‘singling out’ a particular user and profiling them, making that user ‘identified or identifiable, directly or indirectly’, particularly when compared to other information you or another person may obtain or possess. For example, this means that you must ensure that your processing is fair, lawful and transparent – this is particularly important if you are seeking to match an individual’s ‘online’ behaviours with their ‘offline’ life.’¹⁸⁶¹

The UK’s ongoing Online Advertising Programme consultation identifies that harms associated with online advertising can broadly be divided into harmful content of advertisements and harmful placement or targeting of advertisements (especially when harmful content is targeted at vulnerable groups). A lack of transparency and accountability are labelled as the two core factors driving the prevalence of these harms.

The Online Advertising Programme is considering three options:

1. self-regulatory: expanding the Advertising Standards Authority’s (ASA) scope to include intermediaries, publishers and platforms as well as advertisers
2. introducing a statutory regulator to support the self-regulatory approach: backstopping the ASA’s powers with a newly appointed statutory regulator that could enforce more stringent sanctions (e.g. following serious or repeated breaches), and
3. full statutory approach: appointing a statutory regulator that would put in place new measures and use statutory enforcement powers.¹⁸⁶²

The UK GDPR does not include specific obligations for trading in personal data. As noted above, trading in personal data is processing, for which organisations need to identify a lawful basis. In the data brokering context, the lawful bases generally referred to are consent and legitimate interests.¹⁸⁶³ The UK ICO draft direct marketing code of practice states that ‘profiling and enrichment activities must be done in a way that is fair, lawful and transparent. If you are considering using profiling or enrichment services you must ensure you have completed appropriate due diligence’¹⁸⁶⁴. It goes on to state, ‘If you are planning on selling or sharing personal data for direct marketing purposes you must ensure that it is fair and lawful to do so. You must also be transparent and tell people about the selling or sharing.’¹⁸⁶⁵

¹⁸⁵⁸ UK ICO, [Investigation into data protection compliance in the direct marketing data broker sector](#) (2020) 15.

¹⁸⁵⁹ Ibid.

¹⁸⁶⁰ Ibid.

¹⁸⁶¹ UK ICO, [Direct marketing code of practice Draft code for consultation](#) (2020), 88. Following consultation, the Information Commissioner’s Office has since published [Direct marketing guidance](#).

¹⁸⁶² Department for Digital, Culture, Media and Sport (UK) [Online Advertising Programme consultation](#) (2022).

¹⁸⁶³ UK ICO, [Investigation into data protection compliance in the direct marketing data broker sector](#) (2020) 15.

¹⁸⁶⁴ UK ICO, [Direct marketing code of practice Draft code for consultation](#) (2020) 4. Following consultation, the Information Commissioner’s Office has since published [Direct marketing guidance](#).

¹⁸⁶⁵ UK ICO, [Direct marketing code of practice Draft code for consultation](#) (2020), 5, 99-104.

20.4.3 Canada

The PIPEDA provides that organisations may only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. The knowledge and consent of the individual are also required for the collection, use and disclosure of personal information, except in certain circumstances.¹⁸⁶⁶ The purposes for which an individual's information is to be collected, used or disclosed must be explained in a clear and transparent manner. Individuals may provide express or implied consent, but should provide express consent for the collection, use or disclosure of sensitive information. Organisations shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of information beyond what is required to fulfil the explicitly specified and legitimate purposes.

The Office of the Privacy Commissioner of Canada's policy position on online behavioural advertising notes that online behavioural advertising should not be considered a term or condition for individuals to use the internet generally and that there are other forms of advertising that websites can rely on.¹⁸⁶⁷ There must also be meaningful consent, and there should be limitations on the types of information collected and used for profiling.

Implied consent may be reasonable if information is non-sensitive and individuals are well informed. Any collection or use of an individual's web browsing activity must be done with that person's knowledge and consent. Therefore, if an individual is not able to decline the tracking and targeting using an opt-out mechanism because there is no viable possibility for them to exert control over the technology used, or if doing so renders a service unusable, then organisations should not employ that type of technology.¹⁸⁶⁸ The consent of an individual is only valid if it is reasonable to expect that an individual to whom the organisation's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. The Canadian Privacy Commissioner noted that it is difficult to ensure meaningful consent from children to online behavioural advertising and suggested that for best practice, organisations should avoid tracking children and tracking on websites aimed at children.¹⁸⁶⁹

Trading in personal information constitutes a disclosure under the PIPEDA, for which consent must be obtained. As noted in Chapter 4, Canada's proposed Bill C-27 recognises a concept of de-identified information which is considered to be personal information and must be treated as such with the exception of data subject rights.¹⁸⁷⁰

20.4.4 United States

The state privacy laws of Colorado,¹⁸⁷¹ Virginia¹⁸⁷² and Utah¹⁸⁷³ allow consumers to opt out of the controller using the consumer's personal data in connection with targeted advertising. Targeted advertising means display advertisements to a consumer where the advertisement is selected and based on personal data obtained from that consumer's activities over time and across non-affiliated websites or online applications to predict such consumer's preferences or interests. Controllers must conduct a data protection assessment for targeted advertising and the sale of personal data. These states also allow consumers to opt-out of the sale of their personal data.

In California, consumers can opt-out of the sale of their personal information and the sharing of their personal information. Sharing means sharing, renting, releasing, disclosing, disseminating, making available or transferring a consumer's personal information by the business to a third party for cross-context behavioural advertising, whether or not for monetary or other valuable consideration.¹⁸⁷⁴ Cross-context behavioural advertising means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses or distinctly branded websites. Businesses must either provide a link on the business' homepage titled 'Do Not Sell or Share My Personal Information' or recognise 'opt-out preference signals' that are sent with the consumer's consent.¹⁸⁷⁵

¹⁸⁶⁶ *Personal Information Protection and Electronic Documents Act* (Canada) sch 1, 4.3.

¹⁸⁶⁷ Office of the Privacy Commissioner (Canada) [Policy position on online behavioural advertising](#) (2021).

¹⁸⁶⁸ Office of the Privacy Commissioner (Canada) [Guidelines on privacy and online behavioural advertising](#) (2021).

¹⁸⁶⁹ Office of the Privacy Commissioner (Canada) [Guidelines on privacy and online behavioural advertising](#) (2021).

¹⁸⁷⁰ Bill C-27 s 2(3).

¹⁸⁷¹ *Colorado Privacy Act* (Colorado, US) sections 6-1-1306 (1)(a)(I)(A) and (1)(a)(I)(B).

¹⁸⁷² *Consumer Data Protection Act* (Virginia, US) section 59.1-573.

¹⁸⁷³ *Utah Consumer Privacy Act* (Utah, US) subsection 13-61-201 (4).

¹⁸⁷⁴ *California Consumer Privacy Act of 2018* (California, US) § 1798.140 (ah)(1) and § 1798.120

¹⁸⁷⁵ *Ibid* § 1798.135.

20.5 Proposals

20.5.1 Need for reform

There is significant community concern about the potential for targeting to cause privacy harms and other associated harms. Advances in technology have facilitated the creation of profiles about individuals which may contain detail on varied characteristics such as financial status, political views, religious affiliations, sexual orientation and personality and behavioural traits. Profiles are created using datapoints collected from multiple sources, traded between entities to build a more complete picture of an individual. These profiles allow entities to make accurate predictions about the types of content an individual is likely to engage with. Targeting has the potential to cause significant harm when individuals have limited awareness of why and how they are being targeted and no control over it, and where targeted content and advertising may be used to manipulate, discriminate, exclude and exploit individuals based on their vulnerabilities. Conversely, targeting brings economic benefits in the form of funding digital platforms, boosting sales and can also be used for socially beneficial purposes, such as public health campaigns and to prevent individuals from being exposed to harmful content.

Where targeting involves the collection, use and disclosure of a broad range of information relating to an individual which may not meet the threshold of personal information, targeting which is not based on personal information is largely outside of the scope of the Act, despite the privacy risks posed to individuals.

However, where targeted content and advertising poses privacy risks to individuals and risks undermining other public interests, including the integrity of the democratic electoral process, there is merit to extending the application of the Act to a broader range of information in relation to this practice. This would be a better approach than extending the definition of personal information to include any information relating to an individual, given the implications for other uses of such information which do not pose risk of harm to individuals, including research and data analytics in a variety of contexts. In the context of targeting however, providing individuals with greater transparency and control and introducing measures to protect against harm should not depend on whether they are able to be distinguished from all others.

20.5.2 Proposal – define key concepts

Direct marketing

In response to concerns that the term ‘direct marketing’ is unclear, it is proposed that ‘direct marketing’ be defined in the Act. The definition would clarify that direct marketing is not limited to promoting goods or services, but also includes promoting the aims and ideals of any organisation.

Targeting

To clarify that targeting is distinct from direct marketing and uses a broader range of information relating to individuals, it is proposed that targeting be defined in the Act to capture the collection, use or disclosure of information relating to an individual, including personal information, deidentified information and unidentified information (discussed further in Chapter 4).¹⁸⁷⁶ In addition, in response to the risks posed by content recommendation systems, it is proposed that the definition of targeting capture the targeting of content that is beyond advertising. This would also address the potential complexity in distinguishing advertising material from organic content posted on a platform.

Trading

To provide clarity to entities, it is proposed that ‘trading’ in personal information be defined in the Act. Consistent with OAIC guidance, the definition would be broader than the sale of information. For example, a company exchanging their customer list in return for that of another entity would constitute trading in personal information.

¹⁸⁷⁶ Submissions to the Discussion Paper: [Salinger Privacy](#), 8-9; [Dr Henry Fraser](#), 2.

20.1 Amend the Act to introduce definitions for:

Direct marketing – capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material.

Targeting – capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class).

Trading – capture the disclosure of personal information for a benefit, service or advantage.

20.5.3 Proposal – give individuals more choice and control

Unqualified right to opt-out of use or disclosure of personal information for direct marketing

There was strong submitter support for the Discussion Paper proposal to introduce an unqualified right to object to direct marketing.¹⁸⁷⁷ Submissions noted there was a strong consumer appetite for regulating unsolicited marketing contact.¹⁸⁷⁸ Some submitters suggested a reasonableness limitation on the effort required to action a request.¹⁸⁷⁹ Telstra suggested the proposal should be refined to a right to object to use or disclosure of personal information and not extend to collection, noting that the use of personal information for marketing would not always be known at the point of collection unless direct marketing was the sole intended use of that information.¹⁸⁸⁰

In response to this feedback, it is proposed that individuals should have an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. While this right will generally apply to more traditional forms of direct marketing (such as communication via email or SMS), there are some circumstances where the use of personal information for targeting may reach the threshold of direct marketing. For example, the use of customer emails to target advertisements on social media to known individuals would fall within the definition of direct marketing. In these circumstances, if an individual had exercised their right to opt-out of the use and disclosure of their personal information for direct marketing, the entity would not be able to use that individual's personal information for targeted advertising. Further consultation will be required on how best to implement this proposal in these circumstances.

The opt out of personal information being used or disclosed for direct marketing purposes would be unqualified, meaning that an entity would have to stop using or disclosing personal information for direct marketing where a person exercised their right to opt out. Importantly, exercising the opt out should not be a barrier to service for individuals who elect to make this choice.

The Discussion Paper sought feedback on a proposal to repeal APP 7 in light of existing protections in the Act and other proposals for reform. Submitters had mixed views about whether APP 7 should be repealed.

¹⁸⁷⁷ Submissions to the Discussion Paper: [Energy and Water Ombudsman NSW](#), 3; [Energy and Water Ombudsman SA](#), 1; [Energy and Water Ombudsman Victoria](#), 1; [Energy and Water Ombudsman Queensland](#), 1; [Office of the Victorian Information Commissioner](#), 8; [Australian Council on Children and the Media](#), 8; [Australian Privacy Foundation](#), 12; [Centre for AI and Digital Ethics](#), 7; [Karlsgate](#), 1; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 8; [Equifax](#), 4; [CHOICE](#), 15; [OAIC](#), 147-148; [Privacy 108](#), 29; [Experian](#), 19; [Consumer Policy Research Centre](#), 8; [Obesity Policy Coalition](#), 14; [Graham Greenleaf](#), 5; [Consumer Action Law Centre](#), 2; [Public Health Association Australia](#), 10; [Financial Rights Legal Centre and Financial Counselling Australia](#), 16; [elevenM](#), 45; [Foundation for Alcohol Research and Education](#), 19-20; [ACCC](#), 6.

¹⁸⁷⁸ Submissions to the Discussion Paper: [Energy and Water Ombudsman NSW](#), 3; [Energy and Water Ombudsman SA](#), 1; [Energy and Water Ombudsman Victoria](#), 1; [Energy and Water Ombudsman Queensland](#), 1.

¹⁸⁷⁹ Submissions to the Discussion Paper: [Woolworths Group](#), 12-13; [Optus](#), 25-26.

¹⁸⁸⁰ Submission to the Discussion Paper: [Telstra](#), 20.

While a number of submitters supported the proposal,¹⁸⁸¹ there was strong opposition to the repeal of APP 7 from organisations that rely on fundraising.¹⁸⁸² These submitters noted that direct marketing is an essential channel in fundraising efforts and suggested the repeal of APP 7 would put an end to fundraising that relies on inferred consent.¹⁸⁸³ Submissions also expressed concern about the overlap between APP 7 and the requirements in the Spam Act and DNCR Act and suggested alignment between legislation to ensure consistency.¹⁸⁸⁴ The OAIC indicated that repealing APP 7 would help address these concerns.¹⁸⁸⁵

If APP 7 is repealed, the use and disclosure of personal information for direct marketing purposes and related activities would then be subject to the existing requirements contained in APP 6.¹⁸⁸⁶ This would be supplemented by the proposal to introduce a requirement that any collection, use or disclosure of personal information must be fair and reasonable in the circumstances (see Chapter 12).¹⁸⁸⁷ Removing APP 7 would recognise that its requirements would be largely replicated or strengthened through other proposals; the introduction of an unqualified right to opt-out of the 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.

Further consideration is required to determine how best to harmonise the requirements across the Privacy Act, Spam Act and DNCR Act. A key issue for consultation would be whether the current carve out in APP 7.8 for the *Interactive Gambling Act*, DNCR Act and Spam Act is still required. In addition, consultation will be required to determine if direct marketing should continue to be regulated through a separate APP, or if direct marketing should instead be subject to the requirements contained in APP 6. This would need to be considered alongside other proposals put forward in this chapter.

20.2 Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes.

Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.

Unqualified right to opt-out of receiving targeted advertising

The ACCC's DPI Report recommended that consumers who prefer to provide their personal information for targeted advertising purposes should be required to actively make this selection.¹⁸⁸⁸ Similarly, the UK Competition and Markets Authority study recommended online platforms give users more control by enabling consumers to use online platforms without requiring the use of data about them for personalised advertising and changing default settings to require an 'opt-in' rather than an 'opt-out' for personalised advertising.¹⁸⁸⁹ A number of submitters expressed support for requiring express consent for the collection, use and disclosure of personal information for targeting.¹⁸⁹⁰ ADMA

1881 Submissions to the Discussion Paper: [Western Union](#), 7; [Australian Communications Consumer Action Network](#), 14; [OAIC](#), 148; [Meta](#), 43; [elevenM](#), 48.

1882 Submissions to the Discussion Paper: [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 8-9; [World Animal Protection](#), 1; [Victor Chang Cardiac Research Institute](#), 1; [CARE Australia](#), 1; [Heart Research Australia](#), 1; [Association of Australian Medical Research Institutes](#), 5; [Garvan Institute of Medical Research and Garvan Research Foundation](#), 9-10.

1883 Submissions to the Discussion Paper: [World Animal Protection](#), 1; [Victor Chang Cardiac Research Institute](#), 1; [CARE Australia](#), 1; [Heart Research Australia](#), 1; [International Fund for Animal Welfare \(Australia\)](#), 2-4; [Garvan Institute of Medical Research and Garvan Research Foundation](#), 9-10.

1884 Submissions to the Discussion Paper: [Australian Banking Association](#), 25; [Commonwealth Bank of Australia](#), 3; [Privacy 108](#), 193; [ADMA](#), 30.

1885 Submission to the Discussion Paper: [OAIC](#), 148.

1886 Submissions to the Discussion Paper: [OAIC](#), 148; [Salinger Privacy](#), 32-33.

1887 Submissions to the Discussion Paper: [OAIC](#), 148; [Salinger Privacy](#), 32.

1888 ACCC, [DPI Report](#), 468.

1889 Competition and Markets Authority (UK) [Online Platforms and digital advertising: Market study final report](#) (2020) 380-381.

1890 Submissions to the Discussion Paper: [Dr Katharine Kemp, UNSW Sydney](#), 15; [Public Health Association Australia](#), 10; [Calabash Solutions](#), 18; [Foundation for Alcohol Research and Education](#), 19; [Obesity Policy Coalition](#), 14; [The Benevolent Society](#), 6; [Uniting Church, Synod of Victoria and Tasmania](#), 9; [Consumer Action Law Centre](#), 2; [Financial Rights Legal Centre and Financial Counselling Australia](#), 16; [Graham Greenleaf](#), 5.

recommended that marketing by third parties, or the use of second party or third party customer data via targeted advertising should be able to be done with an individual's consent.¹⁸⁹¹ Salinger Privacy suggested targeting should be significantly restricted unless done with an individual's consent.¹⁸⁹²

Submissions that supported requiring consent suggested that consent should be express, precise and unbundled and that withdrawing consent should be as easy as providing it.¹⁸⁹³ Submissions also suggested that requiring consent would provide individuals with greater control over their personal information.¹⁸⁹⁴ The Foundation for Alcohol Research and Education submitted that consent mechanisms must not be designed to nudge or coerce individuals to consent to the processing of their personal information through bundled consents, 'consent to all' options or through requiring consent to process personal information for marketing purposes to use a service.¹⁸⁹⁵

However, targeting often relies on 'de-identified' or 'unidentified' information relating to individuals. If consent was required to target, this would require consent for the collection, use or disclosure of de-identified or unidentified information, which would mean individuals would be inundated with consent requests, which would likely reduce the utility of consent by inducing consent fatigue.¹⁸⁹⁶ It may also be technically challenging for entities to comply with such a requirement when handling information about an unknown individual. Such a requirement would be similar to the EU's ePrivacy Directive which requires consent to the use of cookies or other tracking technologies.¹⁸⁹⁷ Feedback provided to the Review has consistently emphasised concerns about increasing consent requirements on the basis that consent is ineffective when overused due to consent fatigue.¹⁸⁹⁸ One way to reduce consent fatigue would be to only require consent to the collection, use and disclosure of *personal information* for targeting. However, this would mean individuals would still see targeted advertising based on information that does not amount to personal information, even if they do not wish to receive that targeted advertising.

A right for individuals to opt-out of receiving targeted advertising would be consistent with current industry practice and would provide the tangible benefit for individuals of stopping targeted advertising based on any information relating to them from being presented to them. Consistent with the IBA Guideline, individuals are able to opt-out of receiving targeted advertisements from Facebook, Google, Twitter and Instagram through 'account settings'. An opt-out of receiving targeted advertising would also recognise the potential impact of any reforms on ad-supported platforms. Individuals would be able to make a choice not to see targeted advertising, but platforms would be able to collect and use information relating to individuals for targeting purposes such as generating audience insights and targeting of similar users who have not elected to opt-out of receiving targeted advertising. However as noted above, where an individual had opted out of their personal information being used or disclosed for direct marketing, this would preclude the use or disclosure of their personal information for targeting that constituted direct marketing.

While a number of platforms already provide the ability for individuals to opt-out of receiving targeted or 'personalised' advertising, the ACCC has expressed concern about the ability for platforms to influence consumers to make certain choices by designing user interfaces that take advantage of certain psychological or behavioural biases.¹⁸⁹⁹ This is sometimes referred to as 'choice architecture'. The ACCC noted that choice architecture can be used to confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions.¹⁹⁰⁰ This form of choice architecture is referred to as 'dark patterns'. The ACCC has found that dark patterns can nudge consumers towards more privacy-intrusive options.¹⁹⁰¹

1891 Submission the Discussion Paper: [ADMA](#), 28.

1892 Submission the Discussion Paper: [Salinger Privacy](#), 32.

1893 Submissions the Discussion Paper: [Financial Rights Legal Centre and Financial Counselling Australia](#), 16; [Consumer Policy Research Centre](#), 8; [Calabash Solutions](#), 18; [Foundation for Alcohol Research and Education](#), 19; [Obesity Policy Coalition](#), 14; [Privacy 108](#), 31.

1894 Submissions the Discussion Paper: [Consumer Policy Research Centre](#), 8; [Deloitte Australia](#), 39.

1895 Submission the Discussion Paper: [Foundation for Alcohol Research and Education](#), 18.

1896 See [Discussion Paper](#), 131 regarding consent fatigue concerns in relation to the EU ePrivacy Directive. The proposed ePrivacy regulation to replace the ePrivacy Directive includes measures to address consent fatigue by providing for consent at the browser level: European Commission, [Proposal for an ePrivacy Regulation](#) (Web Page, 7 June 2022).

1897 Although consent to use tracking technology does not amount to consent to process the data obtained by tracking technology. Where information obtained through tracking technology constitutes 'personal data' it may only be processed under one of the GDPR lawful bases.

1898 Submissions the Discussion Paper: [Deloitte Australia](#), 39; [Avant Mutual](#), 3; [Australian Collectors and Debt Buyers Association](#), 8; [Insurance Council of Australia](#), 15; [Telstra](#), 21.

1899 ACCC, [Digital Platform Services Inquiry: Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services](#) [2022] 45.

1900 Ibid 45.

1901 Ibid 46.

OAIC guidance should clarify how entities can implement opt-out rights on their platforms. This guidance could have regard to the approach adopted in the DSA, which prohibits ‘repeatedly requesting a recipient of the service to make a choice where such a choice has already been made, ... or making certain choices more difficult or time-consuming than others, ... or by default settings that are very difficult to change, and so unreasonably bias the decision making of the recipient of the service, in a way that distorts and impairs their autonomy, decision-making and choice’.

Importantly, opting out of receiving targeted advertising should not be a barrier to service for individuals who elect to make this choice. Given the availability of other forms of advertising, such as contextual advertising, access to a service should not be made conditional on consenting to receiving targeted advertising. As noted above, this is consistent with the Office of the Privacy Commissioner of Canada’s policy position on online behavioural advertising, which notes that online behavioural advertising should not be considered a term or condition for individuals to use the internet generally and that there are other forms of advertising that websites can rely on.¹⁹⁰²

20.3 Provide individuals with an unqualified right to opt-out of receiving targeted advertising.

Require consent to trade in personal information

The Discussion Paper did not put forward specific proposals to regulate trading. However, in response to concerns raised about trading in personal information, it is proposed that entities be required to seek consent before trading in personal information. In order for consent to be voluntary, informed, current, specific and unambiguous, entities should provide individuals with information about the third parties that personal information will be shared with and the types of personal information that will be disclosed. Consultation with industry would be required to determine how these transparency obligations could be met. Individuals would have the right to withdraw consent at any time.

Requiring individuals’ consent to trade their personal information may impact competition where access to data can pose a barrier to entry for some digital platform services.¹⁹⁰³ The ACCC DPS Interim Report No 5 recommended introducing reforms which may oblige digital platforms to share data in certain circumstances. However, it expressly noted that any measures to enhance data sharing to address such barriers should be managed in light of privacy risks.¹⁹⁰⁴ Requiring consent would not prohibit digital platforms from sharing personal information, but it would ensure that individuals are informed and have agreed to the disclosure of their personal information to a third party.

Where consent to trade in personal information was made a condition of accessing goods or services, an APP entity may need to demonstrate that the trading of personal information is reasonably necessary for its functions or activities if an individual objected to their personal information being traded (refer Chapter 18). An entity’s trading of personal information would also have to be fair and reasonable in the circumstances. Consideration will need to be given to whether exceptions to the requirement for entities to seek consent to trade in personal information are required.

20.4 Introduce a requirement that an individual’s consent must be obtained to trade their personal information.

¹⁹⁰² Office of the Privacy Commissioner of Canada, [Policy position on online behavioural advertising](#) (Web Page, 13 August 2021).

¹⁹⁰³ ACCC, [Digital Platform Services Inquiry: Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services](#) (2022) 165.

¹⁹⁰⁴ Ibid.

20.5.4 Proposal - prevent harmful direct marketing, targeting and trading

Submissions to the Issues Paper proposed a number of possible prohibited practices, including profiling and behavioural advertising knowingly directed at children¹⁹⁰⁵ and 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.¹⁹⁰⁶ The Foundation for Alcohol Research and Education submitted that the extensive tracking, profiling and targeting of people for commercial marketing purposes is a major privacy concern, especially when it comes to children and other people who are vulnerable.¹⁹⁰⁷ CHOICE supported prohibiting the for-profit trade in personal information through data brokers.¹⁹⁰⁸

The Discussion Paper suggested certain practices could be prohibited through OAIC guidance interpreting the proposed fair and reasonable test, similar to the approach taken by the Office of the Privacy Commissioner of Canada. As discussed in Chapter 1, where warranted, the principles-basis of the Act should be supplemented by more prescriptive rules. Introducing specific prohibitions against the forms of targeting that pose the greatest risk of harm would be consistent with this approach and would retain the Act's principles-based approach for other forms of targeting. Prohibited practices are discussed further in Chapter 13.

Direct marketing to children

Submissions expressed concern about the marketing of harmful products to children.¹⁹⁰⁹ While these concerns mainly centred around targeted advertising and profiling, under APP 7 there are currently no specific restrictions on direct marketing to children. While some forms of direct marketing are unlikely to cause harm, such as a person under 18 signing up for a mailing list to be notified about new products, privacy harms may arise when a person under 18 receives unsolicited marketing materials from a business they have not provided their contact details to or if they receive direct marketing communication that advertises a harmful product. In response to these risks, direct marketing to persons under 18 should be prohibited unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests.

Chapter 12 considers how entities would determine whether an act or practice is in the best interests of the child in the context of the fair and reasonable test. Development of the proposed Children's Online Privacy Code would clarify what is meant by the best interests of the child for direct marketing provided digitally. The OAIC could also provide guidance to support entities when determining whether direct marketing material is in the child's best interests. For example, if a person under 18 provides their contact details to an activewear brand when making a purchase, it would likely be in that child's best interests to receive communication from that company about new products or discounts, provided the child can opt-out of receiving this communication. However, if the activewear brand expanded their range of products to include diet supplements, it would likely not be in the child's best interests to receive direct marketing communication advertising these products.

20.5 Prohibit direct marketing to a child unless the personal information used for the direct marketing was collected directly from the child and the direct marketing is in the child's best interests.

1905 Submissions to the Issues Paper: [Data Synergies](#), 4; [OAIC](#), 91; [Salinger Privacy](#), 23; [Obesity Policy Coalition](#), 9.

1906 Submission to the Issues Paper: [Consumer Policy Research Centre](#), 12.

1907 Submission to the Discussion Paper: [Foundation for Alcohol Research and Education](#), 18.

1908 Submission to the Discussion Paper: [CHOICE](#), 13.

1909 Submissions to the Discussion Paper: [OAIC](#), 119-121; [Castan Centre](#), 22-23; [UNSW Allens Hub](#), [Deakin CSRI](#) and [IEEE SSIT](#), 9; [Obesity Policy Coalition](#), 1; [Foundation for Alcohol Research and Education](#), 8. See also [CHOICE](#), 12 and [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 12.

Targeting children

A number of submissions supported a prohibition on targeting children.¹⁹¹⁰ This is consistent with UNCRC General Comment 25 that 'States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes...'.¹⁹¹¹ A VicHealth report which examined online advertising of harmful products to children found 'there are little or no protections in place to prevent Australia's children from predatory marketing practices in the digital world'.¹⁹¹² The report noted that children are more susceptible to marketing messages the younger they are¹⁹¹³ and cited an estimate that 72 million data points will be collected on a child by the age of 13.¹⁹¹⁴

The ACCC's DPI Report recommended restrictions on the collection, use or disclosure of children's personal information for targeted advertising or online profiling.¹⁹¹⁵ A research paper commissioned by the OAIC authored by Normann Witzleb and Moira Paterson notes that children are vulnerable online due to limitations in their basic and digital literacy, their cognitive abilities and their capacity for mature decision-making.¹⁹¹⁶ The paper raised concerns about the potential for online marketing to result in manipulation and to impair children's decisional autonomy.¹⁹¹⁷

The UNCRC has highlighted the risks to children resulting from automated processes of information filtering, profiling and marketing and decision-making to supplant, manipulate and interfere with the ability of children to form and express their own opinions online.¹⁹¹⁸ It also noted that behavioural targeting may lead to arbitrary or unlawful interference with children's right to privacy and may have adverse consequences which can continue to affect them at later stages of their lives.¹⁹¹⁹

The Discussion Paper noted that 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. This was noted by the UNCRC which stressed the important function which digital and online content perform in enabling children to realise the right to access to information.¹⁹²⁰ The OAIC also noted the need for appropriate exceptions to any prohibition to ensure that services that are beneficial to children and pose little privacy risk are not prohibited.¹⁹²¹

In light of the risks which targeting poses to children, targeting to a child (defined as an individual who has not reached 18 years of age as per proposal 16.1) should be prohibited with an exception for targeting that is in the best interests of the child. This is consistent with UNCRC General Comment 25 where it stated that 'States parties should make the best interests of the child a primary consideration when regulating advertising and marketing addressed to and accessible to children'.¹⁹²² OAIC guidance and industry consultation in the development of the Proposed Children's Online Privacy Code would play an important role in determining how to apply this test in the context of online targeting.

The DSA includes a prohibition against presenting advertisements based on profiling using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor.¹⁹²³

The DSA further provides that compliance with the prohibition shall not oblige providers to process additional personal data in order to assess whether the recipient of the service is a minor.¹⁹²⁴ The proposed prohibition against targeting to persons under 18 would need to include a similar provision.

1910 Submissions to the Discussion Paper: OAIC, 107; Castan Centre, 22-23; UNSW Allens Hub, Deakin CSRI and IEEE SSIT, 9; Obesity Policy Coalition, 15; Foundation for Alcohol Research and Education, 5. See also CHOICE, 12 and Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise, 12.

1911 United Nations Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment* (2 March 2021) [42].

1912 VicHealth, *Under the radar: Harmful industries' digital marketing to Australian children* (2022) 2.

1913 Ibid 11.

1914 Ibid 8.

1915 ACCC, *DPI Report* 464.

1916 Normann Witzleb et al, *Privacy risks and harms for children and other vulnerable groups in the online environment* (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 22; Submission to the Discussion Paper: OAIC, 99.

1917 Normann Witzleb et al, *Privacy risks and harms for children and other vulnerable groups in the online environment* (Research Paper commissioned by the OAIC, Monash University and elevenM Consulting, 18 December 2020) 33.

1918 United Nations Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment* (2 March 2021) [61].

1919 Ibid [68].

1920 Ibid [50].

1921 Submission to the Discussion Paper: OAIC, 103.

1922 United Nations Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment* (2 March 2021) [41].

1923 *Digital Services Act 2022* (EU) art 24b(1b).

1924 Ibid art 24b(2).

20.6 Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.

Trading in children's personal information

As noted above, targeting is driven by profiling, which often relies on the combining of data points from multiple sources. The ACCC's DPI Report noted that targeted advertising has become more prevalent and more granular as the collection of data and sophistication of data analysis has increased.¹⁹²⁵ The combination of different data sets can enable businesses to draw insights not available when analysing the data they hold alone.¹⁹²⁶ A report released by Human Rights Watch raised concerns about the tracking and sharing of children's information by educational apps and websites.¹⁹²⁷ Children and Media Australia raised similar concerns following an audit of Android entertainment apps, which found 59 per cent of apps reviewed 'had some level of problematic data collection behaviour'.¹⁹²⁸ To support the prohibition against targeting to children, it is proposed that trading in the personal information of children also be prohibited. Further consultation will assist with determining if exceptions to this prohibition are required and how they should be framed.

20.7 Prohibit trading in the personal information of children.

Targeting which exploits vulnerability, manipulates, discriminates and excludes

Submitters expressed concern about the potential for people's vulnerabilities to be exploited by online targeting systems.¹⁹²⁹ The CDEI Online Targeting Report found there is an expectation that organisations using targeting systems should be held to account for harm they cause and a desire for individuals to be able to exercise more control over the way they are targeted.¹⁹³⁰ It noted that most people see the value of targeting, but they want to know that it being done safely and ethically.¹⁹³¹

Submitters to the Review have also expressed concerns about the risk that targeting poses to the integrity of the electoral process through lack of transparency eroding voters trust and confidence and the risk of voter manipulation.¹⁹³² Many stakeholders referenced the Facebook-Cambridge Analytica matter which involved the use of Facebook data matched with voter profiles to determine psychological patterns to target messages during the 2016 United States presidential election, in submitting that political entities¹⁹³³ in Australia should be required to comply with privacy protections.¹⁹³⁴

¹⁹²⁵ ACCC, [DPI Report](#), 392.

¹⁹²⁶ Ibid.

¹⁹²⁷ Human Rights Watch, "[How dare they peep into my private life?](#)" Children's rights violations by governments that endorsed online learning during the Covid-19 pandemic (Web Page, 25 May 2022).

¹⁹²⁸ Children and Media Australia, [Summary of pilot apps can track project 2021-22](#) (2022) 3.

¹⁹²⁹ Submissions to the Discussion Paper: [Energy and Water Ombudsman NSW](#), 3; [Office of the Victorian Information Commissioner](#), 6; [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 18-19; [Consumer Policy Research Centre](#), 5-6; [Salinger Privacy](#), 9-13; [Consumer Law Action Centre](#), 1 referring to Consumer Action Law Centre, [Dirty leads: consumer protection in online lead generation](#), (March 2018) 20-23.

¹⁹³⁰ Centre for Data Ethics and Innovation (UK), [Online targeting: Final report and recommendations](#) (2020).

¹⁹³¹ Ibid.

¹⁹³² Submissions to the Discussion Paper: [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 3; [Castan Centre](#), 12-15; [Digital Rights Watch](#), 18; [Professor David Lindsay](#), 17. See also [Reset Australia](#), 3.

¹⁹³³ 'Political entities' refers to the entities covered by the Act's political exemption: registered political parties, political representatives, contractors and subcontractors for political parties and representatives, and volunteers for registered political parties.

¹⁹³⁴ Submissions to the Discussion Paper: [Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green](#), 3; [Digital Rights Watch](#), 18; [Professor David Lindsay](#), 17; [Castan Centre](#), 13; [elevenM](#), 22. See also submissions to the Issues Paper: [NSW Council for Civil Liberties](#), 6; [Office of the Information Commissioner Queensland](#), 3; [Centre for Media Transition](#), 11; [Reset Australia](#), 5; [Kimberlee Weatherall](#), 4; [OAIC](#), 65; [Australian Communications Consumer Action Network](#), 10; [Australian Privacy Foundation](#), 16.

Submissions supported a prohibition on the handling of information in ways that have been shown to cause harm and discriminate based on a person's emotional stress or mental health circumstances, physical health, or a person's inexperience in a market and potential financial vulnerability.¹⁹³⁵ The Foundation for Alcohol Research and Education highlighted that the people targeted most aggressively by alcohol companies are those who already buy alcoholic products in high amounts. It recommended that even where consent has been provided for collection, use and disclosure of personal information for commercial marketing purposes that companies should be required to ensure that their data processing activities meet the fair and reasonable requirement.¹⁹³⁶

Submitters also expressed support for prohibiting targeting that is directed at vulnerable people (including the use of information about disabilities, addictions, mental health issues, age, physical health, wellbeing, financial situation, addiction, English as a second language)¹⁹³⁷. FARE suggested a prohibition against processing sensitive information, such as factors relating to physical or mental health and wellbeing, whether actual, inferred or generated.¹⁹³⁸

Targeting should satisfy the fair and reasonable test

In response to this feedback, it is proposed that the act or practice of targeting should satisfy the fair and reasonable test as set out in Chapter 12. This would require APP entities to ensure that any collection, use or disclosure of information which relates to an individual, including personal information, deidentified information, and unidentified information for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class) is fair and reasonable in the circumstances. This would require consideration of whether the legislated factors should be calibrated specifically for targeting, but would be likely to include whether a reasonable person would expect the targeting in the circumstances and whether the targeting poses risks of unjustified adverse impact or harm to individuals. The fair and reasonable test would provide a flexible mechanism by which to address targeting which seeks to manipulate or exploit or undermine autonomy.

As proposed in Chapter 8, the fair and reasonable test would also apply to targeting by political entities. This would be consistent with ICO guidance on what the principle of fairness in Article 5 of GDPR requires in the context of political campaigning. It indicates that political parties should only handle personal data in ways that people reasonably expect, and not use it in ways that have unjustified adverse effects on them.¹⁹³⁹ The ICO guidance highlights that processing personal data to influence individuals' opinions and persuade them to vote in a particular way can raise ethical questions which should feed into any assessment of fairness.¹⁹⁴⁰ It further notes that, linked to fairness is transparency, which 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'¹⁹⁴¹.

Prohibit targeting based on sensitive information and sensitive traits

It is also proposed that targeting based on sensitive information and sensitive traits in deidentified and unidentified information relating to individuals should be prohibited. This would be consistent with the DSA, which includes a prohibition against presenting advertisements based on profiling using special categories of personal data.¹⁹⁴² That prohibition is directed at preventing targeting which exploits vulnerabilities, uses manipulative techniques and discriminates against certain groups based on special category data.¹⁹⁴³ Prohibiting targeting based on sensitive information and traits would be consistent with current industry practice.¹⁹⁴⁴

1935 Submissions to the Discussion Paper: [Consumer Policy Research Centre](#), 5; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 9; [Castan Centre](#), 23-25.

1936 Submission to the Discussion Paper: [Foundation for Alcohol Research and Education](#), 18.

1937 Submissions to the Discussion Paper: [Castan Centre](#), 23-25; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 9; [Obesity Policy Coalition](#), 13; [Foundation for Alcohol Research and Education](#), 17. See also [CHOICE](#), 12 and [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 12.

1938 Submission to the Discussion Paper: [Foundation for Alcohol Research and Education](#), 19.

1939 UK ICO, 'Guidance for the use of data in political campaigning: [Lawful, fair and transparent processing](#)' (Web Page).

1940 UK ICO, '[ICO consultation on the draft framework code of practice for the use of personal data in political campaigning](#)' (Web Page, closed 4 October 2019); UK ICO, [Guidance on political campaigning: Draft framework code for consultation](#) (2019), 34-35.

1941 Ibid.

1942 [Digital Services Act 2022](#) (EU) art 24(3). Article 9 of the GDPR defines special category data as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (when used for identification purposes) and data concerning health, a person's sex life or sexual orientation.

1943 [Digital Services Act 2022](#) (EU) recital 52a.

1944 Meta Business Help Centre, [Choosing a Special Ad Category](#) (Web Page); Twitter Business, [Targeting of Sensitive Categories](#) (Web Page); Google Advertising Policies Help, [Personalised Advertising- Policy Principles: Sensitive interest categories](#) (Web Page, 2022).

In the Australian context, consideration should be given to whether such prohibition should not extend to targeting based on the sensitive information categories of information about political opinions, membership of a political association or membership of a trade union so as not to impermissibly burden the implied freedom of political communication. This issue is considered in further detail in Chapter 8.

While a prohibition against targeting based on information relating to an individual which reveals vulnerability would go further to addressing the concern regarding exploitation of vulnerability, such an approach would be problematic as there are likely to be many different interpretations of vulnerability. For example, it could be argued that information that reveals a person's emotional state could indicate vulnerability in some circumstances (e.g. a person feeling lonely or self-conscious) but not in others (e.g. a person feeling excited or elated). Given that the Act expressly lists types of information that fall into the category of 'sensitive information', a prohibition against targeting based on sensitive information or sensitive traits in unidentified and deidentified information is likely to be better understood by industry and consumers.

Other measures to address harmful targeting could be canvassed as part of consultations on other proposals put forward to regulate targeting. For example, the EU's draft AI Act includes a prohibition on the use of certain AI systems intended to distort human behaviour, whereby physical or psychological harms are likely to occur.¹⁹⁴⁵ It states that 'such AI systems deploy subliminal components individuals cannot perceive or exploit vulnerabilities of children and people due to their age, physical or mental incapacities. They do so with the intention to materially distort the behaviour of a person and in a manner that causes or is likely to cause harm'.¹⁹⁴⁶ This approach could be considered in further consultations.

It would also be important to determine the parameters of any exception to the prohibition against targeting based on sensitive traits. For example, if an entity infers that a person may have a mental health condition, it would likely be beneficial for that person to be shown mental health resources or advertisements for mental health support services. An exception for targeting socially beneficial content would also be important for the promotion of government services and health campaigns.

20.8 Amend the Act to introduce the following requirements:

- **Targeting individuals should be fair and reasonable in the circumstances.**
- **Targeting individuals based on sensitive information (which should not extend to targeting based on political opinions, membership of a political association or membership of a trade union), should be prohibited, with an exception for socially beneficial content.**

20.5.5 Proposal – provide individuals with greater transparency

The Discussion Paper put forward a proposal for APP entities to include additional information in their privacy policies. While this proposal was supported by a number of submitters,¹⁹⁴⁷ others suggested the proposal could result in overly lengthy privacy policies that did not highlight the key information-handling practices of concern.¹⁹⁴⁸ Telstra submitted that including the types of information that would be used, generated or inferred would be 'practicably impossible' to determine at the point of notification due to the fluid nature of data analytics and insights. It raised concerns about the volume of parties involved, the often-changing landscape and the varying mechanisms for opting out through third parties.¹⁹⁴⁹ Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise, and the OAIC suggested the proposal would likely generate an overload of uninformative privacy policies.¹⁹⁵⁰

¹⁹⁴⁵ European Commission, [Proposal for an Artificial Intelligence Act](#) [2021] recital 16.

¹⁹⁴⁶ Ibid.

¹⁹⁴⁷ Submissions to the Discussion Paper: [Office of the Victorian Information Commissioner](#), 8; [Australian Council on Children and the Media](#), 8; [Australian Privacy Foundation](#), 12; [DIGI](#), 22; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 9; [CHOICE](#), 15; [Calabash Solutions](#), 15; [Privacy 108](#), 30; [Public Health Association of Australia](#), 11; [Foundation for Alcohol Research and Education](#), 20; [Graham Greenleaf](#), 5.

¹⁹⁴⁸ Submissions to the Discussion Paper: [OAIC](#), 152; [Experian](#), 20; [Telstra](#), 21; [Insurance Council of Australia](#), 14-15; [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 21; [Woolworths Group](#), 12.

¹⁹⁴⁹ Submission to the Discussion Paper: [Telstra](#), 21.

¹⁹⁵⁰ Submissions to the Discussion Paper: [Kimberlee Weatherall, Tom Manousaridis and Melanie Trezise](#), 22; [OAIC](#), 65.

The DSA requires online platforms to ensure users can identify, for each specific advertisement to each individual recipient, in a clear, concise and unambiguous manner and in real time:¹⁹⁵¹

- that the information presented is an advertisement, including through prominent marketing
- the person on whose behalf the advertisement is presented and who paid for it (where this is different to the person on whose behalf the advertisement is presented), and
- meaningful information about the main parameters used to determine the recipient to whom the advertisement is presented and where applicable about how to change those parameters. The information shall be directly and easily accessible from the advertisement.

The DSA also requires online platforms to provide individuals with information about recommender systems. Requiring entities to include information alongside ads as they appear is likely to ensure individuals have a better understanding of how their information is being used, which may empower users to take control of how their personal information is handled (for example, changing advertisement settings or exercising data subject rights under the GDPR).

A report published by the Foundation for Alcohol Research and Education noted that ‘the primary challenge when observing advertisements on digital platforms is that the content is no longer ‘published’. Most advertisements are only visible to users at a particular moment’.¹⁹⁵² The report emphasised the importance of public archives of advertisements published on the platform, but noted this information is of limited utility without transparency of algorithmic advertising models and how individuals are targeted.¹⁹⁵³

In order to provide individuals with greater awareness and understanding about how targeting systems work and why they are being targeted with certain content, entities should provide information to online users about the use of online targeting systems, including clear information about the use of algorithms and profiling to recommend content to individuals. This information would also be useful for enforcing compliance with the Act, and could be requested by the IC as part of an assessment or an investigation into an entity’s compliance with the Act in relation to their targeting activities. Such information should also be made publicly available to facilitate research into emerging risks. Further consultation will help inform the most effective way to implement this requirement.

20.9 Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.

¹⁹⁵¹ [Digital Services Act 2022](#) (EU) art 24.

¹⁹⁵² Foundation for Alcohol Research and Education, [Advertisements on digital platforms: how transparent and observable are they?](#) (2022) 3.

¹⁹⁵³ *Ibid* 5.

21. Security, Destruction and Retention of Personal Information

Security and destruction of personal information are areas of increasing concern. This is driven by the volume of data being handled by both the public and private sectors, the pace of technological advancement and the prevalence of data breaches involving malicious or criminal attacks.¹⁹⁵⁴

The Discussion Paper sought feedback on whether the current security and destruction requirements in the Act were sufficiently clear and strong. This feedback generally indicated that entities do not have enough practical clarity about what reasonable steps they should take to protect and, when necessary, destroy personal information in a way that upholds good privacy practices. As noted in the Discussion Paper, the leading sources of data breaches are malicious or criminal attacks (including cyber incidents), which suggests that the steps APP entities are taking to protect personal information could be improved.¹⁹⁵⁵

Following the release of the Discussion Paper, there were several cyber security incidents that resulted in large scale data breaches which impacted millions of Australians.¹⁹⁵⁶ This has brought further prominence and concern about whether there are the right settings for entities to keep personal information secure and to only retain personal information for the time that is necessary.

This chapter focuses on the specific security requirements under the Act that apply broadly across the economy. However, there are specific industries that are subject to security standards unique to their sector of the economy. For example, banks, insurers and superannuation funds are subject to standards that deal specifically with operational risks, including cyber security.¹⁹⁵⁷ ASIC was recently successful in taking action against Australian Financial Services licensee, RI Advice, for breaching its license obligations under the *Corporations Act 2001* (Cth) to act efficiently and fairly when it failed to have adequate risk management systems to manage its cybersecurity risks.¹⁹⁵⁸

Furthermore, in addition to the Privacy Act Review, the Government has announced that it will be developing the Cyber Security Strategy.¹⁹⁵⁹ The Cyber Security Strategy is being led by the Department of Home Affairs and will explore how Government can work more closely with industry and civil society to achieve effective and appropriate security settings. This may include articulating the security expectations of different entities across the digital economy, supporting victims of cybercrime and supporting all entities, including small and medium enterprises, to operate securely online. The Cyber Security Strategy will build on other initiatives underway to strengthen the security of critical infrastructure and Government with a view to protect sensitive information.

21.1 Current security 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 and is not intended to be prescriptive. This approach gives APP entities flexibility to determine what steps may be reasonable for them in their circumstances to protect the personal information they hold.

¹⁹⁵⁴ OAIC, [Notifiable Data Breaches Report: January – June 2021](#) [August 2021]; OAIC, [Notifiable Data Breaches Report: July – December 2021](#) [February 2022].

¹⁹⁵⁵ [Discussion Paper](#), 145.

¹⁹⁵⁶ Several large-scale cyber incidents occurred in the second half of 2022 including the Optus data breach on 22 September 2022 and the Medibank data breach on 13 October 2022.

¹⁹⁵⁷ Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 1 of 2018 [[Standard CPS 234 Information Security](#)].

¹⁹⁵⁸ *Australian Securities and Investment Commission v RI Advice Group Pty Ltd* [2022] FCA 496.

¹⁹⁵⁹ Clare O'Neil MP, [Working in partnership to address cyber threats](#) (Web Page, 11 October 2022).

21.2 The need for clearer security requirements – what are ‘reasonable steps’?

Submitters highlighted that regulated entities do not commonly understand what are reasonable steps to take to comply with APP 11 and that APP entities would benefit from clearer guidance on this.¹⁹⁶⁰ The Discussion Paper proposed to amend APP 11.1 to state that the ‘reasonable steps’ requirement includes technical and organisational measures. The OAIC has previously explained that APP entities must protect personal information using both technical security measures and by implementing strategies in relation to governance, internal practices, processes and systems, and dealing with third party providers¹⁹⁶¹. Submitters were generally neutral about this proposal. Some submitters noted the importance of implementing technical and organisational controls to address information security risks was already well understood¹⁹⁶² and that this change would not provide greater certainty beyond what is already provided by current guidance.¹⁹⁶³ On the other hand, some submitters noted that this change could provide greater certainty and promote enhanced compliance¹⁹⁶⁴ by removing any possible doubt that the current accepted interpretation of APP 11.1 as including technical and organisational measures, is correct.¹⁹⁶⁵

While this change would not provide greater *specificity* as to what reasonable steps APP entities should be taking, it could assist in clarifying the expected *scope* of measures entities should be taking into consideration when protecting personal information. This amendment would maintain the principles-based nature of the APPs, and help focus any enhanced guidance produced by the OAIC (see Recommendation 21.3). It would also enhance international consistency as the GDPR requires controllers and processors of personal data to *implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*.¹⁹⁶⁶

21.1 Amend APP 11.1 to state that ‘reasonable steps’ include technical and organisational measures.

21.3 Baseline security requirements

Proposal 19.2 of the Discussion Paper was to amend APP 11 to include a list of factors that outlined what reasonable steps may be required under APP 11.1. Submitters in support of the proposal noted that it would create a clearer baseline standard of necessary security measures¹⁹⁶⁷ which would effectively codify existing OAIC guidance on the factors entities should consider when protecting personal information.¹⁹⁶⁸ Those in support also noted that the lack of market incentives to improve cyber security standards of consumer products means there is need for a more robust and enforceable system of regulation¹⁹⁶⁹ and that clearer security requirements would increase protections for individuals from data breaches.¹⁹⁷⁰

However, other submitters suggested the current approach was sufficient¹⁹⁷¹ and considered there would be greater value in providing more detailed, up-to-date and non-binding guidance on technical and organisational ways of managing privacy risks under APP 11.¹⁹⁷² Privacy 108 highlighted that the OAIC’s most recent guidance on security was released in 2018 and that since that time both the risk landscape and business processes had changed

¹⁹⁶⁰ Submissions to the Discussion Paper: [Privcore](#), 3; [Australian Information Security Association](#), 5; [Privacy 108](#), 34; [Western Union](#), 8.

¹⁹⁶¹ Submission in response to Department of Home Affairs, *Australia’s 2020 Cyber Security Strategy: A Call for views*: [OAIC](#) (11 November 2019); OAIC, [Guide to Securing Personal Information](#) [5 June 2018].

¹⁹⁶² Submission to the Discussion Paper: [Privacy 108](#), 34.

¹⁹⁶³ Submissions to the Discussion Paper: [Woolworths Group](#), 14; [MIGA – Medical Insurance Group Australia](#), 8.

¹⁹⁶⁴ Submissions to the Discussion Paper: [Department of Health](#), 15; [Australian Institute of Company Directors](#), 4.

¹⁹⁶⁵ Submission to the Discussion Paper: [elevenM](#), 53.

¹⁹⁶⁶ GDPR art 32(1).

¹⁹⁶⁷ Submissions to the Discussion Paper: [Australian Institute of Company Directors](#), 4; [Access Now](#), 8.

¹⁹⁶⁸ Submission to the Discussion Paper: [Australian Association of National Advertisers](#), 6.

¹⁹⁶⁹ Submission to the Discussion Paper: [Australian Communications Consumer Action Network](#), 16.

¹⁹⁷⁰ Submission to the Discussion Paper: [NSW Council for Civil Liberties](#), 34.

¹⁹⁷¹ Submissions to the Discussion Paper: [Telstra](#), 23; [Calabash Solutions](#), 21.

¹⁹⁷² Submissions to the Discussion Paper: [Privacy 108](#), 34; [Australian Banking Association](#), 27; [Australian Digital Health Agency](#), 4; [Department of Health](#), 15; [elevenM](#), 53.

considerably.¹⁹⁷³ Retaining principles-based and technology-neutral requirements would help ensure the future flexibility of the Act to adapt to rapid developments in information processing technology and data practices.¹⁹⁷⁴ Submitters also expressed concerns that including a list of factors and particular measures would likely add unnecessary prescriptiveness to APP 11, reduce the flexibility offered to entities to tailor appropriate information security capabilities to their circumstances¹⁹⁷⁵ and that it would risk becoming a 'box-ticking' exercise that fails to address risks in a meaningful way to the benefit of individuals.¹⁹⁷⁶ The OAIC noted that it did not consider that greater prescription would provide any additional certainty to APP entities.¹⁹⁷⁷

This feedback was consistent with that received by the Department of Home Affairs to a discussion paper in 2021 about options for regulatory reforms and voluntary incentives to strengthen the cyber security of Australia's digital economy.¹⁹⁷⁸ That discussion paper proposed the idea of an enforceable cyber security code that specified minimum cyber security expectations for entities handling personal information under APP 11. Stakeholders who supported an enforceable cyber security code pointed to the value of improving the clarity of the reasonable steps test under APP 11¹⁹⁷⁹ and the significant cyber security gains of encouraging the consistent adoption of foundational cyber security practices across the economy.¹⁹⁸⁰

Those who did not support the enforceable cyber security code thought that a code would add unnecessary complexity to the regulatory environment¹⁹⁸¹ and would have limited impact because it could not apply to most small businesses¹⁹⁸² or data that is not personal information.¹⁹⁸³

Nonetheless, stakeholder feedback supported the underlying desirability of more consistent uptake of foundational cyber security controls and standards across the economy and noted that the Act is an important mechanism to contribute to cyber security and privacy uplift because of its broad reach across the economy. In order to address the risks associated with poor security practices, rather than including a list of factors or steps entities should take (e.g. encryption, two-factor authentication, etc.), it is proposed that APP 11 include a list which outlines the baseline privacy *outcomes* APP entities should consider when taking reasonable steps to protect the personal information they hold. This could be supplemented with additional OAIC guidance (see Recommendation 21.3).

This alternative approach was supported by submitters who noted that APP 11 should remain principles-based with a closer focus on desired outcomes rather than prescribing how these outcomes should be achieved.¹⁹⁸⁴ It is also consistent with submissions noting that more needs to be done to set the bar for entities and to achieve the desired privacy outcomes, similar to Article 32 of the GDPR which sets out specific measures to ensure a level of security appropriate to the risk.¹⁹⁸⁵

Including non-exhaustive outcomes-based factors into the Act would be consistent with the principles-based nature of the APPs as entities would be able to take reasonable steps to meet those outcomes in accordance with their operating environments, information holdings and the types of privacy risks relevant to them. This approach could promote additional, indirect benefits. One submitter noted that the adoption of principles-based security requirements can incentivise innovation and encourage entities to analyse the probability and severity of threats in line with technological realities, ensuring security evolves with critical technologies.¹⁹⁸⁶

¹⁹⁷³ Submission to the Discussion Paper: [Privacy 108](#), 34.

¹⁹⁷⁴ Submissions to the Discussion Paper: [Calabash Solutions](#), 21; [Avant Mutual](#), 16; [Law Council of Australia](#), 17; [Social Services Portfolio](#), 28; [elevenM](#), 53.

¹⁹⁷⁵ Submission to the Discussion Paper: [Telstra](#), 23.

¹⁹⁷⁶ Submission to the Discussion Paper: [Woolworths Group](#), 14.

¹⁹⁷⁷ Submission to the Discussion Paper: [OAIC](#), 164.

¹⁹⁷⁸ Department of Home Affairs, *Strengthening Australia's cyber security regulations and incentives: A call for views*, [2021].

¹⁹⁷⁹ Submissions in response to the Department of Home Affairs, *Strengthening Australia's cyber security regulations and incentives: A Call for views*: [Australian Information Security Association](#) (referencing its submission to the Review of the Privacy Act), 19-20; [Vaultron](#), 19; [CISCO](#), 5.

¹⁹⁸⁰ Submissions in response to Department of Home Affairs, *Strengthening Australia's cyber security regulations and incentives: A Call for views*: [Telstra](#), 10; [SAP](#), 3-4.

¹⁹⁸¹ Submission in response to Department of Home Affairs, *Strengthening Australia's cyber security regulations and incentives: A Call for views*: [Australian Industry Group](#), 29-30.

¹⁹⁸² Submissions in response to Department of Home Affairs, *Strengthening Australia's cyber security regulations and incentives: A Call for views*: [Telstra](#), 10; [Atlassian](#), 2; [Internet of Things Alliance Australia](#), 7; [Office of the Victorian Information Commissioner](#), 8; [Information Technology Industry Council](#), 8; [Palo Alto Networks](#), 8; [IAG](#), 3; [Google](#), 4; [Communications Alliance and Australian Mobile Telecommunications Association](#), 6.

¹⁹⁸³ Submissions in response to Department of Home Affairs, *Strengthening Australia's cyber security regulations and incentives: A Call for views*: [Atlassian](#), 2; [Internet of Things Alliance Australia](#), 7; [McAfee](#), 10; [IAG](#), 3; [Forum of Australasian Security Executives](#), 7; [Gateway Network Governance Body](#), 3; [Communications Alliance and Australian Mobile Telecommunications Association](#), 6.

¹⁹⁸⁴ Submission to the Discussion Paper: [Woolworths Group](#), 14.

¹⁹⁸⁵ Submission to the Discussion Paper: [Australian Information Security Association](#), 5.

¹⁹⁸⁶ Submission to the Discussion Paper: [CrowdStrike](#), 2.

Article 32(1) of the GDPR provides useful examples of the types of outcomes-based factors which could be included in APP 11. For example, under the GDPR, it is a requirement that entities have the ‘ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services which hold personal information’. The approach in Article 32 of the GDPR and the ACSC’s Cyber Security Principles could be used as a starting point for further consideration and development of the factors.¹⁹⁸⁷

However, further consultation would need to be undertaken prior to implementation of any outcomes-based factors to ensure they are broadly applicable, sufficient and relevant for the Australian context and cohesive with other domestic legal frameworks. Questions of what regulation of these outcomes would look like in practice would also need to be addressed.

By inserting a list of outcomes-based factors that entities should consider, entities would only have to ensure that their current practices enable them to meet those outcomes. The need to make upgrades to an entity’s information security capabilities is therefore not automatically required. In keeping with the APPs, the language of the requirement itself would not mandate how entities are to achieve these outcomes but would instead require them to *consider* them when taking reasonable steps.

21.2 Include a set of baseline privacy outcomes under APP 11 and consult further with industry and government to determine these outcomes, informed by the development of the Government’s 2023-2030 Australian Cyber Security Strategy.

21.4 Guidance on obligations under APP 11

Industry would benefit from further guidance and education outlining the Government’s cyber security expectations under the Act, particularly as the threat environment changes over time.

This could be achieved through enhancing the OAIC’s Guidelines, which would provide increased certainty for APP entities, and broadening its scope to cover much needed contemporary updates – such as cyber-specific elements. This approach would maintain the flexibility of APP 11 and provide more detail in a manner that is easier to update than legislation,¹⁹⁸⁸ which is beneficial in light of how dependent security practices are to new technologies.¹⁹⁸⁹

Submitters noted that providing additional detail on ‘reasonable steps’ for APP 11 presents an opportunity to align with existing cyber security standards as appropriate.¹⁹⁹⁰ In support of alignment, submitters emphasised that it is important to ensure that Australia’s cyber security regulatory frameworks are cohesive to allow entities to focus on understanding their obligations¹⁹⁹¹ and maintaining information security, as opposed to treating security as a compliance exercise.¹⁹⁹²

Provided it is adequately funded and has the right staff expertise, the OAIC is well placed to work with industry, security professionals, standards bodies, government agencies like the Australian Signals Directorate, international counterparts and other relevant stakeholders to provide guidance on baseline and best practice security measures in various contexts.¹⁹⁹³

¹⁹⁸⁷ Australian Cyber Security Centre, [Cyber Security Principles](#) [10 March 2022].

¹⁹⁸⁸ Submission to the Discussion Paper: [Calabash Solutions](#), 20-21.

¹⁹⁸⁹ Submission to the Discussion Paper: [Law Council of Australia](#), 17.

¹⁹⁹⁰ Submissions to the Discussion Paper: [Australian Institute of Company Directors](#), 4; [Australian Information Security Association](#), 5.

¹⁹⁹¹ Submission to the Discussion Paper: [Amazon Web Services](#), 2.

¹⁹⁹² Submission to the Discussion Paper: [Deloitte Australia](#), 42.

¹⁹⁹³ Submission to the Discussion Paper: [elevenM](#), 53.

If (or where) alignment is not possible, submitters noted that it would be useful for the OAIC's guidance to include those standards it considers reasonable¹⁹⁹⁴ or which represent 'safe harbours' or 'gold standards' for entities to follow¹⁹⁹⁵ given there is no one-size-fits-all approach for security standards.¹⁹⁹⁶ While this would be a matter for the OAIC to consider during the development process for such enhanced guidance, the advantage of this approach is that such matters can be considered in detail without being limited by considerations such as prescriptiveness or applicability.

21.3 Enhance the OAIC Guidelines in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre.

21.5 Protecting de-identified information

Chapter 2 proposes to amend the definition of 'de-identification' to make it clear that de-identification of personal information is a process which involves treating it in such a way so that no individual is identified or reasonably identifiable in the current circumstances. It also proposes that certain protections of the Act should apply to de-identified information. One of those protections would be APP 11.1. However, it is expected that the level of protection afforded to de-identified information may be to a lower degree than personal information. See Chapter 2 for further details on this proposal.

21.4 Amend APP 11.1 so that APP entities must also take reasonable steps to protect de-identified information.

21.6 Current destruction and de-identification requirements

APP 11.2 requires APP entities to destroy or de-identify all personal information which they no longer need for any purpose for which the information may be lawfully used or disclosed under the Act. There are exceptions to this requirement, such as if the information is contained in a Commonwealth record or the entity is required to retain the information by another Australian law or court order. The OAIC provides guidance on *De-identification and the Privacy Act*.¹⁹⁹⁷

APP 11.1 complements other requirements under the Act which, together, require entities to only collect and keep the information that they need. For example, APPs 3.1 and 3.2 limit the personal information an entity may collect to that which is reasonably necessary for, and for agencies, directly related to, one or more of its functions or activities. The proposed fair and reasonable requirement set out in Chapter 12 will further reinforce this data minimisation principle. Factors relevant to this requirement would include matters such as whether an individual would reasonably expect the personal information to be collected, use or disclosed in the circumstances, or whether it was reasonably necessary for the functions or activities of the organisation to collect and use the information.

The proposals in this chapter would go further to reinforce the data minimisation principle.

¹⁹⁹⁴ Submission to the Discussion Paper: [Australian Digital Health Agency](#), 4.

¹⁹⁹⁵ Submission to the Discussion Paper: [Australian Medical Association](#), 15.

¹⁹⁹⁶ Submission to the Discussion Paper: [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 11.

¹⁹⁹⁷ OAIC, [De-identification and the Privacy Act](#), [21 March 2018].

21.7 Dealing with personal information that is no longer necessary

The Discussion Paper sought views on whether there was a need to strengthen APP 11.2 and proposed to amend the obligation to require APP entities to take *all* reasonable steps to destroy or de-identify personal information when it is no longer required.

There was some support for this proposal with some submitters noting that this change would strengthen the obligation and reduce its overly permissive nature.¹⁹⁹⁸ However, concerns were expressed that raising the standard alone would be inadequate¹⁹⁹⁹ and would be unlikely to have a significant impact on compliance or the maturity of APP entities' destruction or de-identification standards.²⁰⁰⁰ It was noted that raising the standard would risk putting APP 11.2 out of step relative to the other APPs,²⁰⁰¹ and potentially result in greater ambiguity for businesses.²⁰⁰² It was suggested that without knowing the standard against which *all* reasonable steps would be evaluated, entities may feel obligated to take steps that are onerous and costly in order to meet the standard, regardless of whether such steps are actually reasonable or necessary for their circumstances.²⁰⁰³

As an alternative, more detailed guidance on the destruction and de-identification of personal information, including the actions that would constitute reasonable steps, could be provided by the OAIC. Several submitters indicated this would be beneficial.²⁰⁰⁴ A theme that emerged from the feedback was that although principles-based regulation is desirable, APP entities require more specific guidance to understand the extent of their obligations as well as modern, relevant advice as to what steps may be reasonable in the context of their operations (e.g. healthcare and research). Enhanced guidance could be applied by APP entities according to the specific industry, method of destruction and/or the type or sensitivity of the information.

Given the concern that the proposal to require *all* reasonable steps to destroy or de-identify personal information would create confusion, rather than clarify obligations, and that the key issue appears to be a lack of understanding about what the obligation entails, the most effective way to address this issue would be through OAIC guidance. The guidance in relation to APP 11.2 could be enhanced to cover both destruction and retention matters, as well as de-identification matters in line with its amended definition recommended in Chapter 2.

21.5 The OAIC Guidelines in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information.

21.8 Review legal provisions that require retention of personal information

The obligation under APP 11.2 to take such steps as are reasonable in the circumstances to destroy or de-identify personal information is subject to requirements in other Australian laws to retain the information. Retention requirements in other Australian laws were considered by Parliaments at the relevant times to appropriately achieve particular policy outcomes and objectives. Some of these requirements are subject to regular review through statutory mechanisms, and others have been reviewed as part of separate processes such as the recent review of the retention regime under the *Telecommunications (Interception and Access) Act 1979*.²⁰⁰⁵

1998 Submissions to the Discussion Paper: [NSW Council for Civil Liberties](#), 34; [OAIC](#), 165.

1999 Submission to the Discussion Paper: [Australian Privacy Foundation](#), 15.

2000 Submission to the Discussion Paper: [elevenM](#), 54.

2001 Submission to the Discussion Paper: [Australian Banking Association](#), 27.

2002 Submissions to the Discussion Paper: [Information Technology Industry Council](#), 4; [BSA | The Software Alliance](#), 10; [Communications Alliance Ltd](#), 22.

2003 Submissions to the Discussion Paper: [Communications Alliance Ltd](#), 22; [BSA | The Software Alliance](#), 10.

2004 Submissions to the Discussion Paper: [AANA \(Australian Association Of National Advertisers\)](#), 6; [BSA | The Software Alliance](#), 10; [Australian Privacy Foundation](#), 15; [Privacy 108](#), 37.

2005 Parliamentary Joint Committee on Intelligence Security, [Review of the mandatory data retention regime](#), [2020].

The Australian Government Social Services Portfolio noted that other statutory obligations requiring the retention of information need to be considered, such as the *Archives Act 1983*, or circumstances in which information has been used or disclosed in compliance with an auditing obligation, mandatory reporting obligations or law enforcement request.²⁰⁰⁶ The need for further information about the interactions between varying retention requirements was also highlighted by other Government agencies.²⁰⁰⁷ Submitters also noted that it would be useful for the OAIC to provide additional guidance on retention periods for certain types of information.²⁰⁰⁸

In light of significant cyber incidents and data breaches, and the growing collection of personal information in the digital age, these retention requirements should be examined, where a statutory or other independent review has not recently taken place, to determine whether they appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information. The Australian Government Digital Identity System which enables individuals to prove their identity safely and securely and removes the need for retention of identification documents²⁰⁰⁹ should be considered in the context of reviewing data retention requirements. Given the breadth and scale of legislative provisions that contain data retention requirements, further consideration should be given to the scope and scale of this review, in consultation with States and Territories.

21.6 The Commonwealth should undertake a review of all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information.

This further work could also be considered by the proposed Commonwealth, state and territory working group at Proposal 29.3 as a key issue of concern where alignment would be beneficial.

However, this review should not duplicate the recent independent review of the mandatory data retention regime under the *Telecommunications (Interception and Access) Act 1979* and the independent reviews and holistic reform of electronic surveillance legislative powers.

21.9 Strengthening requirements around the retention of personal information

Whilst Recommendation 21.5 focusses on the standard for *how* personal information that is no longer necessary should be destroyed or de-identified, feedback on the Discussion Paper also highlighted issues with APP entities not taking active steps to determine *when* they no longer need personal information for any purpose for which it may be used or disclosed – i.e. their retention practices.

In their submission, the OAIC noted that when entities hold personal information for longer than is necessary, 'honey pots' of valuable data are created which may increase the risk of the entity's information systems being hacked.²⁰¹⁰ Additionally, there is increased risk that a greater number of individuals would be impacted in the event a data breach does occur.²⁰¹¹

2006 Submission to the Discussion Paper: [Social Services Portfolio](#), 29.

2007 Submission to the Discussion Paper: [CSIRO](#), 11.

2008 Submission to the Discussion Paper: [Privacy 108](#), 37.

2009 Australian Government, [About Digital Identity](#) (Web Page).

2010 Submission to the Discussion Paper: [OAIC](#), 165.

2011 Submission to the Discussion Paper: [Calabash Solutions](#), 21.

To encourage improved retention practices, one submitter suggested that APP entities should state exactly how long each element of personal information is retained, whether personal information is de-identified or destroyed once retention periods are met and how long after the retention period is met that this will occur.²⁰¹² While recognising the advantages of the principles-based approach to the APPs, APP 11.2 does not require entities to actively review and consider their information holdings. A benefit of the suggested approach is that it would allow each individual entity to determine its own retention periods in a manner that is suitable and beneficial for its own specific circumstances while also bringing retention requirements into greater focus. Providing APP entities with the flexibility to set their own retention periods, consistent with retention requirements under APP 11.2 would also enable them to tailor retention periods according to the type of data. This would assist industries where the management of personal information can be more complex, such as in the healthcare sector where it can be challenging for smaller providers who hold numerous sets of health data where those records become no longer required at different times.²⁰¹³

Requiring APP entities to establish their own maximum and minimum retention periods in relation to the personal information they hold would be consistent with international standards. In Canada, the Office of the Privacy Commissioner notes that in order to fulfil its responsibilities under Fair Information Principle 5, entities should institute maximum and minimum retention periods that take into account any legal requirements or restrictions as well as appeal mechanisms.²⁰¹⁴ In addition, Recital 39 which accompanies Article 5 of the GDPR states that *[i]n order to ensure that the personal data are not kept longer than is necessary, time limits should be established by the controller for erasure or for a periodic review.*²⁰¹⁵

In recognition of the vast range of circumstances in which entities handle personal information, amending APP 11 to require APP entities to establish retention periods should be qualified in a manner that allows entities to take into account factors such as type, sensitivity and purpose of the information, as well as their organisational needs and any other legal obligations they may have. This would assist in ensuring that the requirement is not overly burdensome. The retention periods set by entities should also be periodically reviewed. Entities should be conscious of the security risks that present in retaining information for long periods of time.

21.7 Amend APP 11 to require APP entities to establish their own maximum and minimum retention periods in relation to the personal information they hold which take into account the type, sensitivity and purpose of that information, as well as the entity's organisational needs and any obligations they may have under other legal frameworks. APP 11 should specify that retention periods should be periodically reviewed. Entities would still need to destroy or de-identify information that they no longer need.

2012 Submission to the Discussion Paper: [Calabash Solutions](#), 21.

2013 Submission to the Discussion Paper: [MIGA - Medical Insurance Group Australia](#), 8.

2014 Office of the Privacy Commissioner of Canada, [PIPEDA Fair Information Principle 5 – Limiting Use, Disclosure, and Retention](#) (August 2020).

2015 GDPR Recital 39.

21.10 Increasing transparency for the retention of personal information

At present, APP 1 requires APP entities to demonstrate that they manage personal information openly and transparently, including by having a clearly expressed privacy policy. To complement Proposal 21.7 and to ensure consistency with APP 1, entities should be required to specify their personal information retention periods in their privacy policies.

This approach is supported by submitters who stated that entities should be required to articulate their data retention periods in their privacy notices²⁰¹⁶ as too often they do little more than echo APP 11.2 requirements.²⁰¹⁷ It would also be in line with Article 13 of the GDPR which states that in order to ensure the fair and transparent processing of personal information, controllers shall *provide the data subject with... the period for which the personal data [obtained] will be stored, or if that is not possible, the criteria used to determine that period.*²⁰¹⁸

Notwithstanding the issues associated with privacy policies and how many users read and/or understand those policies, transparency remains a fundamental component of fair and reasonable information handling. This amendment would highlight the importance of good retention practices and could be a relevant consideration for the IC in the event of any investigations or complaints.

Given that APP entities are currently required to have privacy policies, this amendment would pose minimal regulatory burden on entities once their retention periods have been established as per Proposal 19.6.

See Chapter 10 for further proposals in relation to privacy policies.

21.8 Amend APP 1.4 to stipulate that an APP entity's privacy policy must specify its personal information retention periods.

2016 Submission to the Discussion Paper: [Privacy 108](#), 37.

2017 Submission to the Discussion Paper: [Calabash Solutions](#), 21.

2018 GDPR Article 13(2)(a).

22. Controllers and processors of personal information

In submissions to the Issues Paper, a number of stakeholders promoted the benefits of data protection laws distinguishing between 'controllers' and 'processors' of personal information. The distinction operates to impose different obligations on those entities that determine the purposes for which personal information is processed and the means of processing (controllers), and those entities which process personal information on behalf of controllers (processors)²⁰¹⁹ – see the below example of a controller processor relationship. The distinction between controllers and processors is a feature of the GDPR.²⁰²⁰

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

The Discussion Paper noted the challenges of introducing the controller processor distinction into the Act in light of the exemption for most small business from the Act and sought feedback on how the distinction could operate alongside the Act's exemptions. The Discussion Paper also sought views on what obligations processors should have under the Act if the distinction was adopted.

22.1 Current approach

The APPs currently apply to any APP entity that 'holds' personal information – this includes entities that control or have possession of a record of personal information.²⁰²¹ As the term 'holds' captures both entities that control and possess personal information (such as an outsourced service provider), both types of entities need to ensure they comply with the full suite of APPs.

The application of the APPs to all entities covered by the Act becomes problematic when APP entities hold personal information without any direct relationship with the individual. This can impact an APP entity's ability to comply with all the APPs. For instance, an outsourced service provider (processor) who receives a record of personal information from another entity (controller) may not have the means to directly contact the individual to provide reasonable notice of the collection of their personal information, or gain consent for the use or disclosure of their personal information. Alternatively, if the outsourced service provider is able to contact the individual, the lack of allocation of responsibilities can result in individuals receiving duplicative collection notices and requests for consent from both entities.²⁰²²

A number of international frameworks overcome this tension by distinguishing between controllers and processors; and requiring processors to comply with select obligations.

22.2 Would a controller processor distinction be beneficial?

In response to the Discussion Paper, submitters expressed strong support for introducing the concepts of controllers and processors in the Act. Industry stakeholders were largely supportive on the basis that the distinction would assist with clarifying obligations and allocating responsibilities between entities.²⁰²³

2019 GDPR arts 4(7), 4(8).

2020 GDPR arts 24-43.

2021 Privacy Act s 6(1).

2022 Submissions to the Discussion Paper: [Atlassian](#), 3; [BSA | The Software Alliance](#), 4; [Communications Alliance](#), 13; [ADMA](#), 33.

2023 Submissions to the Discussion Paper: [Atlassian](#), 3; [BSA | The Software Alliance](#), 3; [Association for Data-Driven Marketing and Advertising](#), 33-34; [Australian Information Industry Association](#), 4; [Calabash Solutions](#), 22; [DIGI](#), 24; [elevenM](#), 57; [Information Technology Industry Council](#), 1; [Microsoft](#), 1; [ResMed](#), 5; [Snap Inc.](#), 8; [Amazon Web Services](#), 2; [IoT Alliance Australia](#), 7; [Australian Super](#), 2; [Tech Council of Australia](#), 4; [Workday](#), 1.

The different roles which controllers and processors have in relation to personal information reflects the operational reality of many business relationships, despite the concept not currently being included in the Act.²⁰²⁴ APP entities typically maintain numerous controller-processor relationships and small businesses commonly rely on outsourced software and infrastructure service providers to hold or process personal information to manage their business processes.²⁰²⁵

Submitters emphasised the benefits of aligning with international frameworks, noting that international interoperability would ensure a common understanding with global entities and facilitate global compliance.²⁰²⁶ The controller processor distinction appears in a number of data protection frameworks internationally, including New Zealand, the UK, Brazil, Japan, Hong Kong, the Republic of Korea, Singapore and the EU GDPR. The distinction is also present in draft privacy laws of India, Indonesia and Canada.

Submitters also noted that the distinction could improve the functioning of the Act. In particular, the concept would clarify consent obligations²⁰²⁷ and assist with clarifying obligations in relation to any new individual rights (such as a right to erasure) that may be introduced following this Review.²⁰²⁸ It could also help entities more effectively respond to data breaches.²⁰²⁹ Overall, submitters who supported introducing the distinction considered that it could increase transparency for consumers²⁰³⁰ and provide individuals with a single entity to approach about the protection of their personal information.²⁰³¹

However, other feedback noted shortcomings of the distinction, including that it does not account for data sharing arrangements between two controllers.²⁰³² It was also noted that the current Act does not map neatly onto the controller-processor relationship.²⁰³³ Some submitters raised concerns that the distinction would have limited benefit to consumer privacy²⁰³⁴ and that the Review should prioritise other proposals.²⁰³⁵ The Law Council of Australia suggested the introduction of the concept was unnecessary and would interfere with existing contractual arrangements and descriptions of responsibilities and rights of contracting parties without a corresponding privacy benefit to individuals.²⁰³⁶

Feedback noted that the ability to introduce the distinction is limited by the small business exemption, and to a lesser extent, by the employee records exemption.²⁰³⁷ However, limited feedback was received on how the distinction could be usefully adopted if the exemptions are maintained. One submitter suggested partial adoption would be practical if introduced to apply when both the controller and the processor are APP entities.²⁰³⁸ Another suggested introducing a category of 'processor' for organisations that hold or process data on behalf of other APP entities, irrespective of whether they are an APP entity. However, some submitters also noted that partial adoption would be likely to increase complexity and confusion as to when certain APPs apply.²⁰³⁹

If the distinction was introduced, submitters noted the definitions of controller and processor would need to be carefully considered.²⁰⁴⁰ This is particularly crucial as any determination of whether an entity is a processor or controller is fact-based and hinges on the context in which the personal information is being processed.²⁰⁴¹ An entity may also be a controller and a processor in respect of different sets of personal information.²⁰⁴²

2024 Submissions to the Discussion Paper: [elevenM](#), 56; [Australian Super](#), 2.

2025 Submission to the Discussion Paper: [elevenM](#), 56.

2026 Submissions to the Discussion Paper: [Atlassian](#), 4; [BSA | The Software Alliance](#), 3; [Information Technology Industry Council](#), 1; [Australian Communications Consumer Action Network](#), 17; [Microsoft](#), 2; [Communications Alliance](#), 13; [Google](#), 6; [ResMed](#), 5; [Snap Inc.](#), 8; [Salesforce](#), 2; [Western Union](#); [Amazon Web Services](#), 2; [Australian Super](#), 2; [ACT | The App Association](#), 3.

2027 Submissions to the Discussion Paper: [Atlassian](#), 3; [BSA | The Software Alliance](#), 4; [Workday](#), 4.

2028 Submissions to the Discussion Paper: [Workday](#), 4; [ACT | The App Association](#), 4.

2029 Submissions to the Discussion Paper: [Atlassian](#), 4; [BSA | The Software Alliance](#), 4-5; [Information Technology Industry Council](#), 1; [Microsoft](#), 2-3; [Salesforce](#), 2; [Australian Super](#), 2; [Tech Council of Australia](#), 4; [Workday](#), 2.

2030 Submissions to the Discussion Paper: [Amazon Web Services](#), 2; [Workday](#), 2.

2031 Submissions to the Discussion Paper: [Information Technology Industry Council](#), 1; [ACT | The App Association](#), 4.

2032 Submission to the Discussion Paper: [Telstra](#), 24.

2033 Submission to the Discussion Paper: [elevenM](#), 56.

2034 Submission to the Discussion Paper: [Privcore](#), 2.

2035 Submission to the Discussion Paper: [Australian Privacy Foundation](#), 15.

2036 Submission to the Discussion Paper: [Law Council of Australia](#), 22.

2037 Submission to the Discussion Paper: [Workday](#), 4.

2038 Submission to the Discussion Paper: [Australian Information Industry Association](#), 4.

2039 Submissions to the Discussion Paper: [Microsoft](#), 3; [Salesforce](#), 2.

2040 Submissions to the Discussion Paper: [Australian Communications Consumer Action Network](#), 17; [Telstra](#), 24.

2041 Submission to the Discussion Paper: [BSA | The Software Alliance](#), 6-7.

2042 Submission to the Discussion Paper: [Atlassian](#), 4.

There was strong support for processors to be subject to organisational accountability (APP 1)²⁰⁴³ and security (APP 11.1) requirements.²⁰⁴⁴ Submitters also noted that obligations of processors should be controlled through documented instructions, such as a contract that sets out the obligations of the controller and processor.²⁰⁴⁵ A contract could alleviate any concerns about processors being subject to limited APPs (such as mandatory clauses limiting further use and disclosure of personal information beyond the terms of the contract).

22.2.1 Proposal – introduce a partial controller-processor distinction

Feedback highlights that distinguishing between controllers and processors in terms of their obligations under the Act would be beneficial for industry and individuals. In particular, it would clarify compliance for entities by allocating responsibilities between entities and provide individuals with greater clarity about which entity has primary responsibility for their personal information. Nevertheless, the current scope of the Act (particularly the small business exemption) complicates the introduction of an economy wide controller-processor distinction.

Expanding the scope of the Act to capture all businesses regardless of annual turnover would allow for the wholesale adoption of the concepts of controllers and processors in the Act. However, as noted in Chapter 6, it is proposed that the small business exemption should only be removed once appropriate supports are put in place to enable small business to comply with the obligations under the Act. In practice, this means it is likely that other proposals put forward by the Review would be implemented before the coverage of the Act was expanded. If a distinction between controllers and processors was not introduced until the small business exemption was removed, proposals put forward in other chapters (particularly Chapter 18) would be likely to create considerable complexity in terms of complying with those new obligations for those APP entities that would otherwise be considered processors.

In response, it is proposed that, pending removal of the small business exemption, the controller-processor distinction should be introduced into the Act with relevant obligations to apply to each entity, such that entities that are not otherwise regulated by the Act would be covered if they process personal information for an APP entity controller. That is, if a small business is engaged to process personal information on behalf of an APP entity controller, they would need to comply with the proposed processor obligations under the Act.

This proposal would be similar to the *Californian Consumer Privacy Act* (CCPA) which has a threshold for an entity to be declared a 'business' for the purposes of the Act. Notwithstanding this, the CCPA introduces two types of entities – businesses (controllers) and service providers (processors). Under the CCPA, a business is any legal entity that operates for profit in California, meets at least one of the CCPA's three thresholds, and determines the purposes and means of the processing of personal information.²⁰⁴⁶ A service provider is any legal entity that, operates for profit, receives personal information from a business, processes personal information on behalf of a business and operates under a service provider contract.²⁰⁴⁷

A service provider processes personal information on behalf of a business under a contract. Under the contract, personal information received by the service provider from the business may not be retained, used, or disclosed except for the purposes of the contract or any other purposes permitted under the CCPA.²⁰⁴⁸ Operating under a contract means that a service provider is strictly limited in its functions, and only exists to provide specified services, to specified businesses, with specified sets of personal information. There are no obligations placed on a service provider when the business is not subject to the CCPA. For example, if a controller not subject to the CCPA sends personal information to a processor, neither the controller or the processor would be subject to the CCPA.

There would be a degree of complexity in adopting the controller-processor distinction as proposed. In the short-term, small businesses that act as processors would be required to comply with APP 1, APP 11 and NDB scheme obligations despite the small business exemption. There would also be a gap in coverage where a non-APP entity, such as a small business contracts an APP entity processor. In this circumstance, the non-APP entity would not be subject to the Act while the APP entity processor would only be required to comply with the processor obligations. Neither entity would be required to comply with controller obligations. For example, if a small business contracted an APP entity processor, neither entity would be required to respond to an individual's request to access their personal information. However, the APP entity processor would still be required to comply with the Act in full when it was not acting as a processor.

2043 Submissions to the Discussion Paper: [Association for Data-Driven Marketing and Advertising](#), 33; [OAIC](#), 177.

2044 Submissions to the Discussion Paper: [BSA | The Software Alliance](#), 6; [Atlassian](#), 4; [Association for Data-Driven Marketing and Advertising](#), 33; [OAIC](#), 177; [ResMed](#), 5.

2045 Submissions to the Discussion Paper: [BSA | The Software Alliance](#), 6; [OAIC](#), 177; [Calabash Solutions](#), 22.

2046 *California Civil Code* § 1798.140.

2047 *Ibid.*

2048 *Ibid.*

However, this is unlikely to reduce privacy protection for individuals. Compliance is currently problematic when a non-APP entity engages an APP entity under a contract to process personal information. As discussed earlier in this chapter, where an APP entity in the role of processor does not have a direct relationship with an individual, it may not be practicable for the entity to fulfil obligations imposed by the APPs. This additional complexity would cease if or when small businesses are brought within the scope of the Act.

A proposed table of obligations for APP entity controllers and APP entity processors based on the current APPs is set out below.

APPs and other obligations under the Act	APP entity controller	APP entity processor
APP 1: Open and transparent management of personal information	Yes	Yes
APP 2: Anonymity and pseudonymity	Yes	No
APP 3: Collection of solicited personal information	Yes	No
APP 4: Dealing with unsolicited personal information	Yes	No
APP 5: Notification of the collection of personal information	Yes	No
APP 6: Use or disclosure of personal information	Yes	No
APP 7: Direct marketing	Yes	No
APP 8: Cross border disclosure of personal information	Yes	No
APP 9: Adoption, use or disclosure of government related identifiers	Yes	No
APP 10: Quality of personal information	Yes	No
APP 11: Security of personal information	Yes	Yes
APP 12: Access to personal information	Yes	No
APP 13: Correction of personal information	Yes	No
Reporting under the NDB scheme	Yes (reporting to OAIC and individuals)	Yes (reporting to OAIC and controller)

There would need to be further engagement with small business to determine the extent to which small businesses are effectively operating as processors for APP entities now, and accordingly, what impact this proposal might have on small business, including what support they would need.

22.1 Introduce the concepts of APP entity controllers and APP entity processors into the Act.

Pending removal of the small business exemption, a non-APP entity that processes information on behalf of an APP entity controller would be brought into the scope of the Act in relation to its handling of personal information for the APP entity controller. This would be subject to further consultation with small business and an impact analysis to understand the impact on small business processors.

23. Overseas data flows

The free flow of information across borders is an increasingly important component of international trade and digital service models.²⁰⁴⁹ It is estimated that international data flows will add \$11 trillion to the global economy by 2025.²⁰⁵⁰ McKinsey Global Institute estimates the value of data flows has overtaken the value of global trade in physical goods.²⁰⁵¹ At the same time, concerns about the privacy risks of international data transfers continue to grow. Social media platform TikTok has recently attracted media attention due to the possibility of Australians' data being accessed in China.²⁰⁵² Similarly, the Court of Justice of the European Union's decision in '*Schrems II*' has raised concerns about the ability for the United States Government to access data of EU citizens transferred to the US.²⁰⁵³

The Discussion Paper sought feedback on a number of proposals related to overseas data flows, including proposals to better facilitate overseas disclosures of personal information, provide individuals with greater transparency about overseas disclosures of personal information and ensure that information disclosed overseas is safeguarded by appropriate privacy protections.

23.1 Extraterritorial application

The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Privacy Enforcement Bill) simplified the extraterritorial operation of the Act to ensure it is fit for a global and digital world. The Privacy Enforcement Bill passed both houses of Parliament on 28 November 2022, and commenced on 13 December 2022.

Previously, foreign organisations or small business operators had to meet the obligations under the Act if they had an 'Australian link',²⁰⁵⁴ being:

1. the organisation or operator carries on business in Australia or an external Territory, and
2. the personal information was collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice.

The Privacy Enforcement Bill removed the requirement for an organisation or operator to collect or hold personal information in Australia in order to have an 'Australian link'. With the evolution of technology, it can be difficult to establish that foreign organisations collect or hold personal information in Australia – for example, they may collect personal information from a digital platform that does not have servers in Australia, and transfer it to other entities overseas for processing and storage.

The OAIC's submission to the Issues Paper noted that an increasing number of matters being considered by the IC present situations that enliven these provisions.²⁰⁵⁵ The submission outlined the practical difficulties in establishing that a foreign organisation has collected information directly from Australia, and noted that it can be resource intensive to establish jurisdiction over motivated and well-resourced international companies.²⁰⁵⁶

23.1.1 The Senate Legal and Constitutional Affairs Legislation Committee report

On 27 October 2022, the Senate referred the provisions of the Privacy Enforcement Bill to the Senate Legal and Constitutional Affairs Legislation Committee (the committee) for inquiry and report by 22 November 2022. The committee received 32 submissions, and held a public hearing on 17 November 2022. In its report the committee recommended that the Privacy Enforcement Bill be passed, subject to two recommendations. Recommendation 2 was that, as part of this Review, the Attorney-General's Department examine the appropriateness of section 5B providing for any additional 'Australian link'.²⁰⁵⁷

²⁰⁴⁹ Submission to the Issues Paper: [OAIC](#). By some estimates, cross-border data flows contribute around \$USD 2.8 trillion to global economic activity, or 3.5 per cent of global GDP. See: McKinsey Global Institute, 'Digital Globalization: The new era of global flows', McKinsey & Company (2016).

²⁰⁵⁰ Joshua P Meltzer and Peter Lovelock, 'Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia' (2018).

²⁰⁵¹ McKinsey Global Institute, 'Digital Globalization: The new era of global flows', McKinsey & Company (2016).

²⁰⁵² Jake Evans, '[TikTok admits Australian data can be accessed in China, prompting warnings app may be compromised](#)', ABC News (13 July 2022).

²⁰⁵³ Norton Rose Fulbright, '[Schrems II landmark ruling: A detailed analysis](#)' (Web Page, July 2020).

²⁰⁵⁴ Privacy Act s 5B(3).

²⁰⁵⁵ Submission to the Issues Paper: [OAIC](#), 113.

²⁰⁵⁶ Submission to the Issues Paper: [OAIC](#), 114.

²⁰⁵⁷ Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 [Provisions]* (2022) vii.

The committee noted that they support the amendment in principle, but acknowledged the argument raised by submitters that the extraterritorial operation had been too broadly drafted and must retain some connection with Australians' information, as is the case in GDPR.²⁰⁵⁸

A number of submitters to the committee expressed support for the amendment to the extraterritorial operation of the Act.²⁰⁵⁹ Digital Rights Watch, CHOICE and Electronic Frontiers noted that the amendment would help fix any loopholes foreign organisations may use to avoid meeting the requirements of the Act,²⁰⁶⁰ with Electronic Frontiers noting that 'Australians should expect data about them to be kept safe no matter how it came to be in the possession of an organisation'. The OAIC noted that the amendment would ensure consistency with other domestic legislative frameworks, and CHOICE and Digital Rights Watch noted it would bring the Act closer in line with international counterparts such as GDPR.²⁰⁶¹

However, some submitters did not support the amendment and were concerned that it would dilute the 'Australian link' test,²⁰⁶² which may have the effect that the Act regulates the handling of personal information that has no direct connection with Australia or Australians. The Business Council of Australia and the Law Council of Australia noted it risked bringing Australian laws into conflict with requirements made in other jurisdictions.²⁰⁶³ The Law Council of Australia, the Australian Privacy Foundation and Privacy 108 argued that the Act should align with the approach adopted by the GDPR.²⁰⁶⁴

Approaches in the domestic and international context

Section 5 of the *Competition and Consumer Act 2010* and section 12AC of the *Australian Securities and Investments Commission Act 2001* extend the application of parts of the applicable acts to bodies corporate that carry on a business in Australia. The courts have held that the expression 'carrying on business' when used to establish jurisdiction will have a meaning informed by the requirement to ensure there is sufficient connection with the country asserting jurisdiction, and 'requires resort to the usual and ordinary meaning of the phrase and invites a factual inquiry'.²⁰⁶⁵ Relevant factors have included:

- acts within the relevant territory that amount to, or are ancillary to, transactions that make up or support the business, and²⁰⁶⁶
- activities engaged in for the purpose of profit on a continuous and repetitive basis - for that reason, courts have said that participation in a single transaction or a series of isolated transactions will not satisfy this aspect of the test.²⁰⁶⁷

In New Zealand, the NZ Privacy Act extends to foreign organisations in relation to any action taken by the organisation in the course of carrying on business in New Zealand in respect of personal information collected or held by that foreign organisation. The Act notes it does not matter where the personal information is or was collected, where the personal information is held, or where the individual concerned is or was located. Further, the Act notes an organisation may be treated as carrying on a business in New Zealand without necessarily being a commercial operation, having a place of business in New Zealand, receiving monetary payment for the supply of goods or services, or intending to make a profit from its business in New Zealand.

In the EU, the GDPR extends to controllers or processors who are not established in EU if they process personal data of data subjects who are in the EU, and the processing activities are related to:

- offering goods or services to data subjects in the EU (regardless of whether payment is required), or
- monitoring the behaviour of data subjects in the EU, in so far as their behaviour takes place within the EU (for example, behavioural advertising, marketing surveys).

2058 Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 [Provisions]* [2022] 38.

2059 [Submissions](#) to the Senate Legal and Constitutional Affairs Legislation Committee: Electronic Frontiers; Digital Rights Watch; CHOICE; Dr Bruce Baer Arnold; Dr Elizabeth Coombs; OAIC.

2060 [Submissions](#) to the Senate Legal and Constitutional Affairs Legislation Committee: CHOICE, 2; Digital Rights Watch, 4.

2061 [Submissions](#) to the Senate Legal and Constitutional Affairs Legislation Committee: OAIC, 1; CHOICE, 2; Digital Rights Watch, 4; Electronic Frontiers, 6.

2062 [Submissions](#) to the Senate Legal and Constitutional Affairs Legislation Committee: Australian Privacy Foundation; BSA: Software Alliance; Business Council of Australia; DIGI, Law Council of Australia; Tech Council of Australia.

2063 [Submissions](#) to the Senate Legal and Constitutional Affairs Legislation Committee: Business Council Australia, 8; Law Council of Australia, 9.

2064 [Submissions](#) to the Senate Legal and Constitutional Affairs Legislation Committee: Law Council of Australia, 9; Australian Privacy Foundation, 2; Privacy 108, 4.

2065 *Tiger Yacht Management Ltd v Morris* [2019] FCAFC 8 at [50].

2066 *Gebo Investments (Labuan) Ltd v Signatory Investments Pty Ltd; Application of Campbell & Ors* [2005] NSWSC 544 at [31].

2067 *Australian Competition and Consumer Commission v Valve Corporation [No 3]* [2016] FCA 196 at [177].

The GDPR defines a data subject as a natural person, and is not limited to EU citizens. The European Data Protection Board Guidelines note:²⁰⁶⁸

- The requirement that the data subject be located in the EU must be assessed at the moment when the relevant trigger activity takes place, i.e. at the moment of offering of goods or services or the moment when the behaviour is being monitored, regardless of the duration of the offer made or monitoring undertaken.
- Processing personal data of an individual in the EU alone is not sufficient to trigger the application of the GDPR. The element of 'targeting' individuals in the EU, either by offering goods or services to them or by monitoring their behaviour must always be present in addition. Inadvertent or incidental provision of services to an individual who happens to be in the EU is not enough – for example if a United States citizen travelling through EU using an app offered by a United States company that is directed at the United States market.
- 'Offering goods and services' is more than providing mere access to a website, email address or using the language that is generally used in the country in which the controller is established.

In Canada, the *Personal Information Protection and Electronic Documents Act* is silent on the extraterritorial operation. However, the court has held that it may extend to foreign organisations if there is a real and substantial connection to Canada. The court has stated that the operative question underlying the test is 'whether there is sufficient connection between this country and the [activity] in question for Canada to apply its law consistent with the principles of order and fairness and international comity'.²⁰⁶⁹

Additional 'Australian link'

The current extraterritorial operation of the Act (as amended by the Privacy Enforcement Bill) ensures there is sufficient connection with Australia, through the requirement that the entity will need to 'carry on a business' in Australia. However, there would be benefit in further clarifying that foreign organisations will only be regulated to the extent that their handling of personal information has a connection to Australia. This would assist foreign organisations understand their obligations.

Any additional 'Australian link' would need to be designed in a way that prevents foreign organisations from using loopholes due to advances in technology, and could not be dependent on the means or method of collection or storage of personal information.

Further, it could not be limited to the protection of Australian citizens or residents only. The Enhancing Privacy Protection Bill extended the protection of the Privacy Act to every person, not just Australian citizens or permanent residents, so long as the entity that is dealing with an individual's personal information is an agency or an organisation with an Australian link. This change ensured that the Act applied to foreign organisations that carry on a business in Australia, but handle the personal information of foreign citizens or residents – for example an international hotel chain.

Further clarity may be achieved by requiring that foreign organisations or operators must meet the obligations under the Privacy Act if they have an 'Australian link', being:

1. the organisation or operator carries on business in Australia or an external Territory, and
2. the act done or practice engaged in relates to personal information that is **connected to Australia**.

The expression 'connected to Australia' would have its ordinary meaning, and could involve consideration of whether:

- the personal information is collected or held in Australia; or
- the personal information is of an Australian or other individual physically located in Australia.

This would make it clear on the face of the Act that the extraterritorial operation is not dependent on the means or method of collection or storage. However, any new provision to clarify the 'Australian link' should be subject to careful consideration and further consultation to ensure that it does not have any unintended consequences – such as excluding an entity from the OAIC's jurisdiction that Australians would expect to be covered.

²⁰⁶⁸ European Data Protection Board, [Guidelines 3/2018 on the territorial scope of the GDPR \(Article 3\)](#) (12 November 2019).

²⁰⁶⁹ A.T. v Globe24h.com [2017] 4 FCR 310 at [52].

23.1 Consult on an additional requirement in subsection 5B(3) to demonstrate an ‘Australian link’ that is focussed on personal information being connected with Australia.

23.2 Overview of APP 8

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.²⁰⁷⁰

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.²⁰⁷¹ 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 is taken to have been done by the APP entity and to be a breach of the APPs by the APP entity.²⁰⁷²

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.²⁰⁷³ APP 8.2 provides a number of exceptions to this framework.

Submitters generally expressed support for the accountability approach of APP 8 and section 16C and noted that it creates awareness for data protection during cross-border disclosures.²⁰⁷⁴ However, the European Commission’s submission to the Discussion Paper suggested the accountability approach creates legal uncertainty for companies and individuals and could hamper enforcement.²⁰⁷⁵ Submitters suggested a number of amendments to APP 8 to enhance the operation of APP 8 and section 16C to better protect consumers and support entities disclosing information overseas.

23.2.1 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.²⁰⁷⁶ Submissions to the Issues Paper expressed concern that the current approach places the burden on an APP entity to determine whether overseas laws are ‘substantially similar’ to the APPs,²⁰⁷⁷ and noted that entities have difficulty undertaking this assessment.²⁰⁷⁸

2070 Privacy Act s 2A(f).

2071 Ibid sch 1, APP 8.1. Note APP 8.1 refers to a breach of the APPs with the exception of APP 1.

2072 Ibid s 16C.

2073 OAIC, [APP Guidelines](#) (July 2019) [8.58].

2074 [Discussion Paper](#), 160; 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.

2075 Submission to the Discussion Paper: [European Commission](#), 4.

2076 Privacy Act sch 1, APP 8.2(a).

2077 [Discussion Paper](#), 160; Submissions to the Issues Paper: [Calabash Solutions](#), 10; [CSIRO](#), 9; [KPMG](#), 18; [Experian](#), 22.

2078 Submissions to the Issues Paper: [Calabash Solutions](#), 10; [Cyber Security Cooperative Research Centre](#), 10–11; [Dr Kate Mathews Hunt](#), 13; [Griffith University](#), 18; [Experian](#), 22; [Gadens](#), 11.

Discussion Paper proposal – introduce a mechanism to prescribe countries and certification schemes

The Discussion Paper sought feedback on a proposal to amend the Act to introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a). A large number of submissions supported the proposal,²⁰⁷⁹ and suggested this would provide APP entities with greater certainty when disclosing personal information overseas and would allow consumers to make informed choices about where their information was disclosed.²⁰⁸⁰ The OAIC emphasised the importance of ensuring effective enforcement mechanisms for breaches by overseas entities.²⁰⁸¹

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.²⁰⁸² New Zealand has introduced a similar mechanism to enable countries with privacy laws that provide comparable safeguards to be prescribed.²⁰⁸³ The NZ Privacy 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.²⁰⁸⁴ The New Zealand Ministry of Justice undertook a public consultation on which countries should be prioritised for prescription in late 2020 but no countries have yet been prescribed as providing comparable safeguards.

The UK government announced that it is prioritising an adequacy assessment for Australia as part of its review of international data protection laws post-Brexit for the purpose of determining whether to grant Australia adequacy with the UK GDPR (as distinct from an EU GDPR adequacy decision).²⁰⁸⁵

The proposed mechanism to prescribe countries with substantially similar protection to the APPs could provide an avenue for mutual recognition of data protection laws. Entities would still be able to make an independent assessment of a country's privacy laws under APP 8.2(a) for non-prescribed countries to determine if information would be afforded substantially similar protections in the circumstances.

The OAIC submitted that certification schemes are likely to be considered binding schemes for the purpose of APP 8.2(a), provided the certification has a binding effect and enables individuals to seek redress.²⁰⁸⁶ This could be used as a mechanism to implement the Cross-Border Privacy Rules (CBPR) system, discussed further in Chapter 24. Some submitters suggested the CBPR system should not be prescribed and expressed concern about the effectiveness of the CBPR system's enforcement mechanisms.²⁰⁸⁷

23.2 Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).

2079 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. Submissions to the Discussion Paper: [Telstra](#), 25; [Australian Information Industry Association](#), 5; [KPMG](#), 28; [Calabash Solutions](#), 22; [Uniting Church in Australia](#), [Synod of Victoria and Tasmania](#), 12; [Atlassian](#), 5; [Avant Mutual](#), 17; [MIGA](#), 8; [DIGI](#), 24; [Federal Chamber of Automotive Industries](#), 27; [Australian Council on Children and the Media](#), 9; [Murdoch Children's Research Institute](#), 8; [Australian Institute of Health and Welfare](#), 9; [Australian Medical Association](#), 16; [Optus](#), 27; [Equifax](#), 15–16; [Workday](#), 5–6; [elevenM](#), 57; [OAIC](#), 180; [CPA Australia](#), 4; [Twilio](#), 2; [CSIRO](#), 12; [Meta](#), 8; [Privacy 108](#), 39; [Communications Alliance](#), 17; [Information Technology Industry Council](#), 5; [Western Union](#), 10.

2080 Submissions to the Issues Paper: [AGL Energy Limited](#), 4; [Financial Rights Legal Centre](#), [Consumer Action Law Centre and Financial Counselling Australia](#), 42–3; [ANZ](#), 15; [Atlassian](#), 5. Submissions to Discussion Paper: [Calabash Solutions](#), 22; [Optus](#), 27; [Equifax](#), 15–16; [Workday](#), 5–6; [elevenM](#), 57; [OAIC](#), 180; [CPA Australia](#), 4; [Social Services Portfolio](#), 29–30; [Twilio](#), 2.

2081 Submission to the Discussion Paper: [OAIC](#), 180.

2082 GDPR art 45.

2083 NZ Privacy Act s 214.

2084 NZ Privacy Act s 214(3).

2085 UK Department for Digital, Culture, Media and Sport, [International data transfers: building trust, delivering growth and firing up innovation](#) (Web Page, 26 August 2021).

2086 Submission to the Issues Paper: [OAIC](#), 111. Also raised by [illion](#), 6.

2087 Submissions to the Discussion Paper: [Graham Greenleaf](#), 6; [Dr Katharine Kemp, UNSW Sydney](#), 19.

Discussion Paper proposal – introduce standard contractual clauses

The Discussion Paper proposed making standard contractual clauses (SCCs) available to APP entities for use when transferring personal information overseas, which contain provisions stipulating how an overseas recipient of personal information is expected to handle that information so as not to breach the APPs. These clauses would be able to be used by APP entities to facilitate disclosures to overseas entities located in countries that are not prescribed. Submitters expressed strong support for SCCs²⁰⁸⁸ and suggested the proposal would reduce regulatory burden for APP entities.²⁰⁸⁹

Some submitters suggested it should be clarified that the use of SCCs would not be mandatory to disclose information overseas,²⁰⁹⁰ and that SCCs be developed in consultation with the private sector to ensure they are fit for purpose.²⁰⁹¹ The Federal Chamber of Automotive Industries recommended the use of SCCs should be considered compliance with the relevant requirements of the Act. However, the OAIC recommended the use of SCCs should support compliance with APP 8.1 rather than being recognised as a mechanism through which compliance with APP 8.2 is established.²⁰⁹²

The New Zealand Office of the Privacy Commissioner has published model contract clauses to assist New Zealand entities in meeting their privacy obligations under the New Zealand equivalent of APP 8 when disclosing personal information to overseas recipients.²⁰⁹³ SCCs are used under the GDPR to ensure adequate privacy protections continue to apply to personal data transferred outside of the EU.²⁰⁹⁴ The UK also provides SCCs for international data transfers from the UK to countries without 'essentially equivalent' privacy laws.²⁰⁹⁵ Submitters suggested SCCs should be designed in a way that is interoperable with the clauses developed by other jurisdictions to avoid organisations being required to enter into multiple SCCs.²⁰⁹⁶

23.3 Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.

23.2.2 Exception – informed consent

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.²⁰⁹⁷ Where an entity has obtained express consent under APP 8.2, it is not required to take reasonable steps to ensure that the overseas recipient does not breach the APPs. 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.²⁰⁹⁸

2088 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. Submissions to the Discussion Paper: [Telstra](#), 25; [KPMG](#), 28; [Calabash Solutions](#), 23; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 12; [Atlassian](#), 5; [Department of Health \(Cth\)](#), 16; [Avant Mutual](#), 17; [MIGA](#), 8; [DIGI](#), 24; [Federal Chamber of Automotive Industries](#), 27; [Australian Council on Children and the Media](#), 9; [Australian Institute of Health and Welfare](#), 9; [Australian Medical Association](#), 16; [Optus](#), 27; [Workday](#), 6; [elevenM](#), 57-58; [OAIC](#), 181; [CPA Australia](#), 4; [Social Services Portfolio](#), 29-30; [Twilio](#), 2; [European Commission](#); [Australian Banking Association](#), 28; [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 10; [CSIRO](#), 12; [Meta](#), 8; [Privacy 108](#), 39; [ResMed](#), 5; [Communications Alliance](#), 17; [FinTech Australia](#), 16; [Information Technology Industry Council](#), 5; [Western Union](#), 10-11; [National Health and Medical Research Council](#), 3.

2089 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. Submissions to the Discussion Paper: [Atlassian](#), 5; [Department of Health \(Cth\)](#), 16; [Optus](#), 28; [elevenM](#), 58; [CPA Australia](#), 4; [Twilio](#), 2.

2090 Submissions to the Discussion Paper: [Telstra](#), 25; [Australian Information Industry Association](#), 5; [Australian Medical Association](#), 16; [Australian Banking Association](#), 28; [Communications Alliance](#), 17; [Information Technology Industry Council](#), 5.

2091 Submissions to the Discussion Paper: [Twilio](#), 2; [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 10; [Information Technology Industry Council](#), 5.

2092 Submission to the Issues Paper: [OAIC](#); Submission to the Discussion Paper: [OAIC](#), 181.

2093 New Zealand Privacy Commissioner, [Model Clause Agreement Builder](#) (Web Page).

2094 GDPR art 46.

2095 UK ICO, [International data transfer agreement and guidance](#) (Web Page, 17 November 2022).

2096 Submissions to the Discussion Paper: [Telstra](#), 25; [FinTech Australia](#), 16.

2097 Privacy Act sch 1, APP 8.2(b).

2098 OAIC, [APP Guidelines](#) (July 2019) [8.32].

Discussion Paper proposal – remove the exception to accountability where consent is obtained

The Discussion Paper proposed removing the informed consent exception in APP 8.2(b). This was in response to concerns about the effectiveness of consent and submitter feedback that retaining the consent exception could 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. A number of submissions supported the proposal,²⁰⁹⁹ and suggested the 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.²¹⁰⁰ The OAIC submitted that expecting individuals to understand and consent to complex overseas data flows may be impracticable, which limits the value of consent.²¹⁰¹

A large number of submitters did not support the proposal,²¹⁰² on the basis that informed consent is often relied on for data transfers.²¹⁰³ Submissions suggested informed consent is a useful mechanism in circumstances where decisions and relationships are being managed at an individual level²¹⁰⁴ and that removing the exception would increase the regulatory burden for entities that rely on the exception.²¹⁰⁵ The Communications Alliance submitted that the exception provides a mechanism for transfers in scenarios where alternative arrangements are not available, but the transfer may be desirable from a consumer perspective. For example, a travel agent would likely need to transfer personal information of travellers to entities in a foreign country. If the informed consent exception were removed, and other transfer mechanisms were not available, this would impede the travel agent's ability to carry out their business and would inconvenience consumers.²¹⁰⁶

The Communications Alliance suggested it would be more useful to strengthen the notice requirements to ensure individuals are adequately informed about the potential risks of a disclosure.²¹⁰⁷ Similarly, Optus submitted that individuals should continue to be able to provide consent to overseas disclosures against the backdrop of the additional safeguards in the proposed fair and reasonable test, the requirement that consent be voluntary, informed, current and specific and the proposal to increase transparency in relation to overseas disclosures.²¹⁰⁸

Submitters also raised concerns about the proposal's potential impact on research.²¹⁰⁹ Murdoch Children's Research Institute noted that consent is often the simplest way to deal with potential overseas disclosures for global research studies and sharing research data with overseas collaborators.²¹¹⁰ Submissions also noted that the proposal would have impacts on websites that publish personal information.²¹¹¹ CSIRO suggested there may not be an ability to enforce contractual measures when undertaking research in countries without equivalent privacy laws.²¹¹²

Atlassian noted that an equivalent exception is available under GDPR.²¹¹³ Entities are able to transfer personal data to a country without an adequacy decision if an individual has explicitly consented to the proposed transfer, after having been informed of the possible risks of the transfer for the individual due to the absence of an adequacy decision and appropriate safeguards.²¹¹⁴ New Zealand entities are also able to disclose personal information overseas with the permission of an individual after the individual has been expressly informed that their information may not be given the same protection as provided by the NZ Privacy Act.²¹¹⁵ In light of submitter feedback, it is proposed that the informed consent be retained, with a requirement that disclosing entities consider the risks of an overseas disclosure and specifically inform individuals of any risks.

2099 Submissions to the Discussion Paper: [Calabash Solutions](#), 23; [Avant Mutual](#), 17; [Australian Council on Children and the Media](#), 9; [Australian Institute of Health and Welfare](#), 10; [Australian Medical Association](#), 16; [elevenM](#), 58; [OAIC](#), 183; [Meta8](#); [Illion](#), 3; [Benevolent Society](#), 6.

2100 Submissions to the Issues Paper: [Australian Privacy Foundation](#), 42–3; [Dr Kate Mathews Hunt](#), 13. Submissions to the Discussion Paper: [Calabash Solutions](#), 23; [elevenM](#), 58; [Illion](#), 3; [Benevolent Society](#), 6; [OAIC](#), 183.

2101 Submission to the Discussion Paper: [OAIC](#), 183.

2102 Submissions to the Discussion Paper: [Australian Information Industry Association](#), 5; [Atlassian](#), 5; [MIGA](#), 9; [Murdoch Children's Research Institute](#), 9; [Optus](#), 28; [Twilio](#), 2; [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 10; [Communications Alliance](#), 17–18; [Salinger Privacy](#), 41–42; [Australian Communications Consumer Action Network](#), 17; [BSA | The Software Alliance](#), 11; [Global Data Alliance](#), 2; [Australian Financial Markets Association](#), 10.

2103 Submission to the Discussion Paper: [Google](#), 6.

2104 Submissions to the Discussion Paper: [Salinger Privacy](#), 41–42; [Australian Communications Consumer Action Network](#), 17.

2105 Submissions to the Discussion Paper: [BSA | The Software Alliance](#), 11; [Global Data Alliance](#), 2.

2106 Submission to the Discussion Paper: [Communications Alliance](#), 17–18; the [OAIC](#), at 183, also noted that consent is used in the overseas travel and tourism industry.

2107 Submission to the Discussion Paper: [Communications Alliance](#), 18.

2108 Submission to the Discussion Paper: [Optus](#), 28.

2109 Submissions to the Discussion Paper: [Murdoch Children's Research Institute](#), 9; [CSIRO](#), 12–13; [Australian Genomics](#), 6; [Geoscience Australia](#), 6–7.

2110 Submission to the Discussion Paper: [Murdoch Children's Research Institute](#), 9.

2111 Submissions to the Discussion Paper: [Department of Health \(Cth\)](#), 16; [CSIRO](#), 13; [Geoscience Australia](#), 6–7.

2112 Submission to the Discussion Paper: [CSIRO](#), 13.

2113 Submission to the Discussion Paper: [Atlassian](#), 5; GDPR art 49.

2114 GDPR art 49.

2115 NZ Privacy Act IPP 12.

23.4 Strengthen the informed consent exception to APP 8.1 by requiring entities to consider the risks of an overseas disclosure and to inform individuals that privacy protections may not apply to their information if they consent to the disclosure.

Discussion Paper proposal – strengthen notice requirements

APP entities are required to give notice that they are likely to disclose an individual's personal information to an overseas recipient.²¹¹⁶ The APP Guidelines state 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 be aware of.²¹¹⁷ Under APP 1, entities are also required to include information about whether the entity is likely to disclose personal information to overseas recipients in their privacy policy.²¹¹⁸

The Discussion Paper proposed limiting the amount of information in collection notices to improve individuals' comprehension of information relevant to a particular collection of personal information, and proposed that the 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. The Discussion Paper also sought feedback on a proposal to strengthen transparency requirements in relation to potential overseas disclosures by including the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas, in an entity's up-to-date APP privacy policy required to be kept under APP 1.3.

A number of submitters expressed support for these proposals.²¹¹⁹ elevenM suggested the proposal would allow individuals to better understand how their personal information was moving and better understand any risks.²¹²⁰ Other submitters did not support the proposals,²¹²¹ and suggested that including more granular detail in privacy policies would increase their complexity and the burden on customers to understand them and would require regular updates.²¹²² Submissions also noted that privacy policies are designed to address arrangements that are in place for all customers and overseas disclosures may not universally apply across the customer base.²¹²³ It was considered that setting out all countries to which information may be disclosed could potentially add to confusion, rather than provide clarity²¹²⁴ and would not be effective in achieving the purpose of transparency relevant to a specific individual's interaction with an entity.²¹²⁵

In light of submitter feedback, it is proposed that entities be required to include information about overseas disclosures in an APP 5 notice instead of a privacy policy. Entities would be required to specify the overseas locations of entities to which personal information would be disclosed as well as the types of personal information that may be disclosed to those overseas recipients. Combined with proposal 23.4, this would give APP entities flexibility when disclosing information overseas and allow individuals to make informed decisions about how their personal information is handled.

Stakeholder feedback on the Discussion Paper proposal to reduce the number of matters in collection notices is considered in Chapter 10. It concludes that the matters for inclusion in collection notices as set out in APP 5.2 should be retained with some additional matters as a result of proposals in this Report, including specifying the types of personal information which may be disclosed to recipients located overseas as per this proposal.

2116 Privacy Act sch 1, APP 5.2(i).

2117 OAIC, [APP Guidelines](#) (July 2019) [5.33].

2118 Privacy Act sch 1, APP 1.4(f).

2119 Submissions to the Discussion Paper: [Calabash Solutions](#), 23; [Department of Health \(Cth\)](#), 17; [Avant Mutual](#), 17; [Australian Council on Children and the Media](#), 9; [Australian Institute of Health and Welfare](#), 10; [elevenM](#), 58; [OAIC](#), 184; [Meta](#), 8; [Privacy 108](#), 40.

2120 Submission to the Discussion Paper: [elevenM](#), 58-59.

2121 Submissions to the Discussion Paper: [Australian Information Industry Association](#), 5; [MIGA](#), 9; [Australian Banking Association](#), 28; [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 10; [Australian Financial Markets Association](#), 10-11; [National Australia Bank](#), 6.

2122 Submissions to the Discussion Paper: [Australian Medical Association](#), 17; [Australian Banking Association](#), 28; [Australian Financial Markets Association](#), 11; [National Australia Bank](#), 6.

2123 Submissions to the Discussion Paper: [Australian Banking Association](#), 28; [National Australia Bank](#), 6.

2124 Submissions to the Discussion Paper: [Australian Banking Association](#), 28; [National Australia Bank](#), 6.

2125 Submission to the Discussion Paper: [Australian Banking Association](#), 28.

23.5 Strengthen APP 5 in relation to overseas disclosures by requiring APP entities, when specifying the countries in which recipients are likely to be located if practicable, to also specify the types of personal information that may be disclosed to recipients located overseas.

23.2.3 Use versus disclosure

APP 8 explicitly applies to ‘disclosure’ of personal information to overseas recipients rather than to overseas ‘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.²¹²⁶

APP 8 is not intended to apply ‘where personal information is routed through servers outside Australia. However, entities are still required to take a risk management approach to ensure that personal information routed overseas is not accessed by third parties. If the information is accessed by a third party, this will be a disclosure subject to the Act’.²¹²⁷

The requirements of APP 8 apply where an APP entity contracts a function to an overseas entity. The chain of accountability for the APP entity will not be broken if that overseas contractor then engages a subcontractor. However, submitters raised concerns that the application of APP 8 to transfers of personal information to cloud service providers is unclear²¹²⁸ as it is difficult to distinguish between a ‘use’ and a ‘disclosure’ where these terms are not defined in the Act.²¹²⁹

23.2.4 Data localisation

Some submitters were of the view that APP 8 and section 16C should apply to any movement of personal information outside Australia.²¹³⁰ This would be consistent with the approach adopted in the GDPR, which imposes obligations on all forms of data processing, including storage.²¹³¹ Prior to the introduction of APP 8, cross border transfers were prohibited unless there were adequate protections in place.²¹³² The suggestion to extend APP 8 to all 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.²¹³³ 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 rights and access justice for overseas privacy infringements.²¹³⁴

As noted in the Department of Home Affairs’ National Data Security Action Plan discussion paper, data localisation requirements can protect sensitive information or information which may pose national security threats if transferred overseas.²¹³⁵ For example, data localisation requirements are present in the MHR Act, which prevents registered operators and service providers from storing, transferring, processing or handling My Health Record information outside Australia. Information collected by the COVIDSafe App was also required to be stored in Australia. However, local storage of data cannot in itself guarantee security.²¹³⁶ This was supported by submissions that suggested

²¹²⁶ Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 83.

²¹²⁷ Ibid.

²¹²⁸ 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.

²¹²⁹ Submissions to the Issues Paper: [CSIRO](#), 9; [Roche](#), 8; [Interactive Games and Entertainment Association](#), 18; [Avant Mutual](#), 14.

²¹³⁰ Submissions to the Issues Paper: [Calabash Solutions](#); Submissions to the Discussion Paper: [Calabash Solutions](#), 22; [Privacy 108](#), 40; [ResMed](#), 6.

²¹³¹ GDPR art 4.

²¹³² Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 70.

²¹³³ Submissions to the Issues Paper: [Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia](#), 43; [Dr Kate Mathews Hunt](#), 13.

²¹³⁴ Ibid.

²¹³⁵ Australian Government, [National Data Security Action Plan](#) (discussion paper, April 2022) 20.

²¹³⁶ Ibid.

personal information is not inherently safer or more secure simply because it is stored in Australia.²¹³⁷ 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 8.²¹³⁸ In addition, widespread data localisation requirements can represent significant barriers to trade and economic cost.²¹³⁹ Australia also has commitments in treaties to prohibit data localisation and enable cross border data flows, with certain exceptions.²¹⁴⁰

Discussion Paper proposal – introduce a definition of ‘disclosure’

The Discussion Paper sought feedback on a proposal to introduce a definition of ‘disclosure’ that is consistent with the current definition in the APP Guidelines. 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.²¹⁴¹ 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.²¹⁴² OAIC guidance notes that the publication of personal information online constitutes an overseas disclosure of personal information. Further consideration should be given to whether an exception is required for such disclosures that are in the public interest.

A large number of submitters supported the proposal²¹⁴³ and noted that 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.²¹⁴⁴

23.6 Introduce a definition of ‘disclosure’ that is consistent with the current definition in the APP Guidelines.

Further consideration should be given to whether online publications of personal information should be excluded from the requirements of APP 8 where it is in the public interest.

Discussion Paper proposal – amend APP 8.1 to clarify the meaning of ‘reasonable steps’

The Discussion Paper proposed amending the Act to clarify what circumstances are relevant to determining what are ‘reasonable steps’ for the purpose of APP 8.1 by elevating the factors in the APP Guidelines into the wording of APP 8. This proposal was intended to assist entities in understanding what their obligations are before disclosing personal information overseas.

2137 Submissions to the Issues Paper: [Global Data Alliance](#), 2; [BSA – The Software Alliance](#), 9; [ANZ](#), 15; [Facebook](#), 44.

2138 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.

2139 Australian Government, [National Data Security Action Plan](#) (discussion paper, April 2022) 20.

2140 See for example Australia-Singapore Digital Economy Agreement (Art 24-25), the Comprehensive and Progressive Agreement for a Trans-Pacific Partnership (Art 14.11 and 14.13), the Regional Comprehensive Economic Partnership Agreement (Art 12.14 and 12.15), and the Australia-United Kingdom Free Trade Agreement (Art 14.10 and 14.11), among others.

2141 OAIC, [APP Guidelines](#) (July 2019) [B.67], [B.71].

2142 Ibid [B.67]–[B.68].

2143 Submissions to the Discussion Paper: [Australian Information Industry Association](#), 5; [Department of Health \[Cth\]](#), 17; [Avant Mutual](#), 17; [DIGI](#), 24; [Australian Council on Children and the Media](#), 9; [Australian Institute of Health and Welfare](#), 10; [Australian Medical Association](#), 17; [Workday](#), 7; [elevenM](#), 59; [OAIC](#), 185; [Meta](#), 9; [Salinger Privacy](#), 42; [Australian Communications Consumer Action Network](#), 17; [Australian Financial Markets Association](#), 11.

2144 Submissions to the Discussion Paper: [MIGA](#), 9; [Australian Medical Association](#), 17; [Salinger Privacy](#), 42; [Australian Communications Consumer Action Network](#), 17.

The APP Guidelines indicate that whether ‘reasonable steps’ requires a contract to be entered into, the terms of any contract, and the steps which an entity should take to monitor compliance with any contract (such as auditing), will depend upon the circumstances of the disclosure. These include:

- 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 was put forward in response to submitter concerns that the wording of APP 8 is overly subjective, in particular the phrase, ‘such steps as are reasonable in the circumstances’.²¹⁴⁵ Submissions noted that this language often leads to disputes about what measures entities must put in place to protect personal information.²¹⁴⁶

While a number of submitters supported the proposal,²¹⁴⁷ others suggested the factors should remain in OAIC guidelines.²¹⁴⁸ The OAIC considered that the proposal could result in inconsistency with the other APPs that are also centred around the ‘reasonable steps’ test and that OAIC guidelines can be more easily amended to take account of technological developments in personal information handling practices, and could quickly reflect any judicial interpretation of APP 8.²¹⁴⁹ In response to this feedback, a specific proposal to clarify the meaning of reasonable steps in this context is not recommended. The relevant factors will instead remain in the APP Guidelines.

23.3 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 secure flow of information to and from overseas jurisdictions such as the European Union.²¹⁵⁰

23.3.1 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.²¹⁵¹ 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.²¹⁵² 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 entities located in countries outside the EU that have been deemed adequate.

2145 Submissions to the Issues Paper: [Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia](#), 43; [Minderoo Tech and Policy Lab – University of Western Australia School of Law](#), 20; [Australian Privacy Foundation](#), 27; [ANZ](#), 15.

2146 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.

2147 Submissions to the Discussion Paper: [Calabash Solutions](#), 23; [Department of Health \(Cth\)](#), 17; [Avant Mutual](#), 17; [DIGI](#), 24; [Federal Chamber of Automotive Industries](#), 27; [Australian Council on Children and the Media](#), 9; [Australian Institute of Health and Welfare](#), 10; [Workday](#), 7; [Meta](#), 9; [Privacy 108](#), 40; [Western Union](#), 11.

2148 Submissions to the Discussion Paper: [Australian Information Industry Association](#), 5; [elevenM](#), 59; [OAIC](#), 186; [Australian Banking Association](#), 29; [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 10.

2149 Submission to the Discussion Paper: [OAIC](#), 186.

2150 ACCC, [DPI report](#), 36.

2151 GDPR art 45.

2152 Ibid art 46.

As noted above, the GDPR recognises contracts as a method of ensuring personal information transferred outside the EU is adequately protected.²¹⁵³ As Australia's privacy laws have not been 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.²¹⁵⁴ The Court of Justice of the European Union's decision in *Schrems II* could result in stricter scrutiny of contracts that allow the transfer of information outside the EU in the absence of an adequacy decision. EU data exporters must carefully review whether an adequate level of protection can be delivered to transferred data and may require the data exporter to review the national security and surveillance legislation of the country the data is being transferred to. This could make it more difficult for Australian entities to negotiate contractual provisions with organisations in the EU. 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. Submitters noted that this can result in additional regulatory burden.

23.3.2 Benefits of seeking adequacy

A number of submitters expressed support for Australia seeking an adequacy decision under the GDPR.²¹⁵⁵ Submissions noted that an adequacy decision would benefit Australian businesses by reducing regulatory costs associated with contractual provisions,²¹⁵⁶ and allowing businesses to compete more effectively in international markets.²¹⁵⁷ As well as streamlining interactions with businesses trading in the EU,²¹⁵⁸ 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.²¹⁵⁹ The European Commission has recognised Andorra, Argentina, Canada,²¹⁶⁰ Israel, Japan, New Zealand, Republic of Korea, Switzerland, the UK and Uruguay as providing adequate protection.²¹⁶¹ Submissions noted that an adequacy decision could serve as a certificate of trust in Australia's privacy practices, and would increase the confidence of Australia's trading partners.²¹⁶² In addition, five out of Australia's top 10 two-way trading partners are either a GDPR country or a country with GDPR adequacy.²¹⁶³ As a bloc, the EU is Australia's second largest two-way trading partner of goods and services and fourth largest source of foreign direct investment.²¹⁶⁴ Some submitters suggested that without an adequacy decision, Australia is competitively disadvantaged when participating in global markets, potentially preventing technical innovation from entering Australia.²¹⁶⁵

2153 Ibid.

2154 ALRC Report 108, 1329.

2155 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. Submissions to the Discussion Paper: Workday, 8; Fundraising Institute Australia and Public Fundraising Regulatory Association, 10; ResMed, 6; Western Union, 10; BSA | The Software Alliance, 11; Interactive Games and Entertainment Association, 4; Salesforce, 3; Australian Privacy Foundation, 16; Law Council of Australia, 18; ADMA, 14.

2156 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.

2157 Submissions to the Issues Paper: Fintech Australia, 12–3; Interactive Games and Entertainment Association, 20; Australian Information Security Association, 24.

2158 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.

2159 Submissions to the Issues Paper: 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.

2160 For commercial organisations.

2161 European Commission, *Adequacy decisions* (Web Page, 17 December 2021).

2162 Submissions to the Issues Paper: 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.

2163 Germany is bound by the GDPR, the UK, Japan, New Zealand and the Republic of Korea have adequacy decisions, see Department of Foreign Affairs and Trade, *Trade and investment at a glance 2021* (Web Page, 8 December 2021).

2164 Department of Foreign Affairs and Trade, *Trade and investment at a glance 2021* (Web Page, 8 December 2021).

2165 Submissions to the Issues Paper: Fintech Australia, 12; Interactive Games and Entertainment Association, 19; OAIC, 116.

23.3.3 Challenges in seeking adequacy

Submissions also noted that an adequacy assessment could require major legislative changes and that organisations would bear a regulatory cost in stepping up to GDPR standards.²¹⁶⁶ As noted in the Discussion Paper, 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. While a formal EU adequacy decision would not require Australia's framework to mirror that of the GDPR,²¹⁶⁷ 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, in particular, the small business and employee records exemptions.²¹⁶⁸ 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.²¹⁶⁹

While obtaining an adequacy decision is not the goal of this Review, following implementation of any reforms arising out of this Review, consideration should be given to whether to pursue adequacy.

²¹⁶⁶ Submissions to the Issues Paper: [Queensland University of Technology Faculty of Law](#), 24; [Optus](#), 13; [Facebook](#), 45.

²¹⁶⁷ GDPR art 45(1).

²¹⁶⁸ 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].

²¹⁶⁹ 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).

24. Cross-Border Privacy Rules and domestic certification

The Discussion Paper sought feedback on a proposal to continue progressing implementation of the CBPR system domestically. Submitters were generally supportive of the continued implementation of the CBPR system,²¹⁷⁰ and were of the view that the system could provide a mechanism to facilitate further cross-border data flows and deliver trade benefits across Asia-Pacific Economic Cooperation (APEC) economies.²¹⁷¹

24.1 Cross-Border Privacy Rules

The CBPR system is a voluntary certification scheme, originally developed in APEC, which enables a business' personal information handling practices to be certified as meeting privacy standards in relation to notice, collection, use, choice, integrity and security of personal information, access, correction and accountability (known as CBPR program requirements).²¹⁷² Entities seeking CBPR certification must submit to an audit of their privacy practices and procedures by a 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. CBPR certification is intended to enhance consumer trust that certified businesses will handle data responsibly, and to provide dispute resolution services if an issue arises. Accountability Agents provide privacy dispute resolution services to certified businesses and consumers if a privacy complaint is made against a certified business in that jurisdiction. Unresolved privacy complaints against certified businesses are referred to the privacy regulator in the country in which the business is located. If the CBPR certification system was assessed as providing substantially similar protections to the APPs, it could be prescribed as a binding scheme under APP 8.2(a) which would enable an APP entity to transfer personal information to a certified business overseas with the assurance that it would be adequately protected (see Chapter 23). To date, no assessment has been undertaken.

APEC endorsed Australia's application to participate in the CBPR system in November 2018. The other participating economies in the APEC CBPR were the United States of America, Mexico, Canada, Japan, Republic of Korea, Singapore, Chinese Taipei and the Philippines. At the time of writing, various countries are working toward implementation and the US, Japan and Singapore have fully implemented the system domestically.

24.1.1 Global CBPR Forum

The Global CBPR Forum was established in April 2022 to support the free flow of data and effective data protection and privacy globally.²¹⁷³ The Global CBPR Forum intends to promote expansion and uptake of the CBPR system globally, disseminate best practices for data protection and interoperability and pursue interoperability with other data protection frameworks.²¹⁷⁴ Although the Global CBPR Forum is based on the APEC CBPR systems, the system will be independently administered and separate from APEC. Australia joined the Global CBPR system in August 2022.

24.2 Domestic implementation

The CBPR system could 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. The code would incorporate the CBPR program requirements, while ensuring interoperability with the APPs. Implementation would also require an Australian Accountability Agent.

2170 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. Submissions to the Discussion Paper: [Interactive Games and Entertainment Association](#), 5; [OAIC](#), 187; [Workday](#), 8; [National Australia Bank](#), 6; [Salesforce](#), 3; [Meta](#), 49; [DIGI](#), 25; [BSA | The Software Alliance](#), 11; [Western Union](#), 11; [Global Data Alliance](#), 2; [Australian Banking Association](#), 29.

2171 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. Submissions to the Discussion Paper: [Interactive Games and Entertainment Association](#), 5; [Workday](#), 8; [Western Union](#), 11; [elevenM](#), 60.

2172 APEC, *Cross-Border Privacy Rules System Program Requirements* (Report, November 2019).

2173 Global CBPR Forum, [Welcome to the Global Cross-Border Privacy Rules \(CBPR\) Forum](#) (Web Page, 2022).

2174 Ibid.

24.2.1 Benefits and challenges in implementing the CBPR system

The CBPR system could facilitate cross-border data flows and consequently trade benefits, allowing participants to take advantage of the growing digital economy. Salesforce noted that CBPR implementation would provide another useful tool to support APP entities as they manage international data flows.²¹⁷⁵ Submissions also noted a number of challenges to domestic implementation. These included limited understanding of the CBPR system within industry,²¹⁷⁶ the costs and resources required for businesses to participate,²¹⁷⁷ the limited adoption of the CBPR system internationally (at both the jurisdictional and organisational level)²¹⁷⁸ and the difficulty of encouraging organisations to become Accountability Agents.²¹⁷⁹ A number of submitters also considered there are limited benefits of CBPR implementation for individuals or businesses,²¹⁸⁰ with some suggesting the CBPR system provides a lower standard of protection than the Act and that Australia should not take further steps to implement CBPR.²¹⁸¹

If adopted, a number of proposals in this Report could increase Australia's privacy protections above the CBPR standards. An assessment would need to be made following the outcomes of the Review to determine if the CBPR standards provide a 'substantially similar' level of protection, as required by APP 8. If the protections provided by the CBPR system were not substantially similar to the protections provided by the Act, and so constitute a 'binding scheme' for the purposes of APP 8.2(a), participating in the CBPR system may be less appealing to Australian businesses. This is because a CBPR certified overseas business transferring information to an Australian business would not benefit from the Australian CBPR certified business being able to reciprocate the transfer of information unless the overseas business was able to meet Australia's stronger protections under the Privacy Act. Likewise, CBPR certification of an overseas business would not alleviate the obligation on an Australian business transferring personal information to the CBPR certified business overseas to take reasonable steps to ensure that the business did not breach the APPs as required by APP 8.1.

24.2.2 Next steps

It is possible that the CBPR program requirements may be considered further in light of the CBPR system's expansion beyond the APEC region and the aim of the Global CBPR Forum to pursue interoperability with other data protection frameworks. For these reasons, a decision on progressing domestic implementation of the CBPR system should not be made until the reforms to the Act arising out of this Review have been implemented, at which point, a comparison of the protections offered under the Act and the Global CBPR Forum can be undertaken.

24.3 Domestic certification scheme

The DPI Report recommended that government consider introducing an independent certification mechanism to monitor and demonstrate compliance of particular APP entities collecting, using and disclosing a large volume of personal information.²¹⁸² The Discussion Paper put forward a proposal to introduce a voluntary domestic privacy certification scheme that was based on, and would work alongside the CBPR system.

²¹⁷⁵ Submission to the Issues Paper: [Salesforce](#), 3.

²¹⁷⁶ Submissions to the Issues Paper: [Salesforce](#), 3; [Experian](#), 23; [Privacy 108](#), 15.

²¹⁷⁷ Submissions to the Issues Paper: [Experian](#), 23; [Roche](#), 9; [Australian Information Security Association](#), 24; [Gadens](#), 2. Submissions to the Discussion Paper: [Western Union](#), 11-12; [Australian Data and Insights Association](#), 5; [Australian Institute of Company Directors](#), 3; [Australian Collectors and Debt Buyers Association](#), 10; [ResMed](#), 5-6.

²¹⁷⁸ Submissions to the Issues Paper: [Roche](#), 9; [Privacy 108](#), 15; [Western Union](#), 3; [Australian Financial Markets Association](#), 13; Submissions to the Discussion Paper: [Western Union](#), 11; [ResMed](#), 5-6.

²¹⁷⁹ Submissions to the Issues Paper: [OAIC](#), 117; [Openly Australia](#), 2.

²¹⁸⁰ Submissions to the Discussion Paper: [Australian Data and Insights Association](#), 5; [Australian Institute of Company Directors](#), 3; [Australian Collectors and Debt Buyers Association](#), 10; [ResMed](#), 5; [Privacy 108](#), 41.

²¹⁸¹ Submissions to the Discussion Paper: [Graham Greenleaf](#), 6-7; [Dr Katharine Kemp](#), UNSW Sydney, 19; [Australian Privacy Foundation](#), 17.

²¹⁸² ACCC, [DPI report](#) 480.

24.3.1 Proposed model

Under the proposed model, 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. The Discussion Paper noted that an accredited certification agent for the domestic scheme could 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 and these complaints would instead be made directly to the OAIC.

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 within the DPI inquiry.²¹⁸³ Some submitters expressed support for the proposed scheme²¹⁸⁴ and suggested a domestic certification scheme could provide consumers evidence-based information about the privacy credentials of an entity they were dealing with.²¹⁸⁵

24.3.2 Challenges in implementing a domestic certification scheme

Some submitters suggested there was limited merit in developing a domestic certification scheme²¹⁸⁶ and that the value offered to businesses was not clear when balanced against the costs of certification.²¹⁸⁷ Given the costs associated with establishing a domestic certification scheme, its feasibility depends on the domestic implementation of the CBPR system. This is because a domestic certification scheme would require significant resources to develop. Furthermore, the benefits to entities acting as certification agents would be less tangible if they were not able to also act as Accountability Agents under the CBPR system. Further consultation should be undertaken with industry once a decision is reached on domestic implementation of the CBPR system. This consultation should explore the utility of a domestic certification scheme and whether an alternative model could be introduced in place of the model put forward in the Discussion Paper if the CBPR system is not implemented domestically.

2183 Ibid 480-81.

2184 Submissions to the Discussion Paper: [OAIC](#), 188; [Meta](#), 49; [DIGI](#), 25; [Western Union](#), 11-12; [elevenM](#), 61; [FinTech Australia](#), 15; [AssuranceLab](#), 3.

2185 Submissions to the Discussion Paper: [National Australia Bank](#), 6; [Australian Banking Association](#), 29; [elevenM](#), 61; [FinTech Australia](#), 16; [Avant Mutual](#), 18.

2186 Submissions to the Discussion Paper: [Australian Collectors and Debt Buyers Association](#), 10; [ResMed](#), 5; [Privacy 108](#), 41.

2187 Submissions to the Discussion Paper: [Western Union](#), 11; [Privacy 108](#), 41; [Information Technology Industry Council](#), 3.



Contents | Part 3:

25.	Enforcement	252
26.	A direct right of action	272
27.	A statutory tort for serious invasions of privacy	280
28.	Notifiable data breaches scheme	288
29.	Interactions with other schemes	299
30.	Further review	304

Part 3: Regulation and enforcement

25. Enforcement

Effective enforcement of the Act is essential to protecting the privacy of individuals and the public interest in privacy. 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 has raised questions 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 Discussion paper explored ideas for how the role and enforcement options available to the OAIC could be improved so that the OAIC can operate well in the contemporary environment.

25.1 Current regulatory framework

The OAIC is responsible for complaint handling, compliance, monitoring, education and promotion of privacy laws. If an individual or individuals are concerned that an interference with their privacy has occurred, they may complain to the OAIC. There is no avenue for individuals to seek damages in the courts for breaches of the APPs.

The IC must make a reasonable attempt to conciliate a privacy complaint if it is 'reasonably possible' that it can be conciliated successfully.²¹⁸⁸ The IC may decline to investigate matters for specified reasons, including where satisfied there is no interference with privacy or an investigation is not warranted in the circumstances.²¹⁸⁹ If a complaint is substantiated following investigation, the IC may decide to make a determination that includes remedial actions; such as declaring that an individual is entitled to compensation, or directing an entity to take certain steps.²¹⁹⁰ Complainants or the IC may apply to the Federal Court or the Federal Circuit and Family Court of Australia (FCFCOA) for an order enforcing a determination made by the IC if it is not complied with.²¹⁹¹ A complainant or a respondent may seek AAT review of a decision by the IC to make a determination.²¹⁹²

In the 2021-22 financial year, the OAIC received 2,544 privacy complaints and finalised 2,203 privacy complaints in an average time of six months.²¹⁹³ It also dealt with 10,931 privacy enquiries.²¹⁹⁴ The IC made three determinations following Commissioner-initiated investigations and an additional 14 privacy complaint determinations.²¹⁹⁵ The IC awarded compensation in three cases, ranging from \$2,500 to \$5,000. Since 2014, the IC has had the power to apply to the Federal Court for a civil penalty for 'serious' or 'repeated' interferences with privacy. The IC has commenced one civil penalty proceeding.²¹⁹⁶

25.2 Issues with the current framework

Despite the IC making a record number of determinations in the 2020-21 and 2021-22 financial years, the regulatory framework raises questions as to whether there is adequate deterrence for entities to not breach privacy laws. The compensation amounts awarded by the IC have to date been relatively low. In addition, the number of determinations issued by the IC are fairly infrequent considering the number of privacy complaints lodged each year (there were 17 determinations from 2,203 resolved privacy complaints in the 2021-22 financial year). Further, the civil penalty framework for 'serious' or 'repeated' interferences with privacy presents some challenges as the court has no power to order compensation.

The proposed reforms would increase the range of enforcement mechanisms available to the IC, address gaps in current powers, introduce new powers to undertake public inquiries and give the Federal Court broader powers when making civil penalty orders. Reforms are also proposed to increase transparency in relation to complaint outcomes

²¹⁸⁸ Privacy Act s 40A.

²¹⁸⁹ Ibid s 41.

²¹⁹⁰ Ibid s 52.

²¹⁹¹ Ibid ss 55A, 62. Noting the administrative unification of the Federal Circuit Court of Australia and Family Court of Australia to the FCFCOA on 1 September 2021.

²¹⁹² Ibid s 96.

²¹⁹³ OAIC, [Annual Report 2021-22](#) 11.

²¹⁹⁴ Ibid 12.

²¹⁹⁵ Ibid 21.

²¹⁹⁶ *Australian Information Commissioner v Facebook Inc* [2020] FCA 531, *Australian Information Commissioner v Facebook Inc* (No 2) [2020] FCA 1307.

and make changes to the regulatory model which would enable a greater focus on enforcement, alongside the handling of complaints. To ensure the OAIC is appropriately resourced to carry out its regulatory functions and use the full suite of its enhanced regulatory powers to maximum effect, more work should be undertaken to explore the feasibility of industry funding models.

The proposals in this chapter build on reforms to the Act recently passed in the Privacy Enforcement Act.²¹⁹⁷ These reforms strengthen the OAIC's powers and increased the deterrent effect of breaching privacy laws.

25.3 Civil penalty provisions

25.3.1 A tiered approach to civil penalties and infringement notices

The powers that are currently available to the IC are based on an 'enforcement pyramid' approach to regulation. The Act initially relies upon the IC encouraging compliance, and then determinations (and enforcement in the courts) if that is not successful. For the most egregious interferences with privacy, section 13G of the Act provides for the IC to take civil penalty action against the entity in the Federal Court or FCFCOA.

Section 13G applies if an APP entity does an act or engages in a practice that is a serious interference with the privacy of an individual; or the entity repeatedly does an act, or engages in a practice, that is an interference with the privacy of one or more individuals. The maximum penalty for a breach of section 13G by a body corporate was \$2.22 million prior to amendments passed in the Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (the Privacy Enforcement Act). The Privacy Enforcement Act increased that maximum penalty for a body corporate to an amount not exceeding the greater of \$50 million; three times the value of the benefit obtained; or, if the court cannot determine the value of that benefit, 30 per cent of their adjusted turnover in the relevant period. The purpose of this amendment is to incentivise entities to ensure they comply with their obligations under the Act, and to reflect the very serious privacy harms that can result from breaches of those obligations.

The Discussion Paper proposed that the spectrum of enforcement mechanisms was too limited because it did not appropriately allow for regulatory responses that could target the different levels of seriousness with which interferences with privacy occur. It put forward two additional categories of civil penalty provisions that cover less serious conduct than in section 13G, but that still warrant enforcement action. The first new category would be a new mid-tier civil penalty for any interference with privacy (aside from administrative breaches) with a lesser maximum penalty amount. The second new category would be a series of low-level civil penalty provisions for administrative breaches of the APPs with attached infringement notice powers for the IC.

Mid-tier civil penalty

A large number of submitters supported the proposal to create tiers of civil penalty provisions to give the OAIC more options to better target regulatory responses.²¹⁹⁸ Stakeholders in support highlighted the benefits of more regularly applied penalties, particularly in terms of improving compliance with the Act.²¹⁹⁹ However, stakeholders also commented that the OAIC must be appropriately resourced to use the full suite of its enforcement powers effectively and funding may dictate the effectiveness of these reforms.²²⁰⁰

UNSW submitted that this reform 'has the potential to assist the development of the OAIC into a true enforcement regulator and the consequent acceptance by industry that privacy compliance is not optional'.²²⁰¹ Michael Douglas,

2197 The Privacy Enforcement Act was passed on 28 November 2022 and commenced on 13 December 2022.

2198 Submissions to the Discussion Paper: [Public Health Association of Australia](#), 12; [CHOICE](#), 17; [DIGI](#), 25; [Australian Privacy Foundation](#), 17; [Foundation for Alcohol Research and Education](#), 22; [Information and Privacy Commission NSW](#), 6; [Privacy 108](#), 42; [Graham Greenleaf, UNSW Sydney](#), 7; [Office of the Information Commissioner Queensland](#), 4; [The Australia Institute – Centre for Responsible Technology](#), 11; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 12; [elevenM](#), 61; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 11; [Calabash Solutions](#), 25; [Australian Digital Health Agency](#), 5; [ACCC](#), 6-7; [Obesity Policy Coalition](#), 17; [Australian Council on Children and the Media](#), 10; [Australian Communications Consumer Action Network](#), 17.

2199 Submission to the Discussion Paper: [elevenM](#), 61.

2200 Submission to the Discussion Paper: [Privacy 108](#), 42; [Information and Privacy Commission NSW](#), 6; [The Australia Institute – Centre for Responsible Technology](#), 11; [Law Council of Australia](#), 19.

2201 Submission to the Discussion Paper: [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 11.

Senior Lecturer at University of Western Australia Law School stated that ‘a serious problem with the current Act is that the consequences of non-compliance are far too weak.’²²⁰² The Law Council of Australia noted that ‘in regimes where penalties are significant, such as the GDPR fines in the EU, large businesses routinely include GDPR compliance in their terms with their supply chain...This creates an economy-wide positive impact on business behaviour.’²²⁰³

Several stakeholders held the view that there is no compelling reason to introduce a mid-tier penalty.²²⁰⁴ The Business Council of Australia stated that it is not clear ‘that there is a systemic problem that needs to be addressed through providing the regulator with greater enforcement powers.’²²⁰⁵ Optus submitted that it would be premature to extend the civil penalty regime where only one court application had been made by the IC to enforce civil penalties under the current regime, and that targeted regulatory enforcement of breaches that are serious or repeated would deter conduct which has a serious impact on individuals or which is indicative of systemic failures.²²⁰⁶

Other submitters considered that lower level penalties could have a ‘chilling effect on the wider economy’²²⁰⁷ and would potentially penalise small business operators covered by the Act. MIGA submitted that there is no evidence of any need for more proactive enforcement of privacy standards in the healthcare sector and the ‘broad range of healthcare providers, from solo doctors to large hospitals, should not face the risk of pecuniary penalty for each and every breach of the APPs.’²²⁰⁸ Justice Connect were also concerned that a focus on penalties and enforcement may discourage small to medium not-for-profits from opting in to the Act and called for a focus on prevention through education and support. They noted that if the small business exemption is removed, many businesses will need support to comply with the Act to avoid unintentional breaches.²²⁰⁹

Provision of more guidance, support and resources to assist entities to improve their capabilities in processing personal information was considered preferable by some submitters.²²¹⁰ Telstra submitted that additional OAIC guidance would be needed to delineate between an interference of privacy which is ‘serious’ or ‘repeated’, and one which is not but is still of sufficient severity that a mid-tier civil penalty is appropriate.²²¹¹

The OAIC welcomed reconsidering the civil penalty framework but called for a ‘simpler’ civil penalty regime, rather than a tiered approach. The OAIC submitted that there should be one civil penalty provision for all interferences with privacy (without the ‘serious’ and ‘repeated’ elements). It would then be for the Court to consider the nature and extent of the contravention in determining the penalty.²²¹² The OAIC submitted that this approach would provide the IC with a broader discretion to identify the most appropriate regulatory action within a simpler civil penalty regime, which it would exercise transparently, consistently and proportionately in line with its Regulatory Action Policy and Guide to privacy regulatory action.²²¹³

Proposal – introduce mid-tier civil penalty

The lack of any civil penalty for interferences with privacy that do not have a ‘serious’ and/or ‘repeated’ element is a gap in the regulatory framework. At present, sanction for any breach of the Act that is less than serious or repeated may only occur as a result of a determination by the IC. In those circumstances, the IC is limited to the outcomes in section 52, involving declarations against a respondent to take certain action including paying compensation. The IC cannot seek a civil penalty in the courts against an entity for anything less than a serious or repeated breach. This limits the effectiveness of the IC’s ability to enforce the Act. Against a backdrop of the IC having brought only one application to the Court seeking civil penalties, an additional option is needed in the regulatory framework to protect individuals’ privacy through incentivising improved compliance. It would be a stronger deterrent than a determination because the court would be able to order an entity to pay a pecuniary penalty in addition to other orders, such as compensation and conduct orders. The midtier civil penalty would not apply to low-level administrative breaches that would be subject to a lower penalty and have an infringement notice scheme attached.

2202 Submission to the Discussion Paper: [Michael Douglas UWA Law School](#), 4.

2203 Submission to the Discussion Paper: [Law Council of Australia](#), 19.

2204 Submission to the Discussion Paper: [Optus](#), 29; [Business Council of Australia](#), 9; [MIGA](#), 9.

2205 Submission to the Discussion Paper: [Business Council of Australia](#), 9.

2206 Submission to the Discussion Paper: [Optus](#), 29.

2207 Submission to the Discussion Paper: [Fundraising Institute of Australia and Public Funding Regulatory Association](#), 10.

2208 Submission to the Discussion Paper: [MIGA](#), 9.

2209 Submission to the Discussion Paper: [Justice Connect](#), 6-7.

2210 Ibid.

2211 Submission to the Discussion Paper: [Telstra](#), 26.

2212 Submission to the Discussion Paper: [OAIC](#), 191; referring to s 82(6) of the *Regulatory Powers Act 2014* (Cth).

2213 Ibid.

A mid-tier penalty provision should be introduced, rather than a single civil penalty provision without the ‘serious’ or ‘repeated’ elements. The maximum penalty that attaches to serious contraventions under section 13G would not be appropriate to attach to a minor interference with privacy. However, the penalty would need to be high enough to ensure deterrence. This approach is consistent with the Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers which states that, ‘if a proposed offence is to cover a wide range of conduct that would make it difficult to set a single penalty, consideration should be given to creating more than one offence, each with its own penalty.’²²¹⁴

Further consideration should be given to the appropriate amount to attach to the mid-tier penalty provision. This could be set at a maximum penalty of 2,000 penalty units which was the maximum penalty for section 13G prior to the amendments to the Privacy Enforcement Act which increased the maximum civil penalty for that provision. It would ultimately be a matter for the court to determine the actual penalty for a breach of the Act. Section 80U of the Privacy Act triggers section 82 of the *Regulatory Powers Act 2014* (Cth) (Regulatory Powers Act) which requires the court to take into account the nature and extent of the contravention and circumstances surrounding the contravention when determining a civil penalty.

Low-level civil penalty with infringement notice powers

There was considerable support for this reform as part of a suite of tiered penalties.²²¹⁵ However, it was noted that processes should be put in place to ensure that the infringement notice regime is not overused in circumstances where the mid and high-tier civil penalty provisions are more appropriate to promote the public interest.²²¹⁶

Some stakeholders specifically opposed the introduction of a tier of civil penalty provisions that respond to low level breaches.²²¹⁷ MIGA considered that issuing infringement notices to entities in the healthcare sector would be ‘entirely inappropriate for supposed healthcare privacy breaches given the provision of healthcare, and its interaction with the Privacy Act and other legal, professional and ethical requirements is complex... [and] requires evaluative judgments.’²²¹⁸

Telstra submitted that an infringement notice regime for low-level privacy breaches is unnecessary and referred to their experience that complaints resulting from low level administrative breaches are commonly resolved quickly between the customer and entity, and in circumstances where these matters are escalated to the OAIC, they are usually resolved by conciliation. Telstra submitted that the existing model ‘creates a clear incentive for entities to review and improve their privacy processes as a consequence of received complaints’.²²¹⁹

The OAIC supported the introduction of infringement notice powers but proposed a broader infringement notice regime attached to the new civil penalty for any interference with privacy, ‘commensurate with the infringement notice framework of the ACCC’.²²²⁰

Proposal – Low-level civil penalty with infringement notices powers

It is proposed that an additional new category of civil penalty provisions be introduced to capture administrative breaches of the Act with attached infringement notice powers. Infringement notice provisions supplement civil penalty provisions to provide an alternative to litigation. A person issued with an infringement notice has the option to pay the amount specified in the notice in full²²²¹ and avoid court proceedings. If the person fails to pay the amount specified in the infringement notice, the regulator is able to take enforcement action through the courts in respect of the civil penalty provision.²²²² Being able to issue infringement notices for administrative breaches would benefit both the OAIC and APP entities by avoiding the need for litigation over minor administrative breaches.

The amount of the low-level civil penalty should be set by legislation. The amount payable under an infringement notice is typically 20 per cent or less of the maximum amount of the related civil penalty provision. The penalty attached to an infringement notice should also be set in the legislation.

²²¹⁴ Attorney-General’s Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (September 2011) 38. This Guide considers framing criminal offences however this point is relevant to the framing of civil penalty provisions.

²²¹⁵ Submissions to the Discussion Paper: [Public Health Association of Australia](#), 12; [CHOICE](#), 17; [DIGI](#), 25; [Australian Privacy Foundation](#), 17; [Foundation for Alcohol Research and Education](#), 22; [Information and Privacy Commission NSW](#), 6; [Privacy 108](#), 42; [Graham Greenleaf, UNSW Sydney](#), 7; [Office of the Information Commissioner Queensland](#), 4; [The Australia Institute – Centre for Responsible Technology](#), 11; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 12; [elevenM](#), 61; [Calabash Solutions](#), 25; [Australian Digital Health Agency](#), 5; [ACCC](#), 6-7.

²²¹⁶ Submission to the Discussion Paper: [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 11.

²²¹⁷ Submission to the Discussion Paper: [NSW Council for Civil Liberties](#), 36.

²²¹⁸ Submission to the Discussion Paper: [MIGA](#), 9.

²²¹⁹ Submission to the Discussion Paper: [Telstra](#), 26.

²²²⁰ Submission to the Discussion Paper: [OAIC](#), 193-194.

²²²¹ Attorney-General’s Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (September 2011) 57.

²²²² Ibid 57-58; ALRC, *Principled Regulation: Federal Civil and Administrative Penalties in Australia* (Report 95, December 2002) 427, 431.

Infringement notices are typically used for administrative failing by entities which do not require an evaluative judgment on the part of the enforcer.²²²³ Accordingly, it would not be appropriate, at this stage, to extend the infringement notice scheme to the proposed mid-tier civil penalty for any interference with privacy. This is because many breaches of the Act require analysis of the precise content of the relevant obligation in the circumstances of the relevant case, and the nature and extent of any contravention.

However, some administrative breaches of the Act would be suitable for a low-level penalty and infringement notice. As a result of recent amendments to the Privacy Act, the IC is able to issue an infringement notice when an APP entity fails to give information to the IC when required to do so under the Act (section 66), which the entity could elect to pay, instead of the matter being heard by a court.

Examples of other administrative breaches suitable for a low-level penalty and infringement notice regime could include:

- a) APP 1.3 The requirement to have a clearly expressed and up to date privacy policy
- b) APP 2.1 The requirement to give individuals the option of not identifying themselves
- c) APP 6.5 The requirement to make a written note of use or disclosure under APP 6.2 (e), and
- d) APP 13.5 The requirement to deal with requests to correct information in specified timeframes

25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses:

- **Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision.**
- **Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties.**

'Serious' or 'repeated' interferences with privacy

There has been no judicial consideration of section 13G to date. While OAIC guidance sets out factors which the OAIC considers relevant when considering whether a breach of the Act is 'serious' or 'repeated'²²²⁴, the Discussion Paper proposed that there could be benefit in clarifying some aspects of the threshold to more clearly express that breaches affecting a large number of individuals without affecting any one individual seriously are covered.

It proposed clarifying that section 13G could capture breaches involving:

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

2223 ALRC, *Principled Regulation: Federal Civil and Administrative Penalties in Australia* (Report 95, December 2002) 431; Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (September 2011) 58.

2224 Relevant factors include:

- the number of individuals potentially affected
- whether it involved 'sensitive information' or other information of a sensitive nature
- whether significant adverse consequences were caused or are likely to be caused to one or more individuals from the interference
- whether vulnerable or disadvantaged people may have been or may be particularly adversely affected or targeted
- whether it involved deliberate or reckless conduct
- whether senior or experienced personnel were responsible for the conduct.

Feedback largely supported defining section 13G further²²²⁵ to give the regulator more confidence to enforce it, and APP entities and the public more clarity on which breaches may trigger the highest maximum penalty. Avant Mutual considered that the threshold could be more clearly expressed in terms of the number of individuals to which it applies.²²²⁶ elevenM submitted that clarification would assist entities in identifying which of their activities may lead to serious or repeated interferences with privacy, and encourage additional resource allocation and focus to minimise such interferences.²²²⁷ It noted that this proposal should clarify whether an APP entity 'repeatedly does an act, or engages in a practice' when the same non-compliant process is applied multiple times or across a number of individuals.²²²⁸

Meta supported clarifying what sort of breach is captured by section 13G, but disagreed that breaches affecting a large number of individuals without affecting any one individual seriously would be covered by this civil penalty provision. Meta submitted that the number of individuals affected by a privacy breach should be a factor in determining whether there has been a 'serious' or 'repeated' interference with privacy, however should not be determinative of a breach in isolation.²²²⁹

Privacy 108 supported clarification of 'serious' and 'repeated' and also suggested that consideration be given to linking serious interferences to breaches of cyber-security regulations; failure to comply with any accepted Code of Practice; failure to carry out a PIA or implement remediations identified in a PIA; and high-risk processing of the type identified as requiring a PIA.²²³⁰

A minority of submitters considered that these factors were best defined in OAIC guidance.²²³¹ Optus submitted that this clarification would be best achieved by more detailed regulatory guidance and noted that 'the OAIC should continue to flexibly update and review such guidance, including so that it is readily responsive to emerging technologies and normative complexities surrounding privacy'.²²³² Telstra submitted that additional clarification to the OAIC's current guidance was needed, it is best placed in OAIC guidance.²²³³

The OAIC recommended replacing section 13G with a single civil penalty provision as it 'imposes legal concepts of seriousness and repeated conduct that distract from the proper focus on whether the Privacy Act itself has been breached'. It considered that 'these concepts are more appropriately addressed after a breach has been established when determining pecuniary penalties'.²²³⁴ However, the OAIC submitted that if section 13G was not replaced, clarification of a 'serious' breach should be provided and the 'repeated' element should be removed to avoid unnecessary arguments about whether actions of an APP entity over time amount to serious or repeated interferences with privacy.²²³⁵ Through specifying factors in the legislation it would be clear that section 13G would also cover breaches affecting a large number of individuals without affecting any one individual seriously and take into account the extent to which the entity responsible for the incident or conduct has been the subject of prior privacy regulatory action by the OAIC, and the outcome of that action.²²³⁶

The Senate Legal and Constitution Affairs Legislation Committee which inquired into the Privacy Enforcement Act also recommended that section 13G of the Act be amended to define the terms 'serious interference' and 'repeated' interference.²²³⁷

2225 Submissions to the Discussion Paper: [Australian Digital Health Agency](#), 5; [Avant Mutual](#), 19; [Public Health Association of Australia](#), 12; [CHOICE](#), 17; [DIGI](#), 25; [elevenM](#), 62; [Australian Privacy Foundation](#), 17; [Foundation for Alcohol Research and Education](#), 22; [Law Council of Australia](#), 19; [Australian Council on Children and the Media](#), 10; [Privacy 108](#), 42; [Graham Greenleaf](#), UNSW Sydney, 7; [Uniting Church in Australia](#), [Synod of Victoria and Tasmania](#), 12; [Calabash Solutions](#), 25; [Obesity Policy Coalition](#), 17; [Meta](#), 50; [Information and Privacy Commission NSW](#), 6; [Social Services Portfolio](#), 5; [Australian Communications Consumer Action Network](#), 17.

2226 Submission to the Discussion Paper: [Avant Mutual](#), 19.

2227 Submission to the Discussion Paper: [elevenM](#), 62.

2228 Ibid.

2229 Submission to the Discussion Paper: [Meta](#), 50.

2230 Submission to the Discussion Paper: [Privacy 108](#), 42.

2231 Submissions to the Discussion Paper: [Optus](#), 30; [Telstra](#), 27.

2232 Submission to the Discussion Paper: [Optus](#), 30.

2233 Submission to the Discussion Paper: [Telstra](#), 27.

2234 Submission to the Discussion Paper: [OAIC](#), 194.

2235 Ibid 195.

2236 Ibid.

2237 Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 [Provisions]* [2022] vii.

Submissions to the Committee highlighted that the words ‘serious’ and ‘repeated’ are not defined or supported by a non-exhaustive list of factors that would give rise to such a contravention.²²³⁸ It was submitted that, in view of the substantial penalties to be imposed under section 13G, what constitutes a serious and repeated interference should be better defined.²²³⁹

Proposal – provide clarity on what constitutes a ‘serious’ breach of privacy

Section 13G should be amended to clarify aspects of the threshold. This could be achieved in two ways. First, section 13G could simply be labelled as a serious interference with privacy, on the basis that if an entity repeatedly interferes with the privacy of one or more individuals, then that is serious and it is not necessary to include ‘repeated’ as an alternative in the legislation. Second, what amounts to a ‘serious’ interference should be clarified. It should be clear that the section applies to interferences with privacy of a large number of individuals without affecting any one individual seriously. This reform would provide greater certainty for the OAIC, APP entities and the courts.

25.2 Amend section 13G of the Act to remove the word ‘repeated’ and clarify that a ‘serious’ interference with privacy may include:

- (a) those involving ‘sensitive information’ or other information of a sensitive nature**
- (b) those adversely affecting large groups of individuals**
- (c) those impacting people experiencing vulnerability**
- (d) repeated breaches**
- (e) wilful misconduct, and**
- (f) serious failures to take proper steps to protect personal data.**

The OAIC should provide specific further guidance on the factors that they take into account when determining whether to take action under section 13G.

Submissions to the Committee also raised concerns about what factors a court should take into account when determining a pecuniary penalty. The BCA proposed that greater clarity could be provided by amending section 80U of the Act, which refers to Part 4 of the Regulatory Powers Act. Part 4 stipulates the factors to be taken into consideration when a court determines pecuniary penalties.²²⁴⁰ The BCA argued that the following factors should be included: whether a breach was the result of deliberate, reckless, or negligent behaviour on the part of the regulated entity; whether a regulated entity was compliant with recognised or prevailing standards for security and had robust privacy frameworks in place; whether an entity acted promptly to investigate the matter, sought appropriate expert assistance, and worked in good faith to address harms to citizens; and whether an entity disclosed the breach at an appropriate time to mitigate damage to all involved.²²⁴¹

Section 82(6) of the Regulatory Powers Act sets out factors that a court must take into account when determining a pecuniary penalty. These include the (i) nature and extent of the contravention and (ii) any loss or damage suffered because of the contravention, (iii) circumstances surrounding the contravention and (iv) previous Court decisions on similar conduct. Given that the court must consider a broad range of factors that include the circumstances surrounding the contravention under the Regulatory Powers Act, which applies across various pieces of legislation, it is unnecessary to include further factors in the Privacy Act or the Regulatory Powers Act that the Court should consider when determining the amount of civil penalty.

²²³⁸ [Submission](#) to the Senate Legal and Constitutional Affairs Legislation Committee: Law Council, 17.

²²³⁹ [Submission](#) to the Senate Legal and Constitutional Affairs Legislation Committee: DIGI, 3.

²²⁴⁰ *Regulatory Powers Act 2014* (Cth) s 82.

²²⁴¹ [Submission](#) to the Senate Legal and Constitutional Affairs Legislation Committee: Business Council of Australia, 7-8.

25.4 OAIC powers: assessments, investigations and inquiries

The Discussion Paper proposed reforms to support a more proactive regulatory model by providing the IC with increased powers to gain meaningful evidence of breaches of privacy laws and new mechanisms to enable the examination of systemic issues.

25.4.1. Assessments

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. The Privacy Enforcement Act amended the Privacy Act to introduce a new information-gathering power for the IC for the purpose 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.

25.4.2 Investigations

When conducting investigations, the IC's current powers include:

- to make such inquiries as she thinks fit, including by holding a hearing²²⁴²
- to be given information and documents by issuing a written notice on the entity²²⁴³
- to examine witnesses on oath or affirmation²²⁴⁴
- to direct a person to attend compulsory conference²²⁴⁵
- to conduct a compulsory conference as she thinks fit²²⁴⁶
- to refer matters to other authorities, and²²⁴⁷
- to enter premises and inspect relevant documents by consent or with a warrant.²²⁴⁸

The Discussion Paper proposed that the IC's ability to gather information in the course of investigating civil penalty provisions could be enhanced by applying the investigation powers listed in Part 3 of the Regulatory Powers Act to such investigations.²²⁴⁹ This would confer powers on an authorised person to exercise general investigation powers including to:

- search premises for evidential material²²⁵⁰
- make copies of information and documents specified in a warrant²²⁵¹
- operate electronic materials to determine whether the kinds of information and documents specified in a warrant are accessible,²²⁵² and
- seize evidential material and other things [which would prevent the destruction of evidence].²²⁵³

The majority of submissions supported this proposal.²²⁵⁴ elevenM noted that these additional powers would assist the OAIC in accessing relevant information for an investigation when required, and result in more thorough and well-informed investigations²²⁵⁵.

A small minority opposed this amendment.²²⁵⁶ The BCA considered there was no evidence that the OAIC's investigations have been hindered by a lack of cooperation by entities and suggested instead that the OAIC increase its engagement with business and the community to ensure that expectations under the Act are well understood.²²⁵⁷ Telstra also queried whether the OAIC's investigations have been obstructed by entities to such a degree that additional powers are required

2242 Privacy Act s 43.

2243 Ibid s 44.

2244 Ibid s 45.

2245 Ibid s 46.

2246 Ibid s 47.

2247 Ibid s 50.

2248 Ibid s 68. Note s 2B of the *Acts Interpretation Act 1901* (Cth) 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.

2249 *Regulatory Powers (Standard Provisions) Act 2014* (Cth) (Regulatory Powers Act).

2250 Ibid ss 49(a) and 49(b).

2251 Ibid s 49(d).

2252 Ibid s 50.

2253 Ibid sub-ss 49(b)(iii) and s 52.

2254 Submissions to the Discussion Paper: CHOICE, 17; DIGI, 26; elevenM, 62; Australian Privacy Foundation, 17; NSW Council for Civil Liberties, 36; Australian Council on Children and the Media, 10; Privacy 108, 43; Graham Greenleaf, UNSW Sydney, 7; Uniting Church in Australia, Synod of Victoria and Tasmania, 12; Calabash Solutions, 25; Governance Institute of Australia, 7; Australian Communications Consumer Action Network, 17.

2255 Submission to the Discussion Paper: elevenM, 63.

2256 Submissions to the Discussion Paper: Business Council of Australia, 9; Optus, 30; Telstra, 26.

2257 Submission to the Discussion Paper: Business Council of Australia, 9.

and noted these powers were highly intrusive and likely to interfere with an entity's ability to carry on its business.

Telstra recommended that these powers be limited to investigations involving suspected serious interferences with privacy; and there are reasonable grounds to believe that the relevant entity is not co-operating with the OAIC in its investigation of the entity or that information relevant to the investigation will be destroyed. It also noted concern that the proposed powers do not afford sufficient protection to any confidential information which may be obtained by the OAIC in the exercise of these powers. Any confidential information obtained as part of the OAIC's exercise of such expanded investigation powers should only be used for the purpose of the investigation.²²⁵⁸

The OAIC supported this proposal on the basis that 'having the right information gathering tools is essential to effectively develop a case in a way that meets evidentiary requirements and ensures successful regulatory outcomes. It noted that this proposal would bring its powers into line with comparable regulators.'²²⁵⁹

The OAIC also proposed making assessments under the Act subject to monitoring under Part 2 of the Regulatory Powers Act in addition to the IC's current assessment powers.²²⁶⁰ Powers under Part 2 of the Regulatory Powers Act would allow the OAIC to search and seize material where appropriate as part of an assessment. However, it is important that there remains a clear distinction between assessments and investigations. Coercive powers are justified for investigations where there is reason to believe that an infringement with privacy has occurred. In the case of assessments, specific coercive powers must be carefully considered. New information gathering powers for assessments introduced by the Privacy Enforcement Act will assist the IC if there are instances of non-compliance by entities in relation to assessments.

Proposal – enhance investigation powers

Having the right information gathering powers is essential to develop a case that ensures successful regulatory outcomes. The IC's current power to enter premises is inadequate and inconsistent with comparable domestic and international regulators.²²⁶¹ The Act should be amended to trigger Part 3 of the Regulatory Powers Act in investigations of civil penalty provisions under the Act.

25.3 Amend the Act to apply the powers in Part 3 of the *Regulatory Powers (Standard Provisions) Act 2014* to investigations of civil penalty provisions in addition to the Information Commissioner's current investigation powers.

25.5 Inquiries

The OAIC has limited means by which to investigate systemic industry-wide acts and practices. The Discussion Paper proposed that the Act could be amended to enable the OAIC to conduct public inquiries and reviews into specified matters as directed by or subject to Ministerial approval. It would be modelled on the inquiry powers of the ACCC²²⁶² and the inquiry and review functions of the AHRC.²²⁶³ It would enable the taking of evidence and requiring production of documents but would not extend to a hearing power.

²²⁵⁸ Submission to the Discussion Paper: [Telstra](#), 26.

²²⁵⁹ Submission to the Discussion Paper: [OAIC](#), 196.

²²⁶⁰ *Ibid* 197.

²²⁶¹ Such as the ACCC in Australia and the UK ICO in the UK.

²²⁶² *Competition and Consumer Act 2010*, s 95H.

²²⁶³ Section 14 of the *Australian Human Rights Commission Act 1986* allows the Australian Human Rights 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).

The majority of submissions supported this proposal.²²⁶⁴ CPA Australia supported enhancements to the OAIC's powers and suggested that the OAIC have the authority to initiate its own public inquiries and publish the results of such work.²²⁶⁵ The Law Council welcomed expanding the powers of the OAIC to undertake public inquiries and reviews into specified matters provided it was coupled with an education role to inform APP entities of their obligations with more nuance or detail.²²⁶⁶ The NSW Council for Civil Liberties supported the proposal and noted the importance that such a 'power be unfettered and be self-referrable'.²²⁶⁷ It heralded the ACCC's Digital Platforms Inquiry which 'resulted in acceptance by the Commonwealth government that there was a need to promote competition, enhance consumer protection and support a sustainable Australian media landscape in the digital age' and the subsequent actions taken by government including this Review.²²⁶⁸

A minority of stakeholders opposed the reform.²²⁶⁹ Fundraising Institute of Australia did not support this proposal and noted the powers of the OAIC were increased in 2012 and remain adequate.²²⁷⁰

Optus noted the value of such additional powers in an increasingly data driven and digital economy to assist the IC to better understand broader issues and target its regulatory and educational efforts. However, it submitted that consideration should be given to the overlap between regulators in the exercise of these powers in consumer law, competition law and privacy law and recommended a clear demarcation of regulatory responsibility for privacy such as a memorandum of understanding as to cooperation between agencies.²²⁷¹

The ACCC noted that its powers to conduct price inquiries under Part VIIA of the CCA and selfinitiated market studies under paragraph 28(1)(c) of the CCA have limitations: price inquiries require a direction from the Treasurer prior to commencement and self-initiated market studies do not provide the ACCC with compulsory information-gathering powers. The ACCC submitted that the OAIC should have the ability to self-initiate inquiries and compel information from relevant parties for such inquiries.²²⁷²

The OAIC supported a new inquiry power as directed by or subject to Ministerial approval and noted that recent public inquiries by comparable regulators have demonstrated the importance of such processes for effective intelligence gathering that can lead to regulatory action or policy changes. The OAIC considered that such a power would enhance the IC's ability to take a more strategic, targeted approach to privacy regulation.²²⁷³

25.5.1 Proposal – introduce inquiry power

A power to undertake inquiries subject to the safeguard of Ministerial approval or direction should be introduced. Inquiries are valuable mechanisms for examining systemic issues and bringing about change in specific industry sectors where required. The power would involve the ability to take evidence and require the production of documents but would not extend to a hearing power.

25.4 Amend the Act to provide the Information Commissioner with the power to undertake public inquiries and reviews into specified matters on the approval or direction of the Attorney-General.

²²⁶⁴ Submissions to the Discussion Paper: [CHOICE](#), 17; [DIGI](#), 26; [elevenM](#), 62-63; [Australian Privacy Foundation](#), 17; [Obesity Policy Coalition](#), 17; [Law Council of Australia](#), 19; [Foundation for Alcohol Research and Education](#), 22; [NSW Council for Civil Liberties](#), 37; [Australian Council on Children and the Media](#), 10; [Privacy 108](#), 43; [Graham Greenleaf, UNSW Sydney](#), 7; [Uniting Church in Australia, Synod of Victoria and Tasmania](#), 12; [Calabash Solutions](#), 25; [Australian Communications Consumer Action Network](#), 17; [Public Health Association of Australia](#), 12; [CPA Australia](#), 5.

²²⁶⁵ Submission to the Discussion Paper: [CPA Australia](#), 5.

²²⁶⁶ Submission to the Discussion Paper: [Law Council of Australia](#), 19.

²²⁶⁷ Submission to the Discussion Paper: [NSW Council for Civil Liberties](#), 37.

²²⁶⁸ Ibid.

²²⁶⁹ Submission to the Discussion Paper: [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 10.

²²⁷⁰ Ibid.

²²⁷¹ Submission to the Discussion Paper: [Optus](#), 30-31.

²²⁷² Submission to the Discussion Paper: [ACCC](#), 7.

²²⁷³ Submission to the Discussion Paper: [OAIC](#), 197.

25.6 Determinations

The Discussion Paper proposed amending the Act to give the IC power to make a determination requiring an entity to take action to identify and mitigate reasonably foreseeable risks or losses to individuals that may result from an interference with privacy.

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 a data breach has been used for identity theft or fraud for a certain time period after the incident. This amendment would be consistent with the protective intent of existing subparagraph 52(1)(b)(iii) and paragraph 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.

The Discussion Paper noted that 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. The Discussion Paper sought feedback on what would or would not be reasonable action to take.

The majority of submissions supported amending the Act to permit the IC to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss.²²⁷⁴ elevenM considered this to be an important reform in the context of privacy harms which 'commonly arise as small or potential impacts spread across groups of individuals' where harms do not materialise immediately, and that 'lost or stolen personal information may remain available online or on the dark web indefinitely and may be aggregated with other data over time before it is exploited against the affected individual'.²²⁷⁵ elevenM further noted a clear community expectation that entities that interfere with privacy should bear all consequent cost and should protect those affected. It is only by internalising these costs that entities will be correctly incentivised to invest in preventing them.²²⁷⁶

The NSW Council for Civil Liberties supported the proposal but considered it important that 'reasonably foreseeable loss or damage' is clearly defined and referred to the definition that is similar to that in negligence—that is, 'whether the loss or damage is reasonably foreseeable by a reasonable person in the APP entity's position and the loss is not far-fetched or fanciful'.²²⁷⁷ Calabash also supported the proposal, subject to clear guidance from the OAIC on the types of reasonable steps that an entity can take, to prevent future loss or damage from occurring.²²⁷⁸

A minority of submitters opposed this reform.²²⁷⁹ The Fundraising Institute of Australia called for greater emphasis on properly funded dispute resolution.²²⁸⁰ The Federal Chamber of Automotive Industries submitted that the reform proposal was too broad and 'could lead to a requirement to conduct a redress program that was disproportionate in scope and cost to the harm sought to be addressed.' It noted that this uncertainty would be reduced if the OAIC included a list of factors to be considered before exercising such a power.²²⁸¹

Optus was critical of the proposal and considered that there was a significant risk that 'APP entities will be saddled with obligations which are unclear and unduly burdensome'.²²⁸² It noted that the 'reasonably foreseeable' test was complex and that there was no compelling reason to justify its use in this context. It was concerned that future loss or damage with very low probability, or which may not eventuate for a long period (i.e. more than 20 years into the future) could still be considered reasonably foreseeable. Optus considered that the change was unnecessary where the IC can already make declarations that the entity take specified steps within a specified period to ensure that such conduct is not repeated or continued,²²⁸³ and APP 11 requires APP entities to take 'reasonable steps' to protect personal information held by the entity from misuse, interference, loss or unauthorised access, modification or disclosure.²²⁸⁴

2274 Submissions to the Discussion Paper: DIGI, 26; elevenM, 63; Australian Privacy Foundation, 17; Obesity Policy Coalition, 17; NSW Council for Civil Liberties, 37; Australian Council on Children and the Media, 10; Privacy 108, 43; Graham Greenleaf, UNSW Sydney, 7; Public Health Association of Australia, 12; Centre for AI and Digital Ethics, 8;

2275 Submission to the Discussion Paper: elevenM, 63.

2276 Ibid.

2277 Submission to the Discussion Paper: NSW Council for Civil Liberties, 37.

2278 Submission to the Discussion Paper: Calabash Solutions, 25.

2279 Submissions to the Discussion Paper: Fundraising Institute Australia and Public Fundraising Regulatory Association, 10-11; Optus, 31, Telstra, 27, Australian Medical Association, 17-18.

2280 Submission to the Discussion Paper: Fundraising Institute Australia and Public Fundraising Regulatory Association, 10-11.

2281 Submission to the Discussion Paper: Federal Chamber of Automotive Industries, 28.

2282 Submission to the Discussion Paper: Optus, 31.

2283 Privacy Act s 52(1)(b)(ia).

2284 Submission to the Discussion Paper: Optus, 31.

Optus called for further consultation on the particular types of mitigation and redress that the IC could order and submitted that the IC may, in some cases, require specialist skillsets or input in order to properly assess what would be reasonable in particular circumstances, given the evolving nature of data handling practices and standards.²²⁸⁵

Telstra opposed this reform as unnecessary as 'it is already in the interests of entities to take remedial action to mitigate likely loss or damages which could be suffered by individuals who have been impacted by an interference with their privacy'. It submitted that any requirement should be principle-based to ensure adequate flexibility as 'entities are better placed to determine what technical and organisational measures are most appropriate, having regard for the personal information that they hold and how they process it'. It considered that the IC should not be able to require certain software be installed or specify an end-to-end process for an entity to implement'.²²⁸⁶

The AMA accepted that medical practices that experience data breaches should take reasonable steps to prevent future loss, however noted that this proposal was not confined to NDB breaches 'likely to result in serious harm'. It also noted that paragraph 52(1A)(c) already empowers the IC to make a declaration relating to the entity taking a reasonable course of action to redress any actual loss or damage suffered by an individual. It was concerned that the proposed reform would put the onus on the organisation (which may be a sole practitioner) to identify any loss or damage that could be suffered and was concerned that a doctor may not know what specifically to do to satisfy a direction made in general terms. It proposed the following wording: A declaration that the respondent must take specified steps (which must be reasonable) within a specified period to mitigate any serious harm that those individuals are likely to suffer in the future.²²⁸⁷

The OAIC supported this reform as an appropriate response for certain types of matters where there may be a reasonable and widely understood risk of loss occurring, particularly after a data breach.²²⁸⁸

25.6.1 Proposal – proactive requirement to mitigate damage

While the IC can make declarations requiring a respondent to redress loss or damage suffered by a complainant, there is currently no express provision in the Act to allow the IC to require a respondent to take reasonable steps to mitigate future loss. This amendment would be consistent with the protective intent of subparagraph 52(1)(ia)(iii) and paragraph 52(1A)(c) but would require the respondent to be more proactive following a breach in identifying reasonably foreseeable consequences of a breach and taking reasonable steps to mitigate these.

Given the concerns about what steps an entity may need to take, OAIC guidance would be required in relation to what is a reasonable act or course of conduct to identify, mitigate and redress actual or reasonably foreseeable loss. Such guidance could include examples such as monitoring whether information the subject of an eligible data breach has been published for sale on the dark web, paying for a credit monitoring service that alerts affected individuals if there are changes to their credit report, assisting individuals to replace compromised credentials such as drivers licences and passports, and engaging service providers such as identity theft and cyber support providers to provide post-incident support to individuals.

This proposal would complement Proposal 28.3 regarding the NDB scheme, which would amend the reporting requirements so 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.

²²⁸⁵ Ibid.

²²⁸⁶ Submission to the Discussion Paper: [Telstra](#), 27.

²²⁸⁷ Submission to the Discussion Paper: [Australian Medical Association](#), 17-18.

²²⁸⁸ Submission to the Discussion Paper: [OAIC](#), 198.

25.5 Amend subparagraph 52(1)(b)(ii) and paragraph 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.

The OAIC should publish guidance on how entities could achieve this.

25.7 Federal Court orders in civil penalty proceedings

Where the IC has been successful in a civil penalty proceeding under section 13G of the Act, the Federal Court has power to order the respondent to pay a pecuniary penalty.²²⁸⁹ While the Act contains some provisions that allow compensation for loss or damage where a civil penalty order has been made in relation to a provision of Part IIIA, this does not extend to awarding compensation following a civil penalty proceeding under s 13G.

Under section 52, the IC may make determinations which include declarations that a person must take certain actions and pay amounts by way of compensation. If a respondent refuses to comply with a determination, the IC or complainant may apply to the Federal Court to enforce it 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.²²⁹⁰ This means that a determination must be made for compensation to be awarded.

Therefore, even if the Court determines 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, which is then enforced, the Court cannot order that a complainant be compensated, nor that a respondent take action to redress the complainant's loss or damage or ensure the conduct is not repeated or continued.

The Discussion Paper proposed that the Federal Court be given the power to make any order it sees fit after a section 13G civil penalty provision has been established. The majority of submissions supported this reform.²²⁹¹ Eleven M submitted that 'allowing the Courts to make orders it sees fit would recognise that the impact of a breach of privacy cannot always be resolved through financial means, and would provide the court with flexibility to make appropriate orders to deal with all aspects of a matter, including to minimise further impacts to the complainant and/or other individuals, where compensation alone may not.'²²⁹²

Meta supported this proposal but called for it to be made clear that where a court makes an order under section 13G, the IC should not be allowed to separately issue a determination on the same matter under section 52, to avoid risk of overlapping or inconsistent orders.²²⁹³

A minority opposed the reform.²²⁹⁴ The Australian Collectors and Debt Buyers Association submitted that the better option would be to only enable the Federal Court to make compensation orders in addition to an order imposing a pecuniary penalty.²²⁹⁵ The Federal Chamber of Automotive Industries submitted that this reform goes further than is needed to address the current inefficiency in the Act which prevents the court from making the type of conduct and compensation orders able to be made by the IC.²²⁹⁶

²²⁸⁹ Privacy Act s 80U provides that each civil penalty provision is enforceable under Part 4 of the Regulatory Powers Act 2014. Section 82 of the *Regulatory Powers Act 2014* enables the Court to make an order for a person to pay a pecuniary penalty.

²²⁹⁰ Privacy Act s 55A(2).

²²⁹¹ Submissions to the Discussion Paper: [Public Health Association of Australia](#), 12; [Obesity Policy Coalition](#), 17; [elevenM](#), 64; [Australian Privacy Foundation](#), 17; [NSW Council for Civil Liberties](#), 17; [Meta](#), 51; [Privacy 108](#), 44; [Graham Greenleaf, UNSW Sydney](#), 7; [Australian Communications Consumer Action Network](#), 17.

²²⁹² Submission to the Discussion Paper: [elevenM](#), 64.

²²⁹³ Submission to the Discussion Paper: [Meta](#), 51.

²²⁹⁴ Submissions to the Discussion Paper: [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 11; [Australian Collectors and Debt Buyers Association](#), 11; [Federal Chamber of Automotive Industries](#), 29.

²²⁹⁵ Submission to the Discussion Paper: [Australian Collectors and Debt Buyers Association](#), 11.

²²⁹⁶ Submission to the Discussion Paper: [Federal Chamber of Automotive Industries](#), 29.

25.7.1 Proposal – Court to have power to make any order it sees fit

The court should have power to impose any order it sees fit in civil penalty proceedings. This reform would give the court discretion to make orders appropriate to the circumstances of a case. In light of the proposal to introduce different tiers of civil penalty provisions (Proposal 25.1), this reform should apply to all civil penalty provisions and not just serious interferences with privacy under section 13G.

25.6 Give the Federal Court and the Federal Circuit and Family Court of Australia the power to make any order it sees fit after a civil penalty provision relating to an interference with privacy has been established.

25.8 Funding model

In the 2021-22 financial year, the total departmental resourcing available to the OAIC was approximately \$28 million. In light of submissions which emphasised the need for an adequately resourced regulator, the Discussion Paper tested support for introducing an industry funding model similar to that used by ASIC, which could include a cost recovery levy and fees and/or a statutory levy to help fund the OAIC's regulatory activities.

Industry funding for the UK Information Commissioner's Office was introduced in 2018 via a data protection fee which accounts for around 85 to 90 per cent of its annual budget.²²⁹⁷ The UK data protection fee applies to all data controllers and ranges from £35 up to £2,900 for the largest entities.

Most submitters who responded to this proposal opposed the OAIC recovering some of its costs from APP entities and instead considered the OAIC should be funded entirely by government.²²⁹⁸ Generally, the rationale for this view was that APP entities currently have high regulatory costs and, because privacy harms affect the individual, the cost of regulating those harms should be taxpayer funded. However, other submitters who commented on various other proposals noted that their effectiveness would depend on the OAIC being adequately resourced to utilise any new powers.²²⁹⁹

Approximately 90 per cent of ASIC's regulatory activities are now recovered through industry funding arrangements, with the remaining 10 per cent recovered via fees for service.²³⁰⁰ ASIC's industry funding model (which took effect on 1 July 2017) was a substantial undertaking with a high level of robust engagement from industry sectors throughout the Government's consultation process.

The OAIC indicated support for consideration of an industry funding model with appropriate supplementary budget appropriations for functions and activities not funded by a levy. It noted that it should be appropriately designed to preserve the OAIC's independence.

The benefit of industry funding is that it would help address funding constraints that limit the OAIC's enforcement activity. However, it would require a significant investment of time and resources to design, implement and administer. Where most small businesses are exempt from the Act, careful consideration would need to be given to whether industry funding would raise sufficient revenue to justify costs associated with its implementation and ongoing administration.

²²⁹⁷ UK Information Commissioner's Office, [How we are funded](#) (Web Page, 2022).

²²⁹⁸ Submissions to the Discussion Paper: [DIGI](#), 26-27; [Privacy 108](#), 42; [Calabash Solutions](#), 25; [Australian Council on Children and the Media](#), 10.

²²⁹⁹ Submissions to the Discussion Paper: [Privacy 108](#), 43; [CHOICE](#), 17; [Law Council of Australia](#), 19; [Electronic Frontiers](#), 16; [Salinger Privacy](#), 44.

²³⁰⁰ Australian Securities and Investments Commission, [Regulatory costs and levies](#) (Web Page, 15 December 2022).

25.8.1 Proposal – consult further on an industry funding model

Further extensive consultation and analysis would need to occur before it would be possible to determine whether an industry funding model would be suitable for the OAIC. Although this could take some time, there would be benefit in undertaking this work.

These investigations would include working with the Department of Finance and Treasury and involve:

- preparing a service catalogue of all of the OAIC’s activities and determining whether there is a basis for cost recovery of any of these activities
- determining whether certain industries are more problematic and costly to regulate
- determining which type of fees/levies may be appropriate or whether a combination of cost recovery levies, cost recovery fees and statutory levies would be feasible, and
- undertaking further consultation with stakeholders on an industry funding model, before deciding on any proposed model.

25.9 Funding litigation costs

The OAIC can be constrained in its ability to take enforcement action due to the cost associated with bringing enforcement proceedings against well-resourced entities and the possibility of significant costs orders being made against it.

The ACCC has a Litigation Contingency Fund which it can draw from to pay litigation cost orders. The fund has a reserve of \$20 million, and is periodically replenished through equity injections. The ACCC is permitted to incur an operating loss for litigation cost orders as it is funded through equity using the fund. The Australian Prudential Regulation Authority (APRA) and ASIC each have an enforcement special account to fund high cost cases against well-resourced entities.

For the OAIC to have assurance regarding its capacity to fund ongoing enforcement litigation and to pay any costs orders made against it, consideration should be given to establishing special accounts to cover costs orders and high litigation costs against well-resourced entities.

25.7 Further work should be done to investigate the effectiveness of an industry funding model for the OAIC.

25.8 Further consideration should be given to establishing a contingency litigation fund to fund any costs orders against the OAIC, and an enforcement special account to fund high cost litigation.

25.10 Annual reporting requirements

In response to submitter concern about lack of transparency about outcomes of complaints, the Discussion Paper proposed to increase transparency in the OAIC’s annual reporting on complaints, including numbers dismissed under each ground in section 41 of the Privacy Act.

All stakeholders who commented on this reform were in support of the proposal.²³⁰¹ The Australian Privacy Foundation submitted that this reporting is important as it is aware of many substantive privacy complaints (including systemic ‘class action’ type complaints) being dismissed under section 41 of the Act.²³⁰² The NSW Council for Civil Liberties considered it would increase accountability and improve the quality of the OAIC’s decision making in regard to their complaint handling process.²³⁰³

²³⁰¹ Submission to the Discussion Paper: [CHOICE](#), 17; [DIGI](#), 27; [elevenM](#), 65; [Australian Privacy Foundation](#), 17; [NSW Council for Civil Liberties](#), 38; [Australian Council on Children and the Media](#), 10; [Privacy 108](#), 45; [Privcore](#), 3; [Calabash Solutions](#), 26; [Australian Communications Consumer Action Network](#), 17.

²³⁰² Submission to the Discussion Paper: [Australian Privacy Foundation](#), 17.

²³⁰³ Submission to the Discussion Paper: [NSW Council for Civil Liberties](#), 38.

elevenM supported the publication of complaint handling-related information as it would 'provide both industry and individuals with greater information on trends and common outcomes, and be a tool for insights and guidance through examples'. It suggested this could be achieved without legislative amendment and that the OAIC could produce a standalone report on its complaint-handling with a consumer and industry-focus, similar to the NDB Report.²³⁰⁴

Privacy 108 considered additional reporting on the OAIC's complaint handling would benefit the regulated community and suggested case notes be published on completed complaints to provide examples of common complaints and outcomes.²³⁰⁵ Salinger Privacy considered better outcomes are needed for complainants who are not seeking compensation but rather a formal decision and other outcome or remedy from the complaints process.²³⁰⁶ Privcore considered that reporting case outcomes should go further than specifying the ground of dismissal and should provide sufficient meaning to assist regulated entities with resolving common and ordinary privacy complaint issues.²³⁰⁷

Calabash Solutions considered increased transparency about the outcome of complaints would prevent similar complaints from being raised and would assist the OAIC to identify where to allocate resources to update guidance to clarify a position, principle or aspect of the Act.²³⁰⁸

Other submitters supported increased transparency but considered that funding constraints on the OAIC are the primary cause of shortcomings in the OAIC's handling of complaints, which must be addressed.²³⁰⁹

The OAIC supported this reform to provide additional information about complaints and noted that it had done so in the past.²³¹⁰ However, it noted that complaints are often dismissed on multiple grounds and every matter is based on different circumstances so reporting these outcomes may not clarify the application of the Act.²³¹¹

25.10.1 Proposal – improve transparency in reporting on complaints

Additional reporting on complaint outcomes would providing greater clarity about how the Act is being interpreted and applied. Publishing the grounds on which complaints are dismissed would assist regulated entities and potential claimants to better understand how complaints are finalised.

In addition, several provisions in the Privacy Enforcement are directed at enhancing transparency such as providing the IC with the power to publish information relating to an assessment on the IC's website.

25.9 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 of section 41 of the Privacy Act.

25.11 Regulatory model

Some submitters to the Review raised concerns about the perceived tension between the OAIC's current dual roles as conciliator and regulator. The OAIC also noted that its ability to achieve its core purpose of promoting and upholding privacy rights in Australia would be enhanced if it was able to take a more targeted enforcement approach to priority areas.²³¹²

2304 Submission to the Discussion Paper: [elevenM](#), 65-66.

2305 Submission to the Discussion Paper: [Privacy 108](#), 45-46.

2306 Submission to the Discussion Paper: [Salinger Privacy](#), 43.

2307 Submission to the Discussion Paper: [Privcore](#), 3.

2308 Submission to the Discussion Paper: [Calabash Solutions](#), 26.

2309 Submission to the Discussion Paper: [Salinger Privacy](#), 43.

2310 Submission to the Discussion Paper: [OAIC](#), 200, referencing the OAIC Annual Report 2014-15.

2311 Ibid.

2312 Ibid 201.

The Discussion Paper proposed the following three options to improve the complaints handling process for complainants and allow the OAIC to focus on more strategic enforcement of the Act.

- **Option 1** - Encourage greater recognition and use of External Dispute Resolution schemes (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 (FPO) 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.

Stakeholder feedback on the three options proposed in the Discussion Paper was mixed. A small number of submitters supported encouraging greater recognition and use of EDRs.²³¹³ Many stakeholders supported creating an Ombudsman with responsibility for conciliating privacy complaints.²³¹⁴ The OAIC considered that a model combining elements of all three options would be beneficial.²³¹⁵ A small number of stakeholders thought that no changes are necessary²³¹⁶ and many of these raised that additional funding was instead needed.²³¹⁷ However the overwhelming majority of submitters supported a Deputy Commissioner for Enforcement role within the OAIC.²³¹⁸

25.11. 1 External Dispute Resolution schemes

The Australian Privacy Foundation strongly supported moving to an EDR model for privacy complaints and noted that the AFCA already handles a range of credit reporting and privacy complaints. It noted key advantages of moving to a separate and independent EDR was that EDR schemes have considerable expertise in resolving complaints and are user friendly and accessible and it would enable the OAIC to deal with systemic issues.²³¹⁹

The Insurance Council of Australia submitted that retaining and bolstering the AFCA's role in relation to privacy complaints would be a sensible outcome and reflect the policy desire for a 'one stop shop' for consumer financial disputes.²³²⁰

Other stakeholders considered this option would be inadequate as the currently registered EDR bodies do not cover the field. elevenM preferred an FPO over increased use of EDR schemes that did not specialise in privacy law. It noted that while EDR schemes can be particularly effective in high volume complaint areas such as telecommunications, energy and water, a deep understanding of privacy is the core component of effective privacy complaint management and consistent management of privacy complaints is an important element in improving consumer understanding, maintaining consumer trust, and educating industry.²³²¹

25.11.2 Privacy ombudsman

Submitters that supported establishing an FPO considered it would free up the OAIC to focus on enforcing breaches of the Act,²³²² concentrate on policy²³²³ and advice²³²⁴ and undertake focused reform and sector analysis²³²⁵ as part of a more strategic, proactive and enforcement-focused regulatory approach.²³²⁶

2313 Submissions to the Discussion Paper: [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 11; [Insurance Council of Australia](#), 18; [Australian Privacy Foundation](#), 18.

2314 Submissions to the Discussion Paper: [CHOICE](#), 17; [elevenM](#), 66; [Financial Rights Legal Centre and Financial Counselling Australia](#), 18; [KPMG](#), 30; [Centre for AI and Digital Ethics](#), 8; [Optus](#), 34; [Calabash Solutions](#), 26.

2315 Submission to the Discussion Paper: [OAIC](#), 202.

2316 Submissions to the Discussion Paper: [Australian Collectors & Debt Buyers Association](#), 12; [MIGA](#), 10; [Centre for Media Transition](#), 4; [Australian Council on Children and the Media, Privacy 108](#), 46; [Electronic Frontiers Australia](#), 17.

2317 Submission to the Discussion Paper: [Privacy 108](#), 46; [Electronic Frontiers Australia](#), 17.

2318 Submissions to the Discussion Paper: [Amazon Web Services](#), 3; [Australian Retail Credit Association](#), 13; [Consumer Policy Research Centre](#), 9; [IIS Partners and Ground Up Consulting](#), 8; [CPA Australia](#), 5; [DIGI](#), 27; [Free TV Australia](#), 35; [Law Council of Australia](#), 20; [NSW Council for Civil Liberties](#), 38-39; [Telstra](#), 28; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 12; [Federal Chamber of Automotive Industries](#), 29; [Minderoo Tech & Policy Lab, UWA Law School](#), 14.

2319 Submission to the Discussion Paper: [Australian Privacy Foundation](#), 18.

2320 Submission to the Discussion Paper: [Insurance Council of Australia](#), 18.

2321 Submission to the Discussion Paper: [elevenM](#), 66.

2322 Ibid.

2323 Submission to the Discussion Paper: [Centre for AI and Digital Ethics](#), 8.

2324 Submission to the Discussion Paper: [Equifax](#), 4.

2325 Submission to the Discussion Paper: [CHOICE](#), 18.

2326 Submission to the Discussion Paper: [elevenM](#), 66.

The DPI Report recommended an ombudsman scheme to resolve complaints and disputes with digital platform providers. It indicated that it may be appropriate for the Telecommunications Industry Ombudsman (TIO) to take on the role of a digital platforms ombudsman.²³²⁷ This was welcomed by the TIO but has not occurred.²³²⁸ It was further recommended in the ACCC's recent Digital Platform Services Interim Report²³²⁹ that an industry-specific ombuds should be established to handle any complaints and disputes that are subject to the mandatory minimum internal dispute resolution standards, and which have not been resolved to the consumer or business user's satisfaction, rather than an existing body such as the TIO. At present, the OAIC continues to handle privacy complaints against digital platforms.

Many submitters considered that an FPO would reduce consumer confusion.²³³⁰ Choice supported a hybrid proposal of a digital ombudsman (which would receive all complaints in relation to digital platforms) and noted that it would be easier for a consumer to identify the context of the breach (i.e. digital) than the type of consumer breach (i.e. privacy, discrimination or consumer rights).²³³¹

The Financial Rights Legal Centre cited the 2017 PC Report on Data Availability and Use recommendation that there be a 'no wrong door' approach to designing a regime for dealing with consumer data issues and complaints.²³³² It noted that this had been largely adopted in the CDR scheme with the OAIC taking primary responsibility for consumer complaints about privacy and data handling in the CDR system but EDR schemes like AFCA accepting complaints under s35A of the Privacy Act.²³³³

KPMG submitted that an FPO may alleviate the burden on entities that must respond to multiple regulators on overlapping areas of law and lessen consumer confusion.²³³⁴ Optus preferred the FPO option as providing clear separation of consumer dispute resolution and general regulatory functions for privacy matters, enabling the OAIC and the FPO to develop institutional expertise in their respective areas of responsibility.²³³⁵ Optus considered that the role of EDR schemes in privacy complaint handling should fall away once an FPO was established and that this was preferable where EDR schemes lack privacy expertise that could be offered by a specialist FPO.²³³⁶

Criticism of the FPO option centred on the concern that the underlying issue behind the OAIC's complaints handling focus is resourcing constraints which would not be addressed by moving responsibility for complaint handling to another entity.

25.11.3 Deputy Commissioner - Enforcement

Creating a Deputy Commissioner for Enforcement was supported by a large number of submitters as a simpler and potentially more cost-effective model.²³³⁷ The criticism of this option was that it did not address the issue of the OAIC having a dual role in complaint handling and enforcement.

Federal Chamber of Automobiles Institute submitted that this option would mean that the highly valued and proactive role the OAIC currently plays in resolving complaints would be preserved, while enabling it to develop a separate, strategically focused division to undertake enforcement activities. It highlighted that having both functions within the one organisation would ensure that knowledge gained from each function would be able to be shared across the organisation. In contrast, the other two options would result in additional cost, inefficiencies and loss of institutional knowledge.²³³⁸

²³²⁷ ACCC, [DPI Report](#), 510.

²³²⁸ Telecommunications Industry Ombudsman, [Response to ACCC's Digital Platforms Inquiry final report](#) (Web Page, 26 July 2019).

²³²⁹ ACCC, [Digital platform services inquiry](#) (Interim Report 5, September 2022) 4.3.

²³³⁰ Submissions to the Discussion Paper: [Financial Rights Legal Centre and Financial Counselling Australia](#), 19; [KPMG](#), 30.

²³³¹ Submission to the Discussion Paper: [CHOICE](#), 17-18.

²³³² Submission to the Discussion Paper: [Financial Rights Legal Centre and Financial Counselling Australia](#), 19 referencing Productivity Commission, [Data Availability and Use](#) (Report 82, March 2017) 37.

²³³³ Submission to the Discussion Paper: [Financial Rights Legal Centre and Financial Counselling Australia](#), 19.

²³³⁴ Submission to the Discussion Paper: [KPMG](#), 30.

²³³⁵ Submission to the Discussion Paper: [Optus](#), 34.

²³³⁶ Ibid.

²³³⁷ Submissions to the Discussion Paper: [Amazon Web Services](#), 3; [Australian Retail Credit Association](#), 13; [Consumer Policy Research Centre](#), 9; [IIS Partners and Ground Up Consulting](#), 8; [CPA Australia](#), 5; [DIGI](#), 27; [Free TV Australia](#), 35; [Law Council of Australia](#), 20; [NSW Council for Civil Liberties](#), 38-39; [Telstra](#), 28; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 12; [Federal Chamber of Automotive Industries](#), 29; [Minderoo Tech & Policy Lab, UWA Law School](#), 14.

²³³⁸ Submission to the Discussion Paper: [Federal Chamber of Automotive Industries](#), 29.

Amazon highlighted the benefit for entities of consistent relationships with regulators and that fragmentation of responsibilities can result in confusion. Amazon submitted that a single and consistent 'front door' will be a key component of the ongoing success of Australia's privacy and data protection laws²³³⁹. The Australian Retail Credit Association highlighted that the advantage of this option would be that the OAIC remains the appropriate home for specialist privacy knowledge and advice²³⁴⁰. The Consumer Policy Research Centre submitted that effective complaints mechanisms need to be supplemented by an adequately resourced regulator with the capacity and capability to monitor and enforce privacy breaches in this complex environment.²³⁴¹

25.11.4 Regulatory model combining all three options

The OAIC considered that the regulatory model could be modified to adopt elements from all three options in the Discussion Paper. It supported increased use of EDRs and noted that use of EDRs is working effectively in relation to credit reporting, where membership of an EDR scheme is a requirement built into Part IIIA of the Act.²³⁴² It submitted that the IC should be permitted to dismiss a complaint where it has already been adequately dealt with by a recognised EDR scheme (in addition to when it is in the process of being dealt with by an EDR scheme).²³⁴³

The OAIC recognised that establishing an independent FPO would send a strong signal about its changed regulatory focus but expressed concern about the high level of engagement that would be needed with the FPO to ensure consistent interpretation of the Act and to seek information about the FPO's complaint handling to gather intelligence to guide the OAIC's strategic enforcement work. It was also concerned about the potential for an FPO to result in individuals having to navigate multiple bodies to resolve their complaints. However, it thought these concerns could be addressed by establishing the FPO as an independent body within the OAIC, somewhat similar to the Australian Energy Regulator which is part of the ACCC but is governed by an independent board.²³⁴⁴ The OAIC also supported a new Deputy Commissioner for Enforcement and submitted that the additional executive capability dedicated to enforcement would be valuable as the OAIC transitions to a more strategic regulator with advanced enforcement powers.²³⁴⁵

25.12 Suggested changes to complaint-handling to support a combined regulatory model

The OAIC submitted that regardless of whether complaint-handling functions remain in the OAIC or are transferred to an FPO, amendments to the complaint handling provisions are required to address the resource-intensive nature of the current complaint model in the Act. It suggested amending the Act to give the IC discretion regarding whether to investigate complaints based on factors such as the IC's regulatory policies and priorities, whether the resources to investigate a complaint are proportionate to the likely outcome or remedy available and whether the substance of the complaint is about matters that fall under the Act.²³⁴⁶ It also thought that, if a direct right of action is introduced, a complaint should be able to be dismissed where the IC considers it would be more appropriately dealt with by the courts.²³⁴⁷

While a direct right of action for individuals to apply to the courts in respect of breaches of the Act is proposed (refer to Chapter 26), the ability for individuals to have their complaints dealt with by the OAIC as a less formal and lower cost avenue is an important safeguard for protecting Australian's privacy. Giving the IC discretion to not investigate complaints and to dismiss complaints in light of the availability of a direct right of action in the courts would undermine this safeguard. There is an existing ground for the IC to dismiss a complaint where it is *being* dealt with by an EDR scheme.²³⁴⁸ A logical extension of this ground would be where a complaint has already *been* adequately dealt with by an EDR scheme. This would make it clear that complaints that have already been dealt with by an EDR scheme would not need to be further considered.

²³³⁹ Submission to the Discussion Paper: [Amazon Web Services](#), 3.

²³⁴⁰ Submission to the Discussion Paper: [Australian Retail Credit Association](#), 13.

²³⁴¹ Submission to the Discussion Paper: [Consumer Policy Research Centre](#), 9.

²³⁴² Submission to the Discussion Paper: [OAIC](#), 203.

²³⁴³ *Ibid* 203.

²³⁴⁴ *Ibid* 204.

²³⁴⁵ *Ibid*.

²³⁴⁶ *Ibid* 205.

²³⁴⁷ *Ibid*.

²³⁴⁸ Privacy Act s 41(dc).

25.12.1 Proposal – Enhance the OAIC’s enforcement function

Strengthening the OAIC’s capacity to undertake its complaint handling and enforcement roles could address the regulatory model issues which have contributed to limited enforcement action by the OAIC in the most simple and cost-effective way. A ‘one-door’ pathway for redress for consumers would enable analysis of complaints types and related issues to inform decisions about where to focus strategic enforcement activity. Given the changes that will result to legislation and the OAIC’s functions as a result of the Review, the OAIC would benefit from conducting a strategic internal organisational review to ensure an enhanced enforcement focus with staff and resources dedicated to enforcement.

25.10 The OAIC should conduct a strategic internal organisational review with the objective of ensuring the OAIC is structured to have a greater enforcement focus.

25.11 Amend subsection 41(dc) so that the IC has the discretion not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme.

26. A direct right of action

The avenues available to individuals to litigate a claim for breach of their privacy under the Act are limited. Individuals may make a complaint to the IC about an alleged interference with their privacy²³⁴⁹ and where a determination is made, it may be enforced in the Federal Court and FCFCOA.²³⁵⁰ Individuals may apply to the Federal Court and the FCFCOA for injunctive relief for contraventions of the Act.²³⁵¹ The Act also allows a person who has suffered loss or damage as a result of contravention of certain credit reporting provisions to apply for a compensation order after the Federal Court or FCFCOA has made a civil penalty order or the entity has been found guilty of an offence.²³⁵² There is otherwise no mechanism by which a breach of the Act may be directly actioned by an individual in the courts.²³⁵³

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.²³⁵⁴

26.1 A right to directly enforce the Act in the courts

The Discussion Paper sought feedback on the following model for a direct right of action:

- 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 FCFCOA.
- The claimant would first need to make a complaint to the OAIC or Federal Privacy Ombudsman 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.

A majority of the submissions to the Discussion Paper that addressed this issue supported introducing a direct right of action. These submitters included academics,²³⁵⁵ regulators and complaints bodies,²³⁵⁶ civil society and consumer groups,²³⁵⁷ professional services,²³⁵⁸ unions,²³⁵⁹ and finance groups.²³⁶⁰ They considered that a direct right of action would provide consumers with greater control over their personal information, whilst also creating additional incentives for APP entities to comply with their obligations under the Act.²³⁶¹

2349 Ibid s 36.

2350 Ibid s 55A.

2351 Ibid s 80W; *Regulatory Powers (Standard Provisions) Act 2014* (Cth) s 121.

2352 Privacy Act ss 25 and 25A.

2353 *Day v Lynn* [2003] FCA 879, [50].

2354 ACCC, [DPI report](#) Recommendation 16(e), 473.

2355 Submissions to the Discussion Paper: [Castan Centre](#), 33; [Professor John V Swinson](#), 9; [Eckstein et al](#), 3; [Michael Douglas, UWA Law School](#), 4; [Graham Greenleaf, UNSW Sydney](#), 7; [Dr Katharine Kemp, UNSW Sydney](#), 19.

2356 Submissions to the Discussion Paper: [OAIC](#), 206; [Telecommunications Industry Ombudsman](#), 5; [Office of the Information Commissioner Queensland](#), 4.

2357 Submissions to the Discussion Paper: [NSW Council for Civil Liberties](#), 39; [CHOICE](#), 18; [Public Interest Advocacy Centre](#), 14; [Digital Rights Watch](#), 20; [Digital Law Association](#), 18; [Access Now](#), 5; [Australian Privacy Foundation](#), 18.

2358 Submissions to the Discussion Paper: [Calabash Solutions](#), 26; [elevenM](#), 67; [Privacy 108](#), 47.

2359 Submission to the Discussion Paper: [ACTU](#), 4.

2360 Submissions to the Discussion Paper: [Financial Services Council](#), 11; [Financial Rights Legal Centre and Financial Counselling Australia](#), 21.

2361 Submissions to the Discussion Paper: [Castan Centre](#), 33; [OAIC](#), 206; [Office of the Information Commissioner Queensland](#), 4; [NSW Council for Civil Liberties](#), 39.

Submitters opposed to introducing a direct right of action included digital platforms,²³⁶² telecommunications companies,²³⁶³ media organisations,²³⁶⁴ technology industry groups,²³⁶⁵ industry bodies,²³⁶⁶ fundraising organisations,²³⁶⁷ medical indemnity insurers,²³⁶⁸ a credit reporting agency,²³⁶⁹ and a consulting firm.²³⁷⁰ These submitters were generally opposed on the basis that a direct right of action would burden the courts²³⁷¹ and adversely impact business.²³⁷² Some considered that the current framework in which the IC deals with complaints and enforces the Act should enable issues to be addressed.²³⁷³ One submitter thought that a direct right of action would mainly benefit wealthy litigants.²³⁷⁴

26.2 Introduction of a direct right of action

The potential benefits for individuals and for compliance with the Act justify introducing a direct right of action into the Act. Such a right would be an important measure to enhance individuals' control of their personal information, and reflect current community expectations. 78 per cent of respondents to the 2020 ACAP survey believed they should have the right to seek compensation in the courts for a breach of privacy.²³⁷⁵

A direct right of action would increase the avenues available to individuals who suffer loss as a result of an interference with privacy to seek compensation. Empowering individuals in this way may also serve to increase consumers' bargaining power with businesses that collect and use their personal information.²³⁷⁶ Introducing a direct right of action into the Act would give Australians comparable rights to those available to individuals under overseas data protection laws including in the EU, New Zealand and Singapore.²³⁷⁷

The possibility of litigation could also encourage compliance with the Act. Michael Douglas noted that 'It is only if offending entities believe there will be serious consequences for interfering with individuals' privacy that they will be sufficiently motivated to not interfere'.²³⁷⁸ Additionally, given the relatively limited judicial consideration of the Act,²³⁷⁹ judicial interpretation of the Act in claims brought by individuals under a direct right of action would benefit individuals and APP entities by clarifying the application of the Act.²³⁸⁰

While there would be costs associated with a direct right of action, including costs associated with defending claims and resourcing the courts, these may be mitigated by ensuring that the design of a right of action strikes an appropriate balance between improving individuals' access to the courts, discouraging unmeritorious claims and efficient use of court resources.

26.2.1 Who could exercise the right?

The Discussion Paper proposed that the right would be available to both individuals and representative proceedings for classes of individuals who have suffered an alleged interference with their privacy.

²³⁶² Submissions to the Discussion Paper: [Snap Inc](#), 8; [DIGI](#), 28; [Meta](#), 10.

²³⁶³ Submissions to the Discussion Paper: [Telstra](#), 28; [Optus](#), 35; [Free TV Australia](#), 32.

²³⁶⁴ Submissions to the Discussion Paper: [ABC](#), 9; [SBS](#), 12.

²³⁶⁵ Submissions to the Discussion Paper: [Information Technology Industry Council](#), 4; [Communications Alliance Ltd](#), 19; [ACT | The App Association](#), 5; [BSA | The Software Alliance](#), 12.

²³⁶⁶ Submissions to the Discussion Paper: [Australian Chamber of Commerce and Industry \(ACCI\)](#), 19; [Business Council of Australia](#), 10; [Ai Group](#), 21; [Federal Chamber of Automotive Industries](#), 30; [FinTech Australia](#), 16.

²³⁶⁷ Submissions to the Discussion Paper: [Fundraising Institute Australia and Public Fundraising Regulatory Association](#), 11; [International Fund for Animal Welfare Australia](#), 4.

²³⁶⁸ Submissions to the Discussion Paper: [Medical Insurance Group Australia \(MIGA\)](#), 11; [Avant Mutual](#), 20.

²³⁶⁹ Submissions to the Discussion Paper: [Equifax](#), 5.

²³⁷⁰ Submission to the Discussion Paper: [KPMG](#), 31.

²³⁷¹ Submissions to the Discussion Paper: [Optus](#), 35; [Meta](#), 10; [Telstra](#), 28; [Equifax](#), 5.

²³⁷² Submissions to the Discussion Paper: [Australian Chamber of Commerce and Industry \(ACCI\)](#), 19; [Free TV Australia](#), 32; [ACT | The App Association](#), 5; [Experian Australia](#), 24; [Optus](#), 35.

²³⁷³ Submissions to the Discussion Paper: [Free TV Australia](#), 33; [KPMG](#), 31; [Business Council of Australia](#), 10; [ABC](#), 9; [Telstra](#), 28; [BSA | The Software Alliance](#), 12; [Optus](#), 35; [Meta](#), 53; [Ai Group](#), 21.

²³⁷⁴ Submission to the Discussion Paper: [Free TV Australia](#), 32.

²³⁷⁵ OAIC, [Australian Community Attitudes to Privacy Survey 2020](#) (Report, September 2020) 67.

²³⁷⁶ Submission to the Discussion Paper: [CHOICE](#), 18.

²³⁷⁷ Submission to the Discussion Paper: [Castan Centre](#), 34; GDPR art 82; *Privacy Act 2020* (NZ) s 98; *Personal Data Protection Act 2012* (Singapore) s 480.

²³⁷⁸ Submission to the Discussion Paper: [Michael Douglas, UWA Law School](#), 4.

²³⁷⁹ Submissions to the Discussion Paper: [Castan Centre](#), 34; [Graham Greenleaf, UNSW Sydney](#), 8.

²³⁸⁰ Submissions to the Discussion Paper: [OAIC](#), 206; [Public Interest Advocacy Centre](#), 15; [Privacy 108](#), 47.

Submissions to the Discussion Paper were generally supportive of the right being available to both individuals and to groups of individuals.²³⁸¹ Submitters in support noted that the availability of representative proceedings would increase access to justice for those who may not otherwise pursue a remedy through the court system due to costs.²³⁸²

Some submitters had reservations about extending the direct right of action to representative groups, as they were concerned that this would result in a proliferation of privacy class actions.²³⁸³ Some businesses and business groups considered that class action litigation is 'complex, costly, lengthy and open to abuse',²³⁸⁴ and reflected on perceived inadequacies regarding current regulation of class actions and litigation funding.²³⁸⁵

The Government completed consultation on 30 September 2022 on draft regulations which will facilitate further access to funding for class actions.²³⁸⁶ The Government is also considering recommendations put forward by the ALRC's report *Integrity, Fairness and Efficiency – An Inquiry into Class Action Proceedings and Third-Party Litigation Funders*.²³⁸⁷

Representative actions are available under the CDR²³⁸⁸ and for interferences with privacy in comparable jurisdictions, including the UK, EU and New Zealand.²³⁸⁹ Submitters highlighted that class actions overseas have shone a light on widespread and systemic privacy interferences in those jurisdictions, demonstrating the benefit of class action claims for enhancing regulatory compliance in a modern digital context.²³⁹⁰

Some submitters suggested that representative groups should have standing to bring actions on behalf of their members, in order to address potential inequality between parties with respect to expertise and resources.²³⁹¹ Representative groups may include non-for-profit organisations, non-governmental organisations and trade unions.

It is proposed that the direct right of action be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.²³⁹² This would include representative groups bringing claims on behalf of members who have been affected by breaches of the Act, with their consent.

26.2.2 Forum for the direct right of action

The DPI Report recommended the Federal Court or the Federal Circuit Court (now the FCFCOA) as the appropriate forum for a direct right of action. The Federal Court or FCFCOA are the forums in which IC determinations are currently able to be enforced²³⁹³ and injunctions may be sought.²³⁹⁴

The majority of submissions supported the Federal Court or the FCFCOA as the forum for a direct right of action.²³⁹⁵ Some considered that the Federal Court has the relevant jurisdiction, and appropriate experience to manage class actions.²³⁹⁶ The FCFCOA also has jurisdiction in consumer protection matters, which was highlighted as being beneficial given the potential for concurrent claims under privacy and consumer laws.²³⁹⁷

Some submitters expressed reservations about the accessibility of the Federal Court and FCFCOA, noting that time, cost, formality of proceedings, onerous evidentiary requirements and risks of adverse costs have acted as barriers to meritorious discrimination claims being brought in the Federal Court and FCFCOA.²³⁹⁸ A number of submitters supported the establishment of a small claims procedure to reduce both the cost and procedural burden on individuals seeking to exercise the direct right of action.²³⁹⁹

2381 Submissions to the Discussion Paper: [Castan Centre](#), 33; [Eckstein et al](#), 3; [elevenM](#), 68; [OAIC](#), 207; [CHOICE](#), 18; [Public Interest Advocacy Centre](#), 14.

2382 Submission to the Discussion Paper: [Michael Douglas, UWA Law School](#), 4.

2383 Submissions to the Discussion Paper: [Australian Institute of Company Directors](#), 5.

2384 Submission to the Discussion Paper: [Experian Australia](#), 24.

2385 Submission to the Discussion Paper: [Ai Group](#), 22; [Australian Institute of Company Directors](#), 6; [Australian Chamber of Commerce and Industry \(ACCI\)](#), 19.

2386 Department of the Treasury (Cth), [Exemptions for litigation funding schemes](#) (Web Page).

2387 ALRC, *Integrity, Fairness and Efficiency—An Inquiry into Class Action Proceedings and Third-Party Litigation Funders* ([ALRC Report 134](#), 24 January 2019).

2388 *Competition and Consumer Act 2010* (Cth) s 56EY.

2389 See GDPR arts 79 and 80; *Data Protection Act 2018* (UK) ss 168 and 188; *Privacy Act 2020* (NZ) ss 69 and 98.

2390 Cases such as C-362/14 Maximilian Schrems v Data Protection Commissioner, 6 October 2015 ("Schrems I Case"). Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximilian Schrems, 16 July 2020 ("Schrems II Case").

2391 Submissions to the Discussion Paper: [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 12; [Graham Greenleaf, UNSW Sydney](#), 8; [ACTU](#), 4.

2392 Note: Class actions under a proposed direct right of action would only be able to be brought in the Federal Court, as the FCFCOA does not have jurisdiction to hear representative proceedings.

2393 *Privacy Act* s 55A.

2394 *Ibid* s 80W.

2395 Submissions to the Discussion Paper: [Castan Centre](#), 36; [OAIC](#), 207; [CHOICE](#), 18; [Public Interest Advocacy Centre](#), 15.

2396 Submission to the Discussion Paper: [Optus](#), 36.

2397 *Ibid*.

2398 Submission to the Discussion Paper: [elevenM](#), 68.

2399 Submissions to the Discussion Paper: [Castan Centre](#), 36; [OAIC](#), 207; [NSW Council for Civil Liberties](#), 39.

A few submissions discussed whether a tribunal would be a lower cost option as the forum for the right.²⁴⁰⁰ In New Zealand, individuals have a direct right of action in relation to privacy through a Human Rights Review Tribunal. Currently under the Act, applications may be made to the AAT for review of the decisions of the Commissioner.²⁴⁰¹ The AAT conducts independent merits review of administrative determinations made under Commonwealth laws. While tribunals have been established in states and territories with administrative and judicial powers across a range of areas, federal tribunals may not exercise judicial power due to constitutional constraints. The same constraint prevents state and territory tribunals from exercising federal judicial power.²⁴⁰² Introducing a direct right of action to the courts would not replace the existing complaints process through the OAIC which would be a lower cost option still available to individuals. Furthermore, the gateway requirement, outlined below, to first lodge a complaint with the OAIC before applying to the courts would ensure that low-cost conciliation processes are available to individuals to resolve their concerns out of court.

It is considered that the Federal Court or the FCFCOA would be the appropriate forums for a direct right of action. The FCFCOA has power to provide injunctive relief and award damages for consumer law breaches of up to \$750,000. The FCFCOA also has a small claims procedure for certain consumer credit applications under \$40,000. The establishment of a small claims process could be considered post-implementation once information on how the right is being used and the resulting caseload and resourcing impact on the courts is clearer. Consideration should be given to appropriate thresholds for damages awards for privacy matters determined by the Federal Court and FCFCOA in the implementation of this proposal.

26.2.3 Gateway to enliven the right

A significant concern raised by submissions to the Issues and Discussion Papers was the potential impact of a direct right of action upon court resources.²⁴⁰³ A gateway model was proposed, aiming to balance the need for increased avenues for individuals to exercise their privacy rights with the need to ensure effective use of court resources.

Under the model proposed in the Discussion Paper, claimants would first be required to make a complaint to the OAIC or other complaint handling body to have their complaint assessed for conciliation. 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.²⁴⁰⁴

The complainant would also need to seek leave of the court to make the application.

Many submissions to the Discussion Paper agreed that a gateway model was an appropriate option if a direct right of action was introduced.²⁴⁰⁵ The OAIC noted in its submission that requiring complaints to be made to the regulator would ensure that it continues to have national oversight of privacy issues, enabling the identification of systemic issues which may direct it toward further regulatory or enforcement action.²⁴⁰⁶ It was also noted that by directing complaints to the OAIC, complainants would be best served by the OAIC's expertise in resolving privacy complaints.²⁴⁰⁷

Some submitters noted that a complainant's ability to 'opt-out' of conciliation may undermine the effective operation of the gateway.²⁴⁰⁸ In light of this, parties could be required to make a complaint to the OAIC first and attempt conciliation where it is deemed suitable by the OAIC. Where the IC is satisfied there is no reasonable likelihood that the complaint will be resolved by conciliation and has notified the complainant and respondent of this, or the IC decides not to investigate a complaint and the matter is deemed unsuitable for conciliation, the complainant would have the option to pursue the matter further in court.

2400 Submissions to the Discussion Paper: [Australian Communications Consumer Action Network](#), 20; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 13; [Salinger Privacy](#), 45.

2401 Privacy Act s 96.

2402 The Hon. Justice Garry Downes AM, 'Tribunals in Australia : Their Roles and Responsibilities' (2004) 84 *Reform* 7. See also Anna Oljnyk, 'Burns v Corbett: the latest word on State tribunals and judicial power' (2017) *Australian Public Law*.

2403 [Discussion Paper](#), 187; Submissions to the Discussion Paper: [ABC](#), 10; [Telstra](#), 28; [Communications Alliance Ltd](#), 19; [Social Services Portfolio](#), 32.

2404 [Discussion Paper](#), 188.

2405 Submissions to the Discussion Paper: [Avant Mutual](#), 20; 19; [Ramsay Health Care Australia](#), 10; [DIGI](#), 28; [Meta](#), 53; [Calabash Solutions](#), 26; [Google](#), 7.

2406 Submission to the Discussion Paper: [OAIC](#), 208.

2407 Submission to the Discussion Paper: [Financial Services Council](#), 12.

2408 Submissions to the Discussion Paper: [Financial Services Council](#), 11; [ABC](#), 10; [Telstra](#), 29; [Google](#), 7.

If the IC decided not to investigate a complaint on the basis that the IC did not consider the act or practice to have involved an interference with the privacy of an individual, or the complaint was frivolous, vexatious, misconceived, lacking in substance or not made in good faith, the complainant could be required to seek leave of the court to bring an application. The intent of requiring leave in these circumstances would be to prevent unmeritorious claims from being commenced.

The proposed model would be similar to that under the *Australian Human Rights Commission Act 1986* (Cth).²⁴⁰⁹ The AHRC receives a similar number of complaints to the OAIC,²⁴¹⁰ and also functions as a 'gateway' for applications to the Federal Court and FCFCOA by assessing complaints and attempting conciliation.²⁴¹¹ Over the period 2016-2021, the AHRC accepted on average 2288 complaints about discrimination and breaches of human rights per year.²⁴¹² Of the matters which were conciliated, 72.2 per cent achieved a successful conciliation outcome.²⁴¹³ In the same period, on average, 3.12 per cent of complaints received by the AHRC resulted in applications filed in the FCFCOA.²⁴¹⁴

Some submissions were critical of the gateway model,²⁴¹⁵ arguing that it may add procedural complexity for complainants. However, as the regulator responsible for privacy protections in Australia, the OAIC is best placed to provide advice and inform complainants of their rights under the Act. Other submitters voiced concerns about the additional time which may be required to assess complaints,²⁴¹⁶ however increased capacity for the OAIC as considered in Chapter 25 should enable it to fulfil this function efficiently. Ultimately, by encouraging the use of conciliation prior to commencing court proceedings, the resources of the court may be better preserved, and matters resolved in a more timely and cost-effective way.

26.2.4 Harm threshold

The Discussion Paper considered whether complainants would need to establish an element of harm to access the right, including whether the action should be limited to serious interferences with privacy to protect the court's resources.

Some submissions considered that if a direct right was introduced, a seriousness threshold would be helpful to prevent frivolous or vexatious claims coming before the courts.²⁴¹⁷ However, the cost and time involved in bringing an action in court, particularly where conciliation must first be attempted, would be likely to discourage frivolous claims. Where the Federal Court and FCFCOA are costs jurisdictions, the prospect of an adverse costs order would operate as a disincentive for claimants to commence unmeritorious claims.

The Castan Centre noted that a requirement for complainants to demonstrate a serious interference with privacy may have the effect of excluding claims affecting a large number of persons with only minor loss or damage, despite a major or systemic privacy breach.²⁴¹⁸ The OAIC also noted that a seriousness threshold may substantially curtail the effectiveness of the right, precluding many individuals from accessing rights under the Act.²⁴¹⁹ Restricting the action to serious interferences would reduce the deterrent effect of the right and would limit the utility of this right by discouraging litigation of breaches that do not clearly meet the seriousness threshold. The Public Interest Advocacy Centre also highlighted that requiring the court to make a determination on whether a breach is sufficiently 'serious' would be a burden on court time, costs, and resources.²⁴²⁰ Proposal 25.1 to introduce a mid-tier penalty provision to cover interferences with privacy (without the 'serious' element and aside from administrative breaches) would address these concerns.

²⁴⁰⁹ *Australian Human Rights Commission Act 1986* (Cth) Part IIB.

²⁴¹⁰ Over the period 2016-2021, the OAIC received on average 2,779 complaints per year. Over the same period, the AHRC received on average 2,288 complaints per year.

²⁴¹¹ *Australian Human Rights Commission Act 1986* (Cth) s 11(1).

²⁴¹² See AHRC Annual Reports 2017 – 2021, [Annual Reports Index | Australian Human Rights Commission](#). 2020-21: 3,113; 2019-20: 2,307; 2018-19: 2,037; 2017-18: 2,046; 2016-17: 1,939.

²⁴¹³ See AHRC Annual Reports 2017 – 2021, [Annual Reports Index | Australian Human Rights Commission](#). 2020-21: 1,517 conciliations, 70 per cent resolved; 2019-20: 1,432 conciliations, 70 per cent resolved; 2018-19: 1,396 conciliations, 72 per cent resolved; 2017-18: 1,262 conciliations, 74 per cent resolved; 2016-17: 1,128 conciliations, 75 per cent resolved.

²⁴¹⁴ See Federal Circuit Court Annual Reports, [Federal Circuit Court Annual Reports | Federal Circuit and Family Court of Australia](#): 2020-21: 75 human rights cases in FCC, 2.5 per cent of complaints accepted at AHRC; 2019-20: 70, 3 per cent of complaints accepted at AHRC; 2018-19: 86, 4.2 per cent of complaints accepted at AHRC; 2017-18: 60, 2.9 per cent of complaints accepted at AHRC; 2016-17: 58, 3 per cent of complaints accepted at AHRC. This figure does not include complaints which resulted in applications to the Federal Court.

²⁴¹⁵ Submissions to the Discussion Paper: [Professor John V Swinson](#), 10; [Michael Douglas, UWA Law School](#), 4; [Castan Centre](#), 36; [Graham Greenleaf, UNSW Sydney](#), 7; [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 12; [NSW Council for Civil Liberties](#), 40; [Public Interest Advocacy Centre](#), 15.

²⁴¹⁶ Submissions to the Discussion Paper: [Access Now](#), 5; [Public Interest Advocacy Centre](#), 16; [Professor John V Swinson](#), 9; [Privacy 108](#), 47.

²⁴¹⁷ Submissions to the Discussion Paper: [Australian Medical Association](#), 19; [Australian Association of National Advertisers](#), 6; [ABC](#), 10; [Telstra](#), 29; [Optus](#), 36; [Communications Alliance Ltd](#), 19; [DIGI](#), 28; [Meta](#), 53; [Calabash Solutions](#), 26; [Social Services Portfolio](#), 33; [FinTech Australia](#), 16.

²⁴¹⁸ Submission to the Discussion Paper: [Castan Centre](#), 41.

²⁴¹⁹ Submission to the Discussion Paper: [OAIC](#), 207.

²⁴²⁰ Submission to the Discussion Paper: [Public Interest Advocacy Centre](#), 17.

The Castan Centre also submitted that a requirement for complainants to demonstrate loss or damage may create an undue barrier to redress.²⁴²¹ However it is considered appropriate that a right of action should require loss or damage to an individual or class of individuals, as breaches of the Act which have not resulted in loss or damage would be better handled using other enforcement mechanisms. Formulating the direct right of action as requiring loss or damage, but not limiting it to serious breaches, would also bring the action into alignment with the existing CDR regime,²⁴²² as well as a number of international jurisdictions, including the UK, EU, New Zealand, and Singapore.²⁴²³ Further, Chapter 27 includes a proposal that a statutory tort for serious interferences with privacy be introduced which would not require proving actual damage to establish a cause of action.

It is proposed that the direct right of action be available to any individual or group of individuals who have suffered loss or damage as a result of privacy interferences by an APP entity. Loss or damage would need to be established within the existing meaning of the Act, including injury to the person's feelings or humiliation.²⁴²⁴

26.2.5 Role of the OAIC

The Discussion Paper considered whether the OAIC should be able to be heard in proceedings concerning the operation of the Act, including claims brought under a direct right of action, either as *amicus curiae* or as an intervener.

Submissions were supportive of the proposal that the OAIC be permitted to appear as *amicus curiae* to provide guidance at the request of the court.²⁴²⁵ An *amicus curiae*, or friend of the court, assists the court by 'drawing attention to some aspect of the case which might otherwise be overlooked',²⁴²⁶ but is not a party to the proceedings. The OAIC noted that the ability to appear as *amicus* would enable them to provide submissions, either at the request of the court or on their own motion, on the broad effect of proceedings, including the administration of the Act, the effect on privacy rights of people generally, or where other special circumstances in the public interest should be considered.²⁴²⁷ This would align with the approach taken for other regulators under domestic laws, including the ACCC, ASIC, and AHRC, where leave of the court to appear as *amicus curiae* may be sought for matters brought under their respective legislation.²⁴²⁸

The Public Interest Advocacy Centre submitted that in addition to the ability to appear as *amicus curiae*, the OAIC should have the power to intervene in proceedings.²⁴²⁹ An intervener, as distinguished from an *amicus curiae*, represents their own legal interests in proceedings. This would enable the OAIC to intervene in matters with future repercussions for its work.²⁴³⁰ As an independent statutory body whose functions include protecting the privacy of individuals in accordance with the Act, there would be no conflict in the OAIC exercising intervention powers in cases involving Government agencies. Other administrative bodies, including the ACCC, ASIC, and AHRC, have statutorily conferred powers to intervene.²⁴³¹ The ALRC in its Report 123 regarding a tort for serious invasions of privacy, recommended that the Privacy Commissioner be given functions to act as *amicus curiae* or to intervene in legal proceedings relating to serious invasions of privacy to assist the court or to represent the Commissioner's interests.²⁴³²

²⁴²¹ Submission to the Discussion Paper: [Castan Centre](#), 41.

²⁴²² Under the CDR, the right to bring an action for damages is available for a person who suffers loss or damage within the meaning of s 25(1) of the Act, *Competition and Consumer Act 2021* (Cth) s 56EY.

²⁴²³ UK: see *Lloyd v Google* [2021] UKSC 50, EU: GDPR Article 82; New Zealand: *Privacy Act 2020* (NZ) s 69; Singapore: *Personal Data Protection Act 2012*, s 480.

²⁴²⁴ *Privacy Act* s 25(1).

²⁴²⁵ Submissions to the Discussion Paper: [Castan Centre](#), 37; [elevenM](#), 68; [Access Now](#), 5; [CHOICE](#), 18; [Public Interest Advocacy Centre](#), 18.

²⁴²⁶ *Bropho v Tickner* (1993) 40 FCR 165, 172.

²⁴²⁷ Submission to the Discussion Paper: [OAIC](#), 209.

²⁴²⁸ The ACCC and ASIC may seek leave to appear as *amicus curiae*, and this may be granted pursuant to the court's inherent power to ensure that it is properly informed of matters which it ought to take into account in reaching its decision (*United States Tobacco Co v Minister for Consumer Affairs* (1988) 83 ALR 79; *Bropho v Tickner* (1993) 40 FCR 165; *Breen v Williams* (1994) 35 NSWLR 522). For the AHRC, an individual 'special-purpose' Commissioner within the AHRC may act as *amicus curiae* with leave of the court under the *Australian Human Rights Commission Act* (Cth) s 46PV.

²⁴²⁹ Submission to the Discussion Paper: [Public Interest Advocacy Centre](#), 31.

²⁴³⁰ [ALRC Report 123](#), 319.

²⁴³¹ The ACCC may intervene in proceedings under the *Competition and Consumer Act 2010* (Cth) s 87CA; ASIC may exercise an intervention function in relation to proceedings about customer protection and financial services: *Australian Securities and Investments Commission Act 2001* (Cth) s 12G0; The AHRC may intervene in proceedings involving issues of discrimination or human rights issues: *Australian Human Rights Commission Act* (Cth) s 11(1)(o) and s 31(j); *Racial Discrimination Act 1975* (Cth) s 20(1)(e); *Sex Discrimination Act 1984* (Cth) s 48(1)(gb); *Disability Discrimination Act 1992* (Cth) s 67(1)(l); *Age Discrimination Act 2004* (Cth) s 53(1)(g).

²⁴³² [ALRC Report 123](#), 317.

It is proposed that the OAIC be able to appear as *amicus curiae* or to intervene in proceedings instituted by individuals under the Act, with leave of the court. The OAIC should develop guidance on their approach to involvement in court proceedings, and the circumstances under which the OAIC may seek to intervene similar to those of other regulators.²⁴³³

26.2.6 Remedies

The Discussion Paper considered what remedies could be available under a direct right of action. The DPI Report recommended that remedies should include compensatory damages as well as aggravated and exemplary damages (in exceptional circumstances) for financial and non-financial harm suffered as a result of infringement of the Act.²⁴³⁴

The majority of submissions to the Discussion Paper supported the court having discretion with respect to damages.²⁴³⁵ Submissions considered it important to allow the courts broad and unrestricted decision-making power to determine appropriate remedies.²⁴³⁶ The OAIC noted that providing the courts with broad scope to interpret the Act would allow them to set the standards for appropriate types and levels of damages, taking the particular facts and circumstances of each case into account. Ultimately, this would allow compensation to 'reflect, and keep pace with, the changing landscape of privacy harms'.²⁴³⁷

The Castan Centre noted the powers of the court with respect to the discrimination cases under the *Australian Human Rights Commission Act 1986* (Cth), highlighting that, similar to unlawful discrimination, privacy breaches may primarily affect the dignitary interests of complainants.²⁴³⁸ It therefore suggested that the court should have broad remedial powers to adequately address non-pecuniary losses in privacy matters.

There was concern expressed that without a cap on damages, a direct right of action may unduly burden business and stifle innovation.²⁴³⁹ Under the proposed model, the costs burden on business would be proportionate to the consequences of breach of the Act, with the courts able to award nominal or low-level damages depending on the circumstances of the case. Submissions to the Issues Paper also noted that any cap on damages may discourage individuals from bringing serious matters, and enable defendants to make settlement offers relative to a cap.²⁴⁴⁰ It was also noted that comparable jurisdictions including the EU, Singapore, and Canada do not have a cap on damages.

Some submissions expressly supported the courts being able to award exemplary and aggravated damages where appropriate.²⁴⁴¹ Providing scope for the Federal Court or FCFCOA to make any order it sees fit would ensure consistency with the proposed reform to the enforcement provisions (refer to Chapter 25), to allow a court to make any order it sees fit when awarding a civil penalty.

It is proposed that remedies available under the direct right of action be any order the court sees fit, including any amount of damages.

2433 For example: ASIC, [ASIC's approach to involvement in private court proceedings](#) (Web Page, 2013); ACCC, [ACCC intervention in private proceedings](#) (July 2002).

2434 ACCC, [DPI Report](#) 473.

2435 Submissions to the Discussion Paper: [Digital Rights Watch](#), 2; [CHOICE](#), 18; [Public Interest Advocacy Centre](#), 19; [elevenM](#), 67; [Calabash Solutions](#), 26; [Michael Douglas, UWA Law School](#), 4; [Eckstein et al](#), 3.

2436 Submission to the Discussion Paper: [Castan Centre](#), 38.

2437 Submission to the Discussion Paper: [OAIC](#), 207.

2438 Submission to the Discussion Paper: [Castan Centre](#), 38.

2439 Submission to the Discussion Paper: [Snap Inc](#), 8.

2440 [Discussion Paper](#), 189-190.

2441 Submissions to the Discussion Paper: [Michael Douglas, UWA Law School](#), 4; [Calabash Solutions](#), 26.

Proposal – Direct Right of Action

The Act should be amended to permit individuals to apply to the courts for relief in relation to an interference with privacy with the following design elements:

- (a) The action would be available to any individual or group of individuals who have suffered loss or damage as a result of privacy interference by an APP entity. This would include claims by representative groups on behalf of members affected by breaches of the Act.
- (b) Loss or damage would need to be established within the existing meaning of the Act, including injury to the person's feelings or humiliation.
- (c) The action would be heard by the Federal Court or the FCFCOA.
- (d) The claimant would first need to make a complaint to the OAIC and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme.
- (e) Where the IC or an EDR is satisfied there is no reasonable likelihood that the complaint will be resolved by conciliation or the IC decides a complaint is unsuitable for conciliation, the complainant would have the option to pursue the matter further in court.
- (f) In cases where the IC has decided that a complaint is unsuitable for conciliation on the basis that the complaint does not involve an interference with privacy or is frivolous or vexatious, the complainant should be required to seek leave of the court to bring an application in the court.
- (g) The OAIC would have the ability to appear as *amicus curiae* or to intervene in proceedings instituted under the *Privacy Act*, with leave of the court.
- (h) Remedies available under this right would be any order the court sees fit, including any amount of damages.

Appropriate resources should be provided to the Courts to deal with these new functions.

26.1 Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in this chapter.

27. A statutory tort for serious invasions of privacy

The Act regulates the handling of personal information by APP entities. It does not regulate information-handling by non-APP entities (such as individuals and most small businesses) and does not provide protections in relation to bodily or territorial privacy. Invasions of bodily privacy may be serious physical invasions during unnecessary medical treatment²⁴⁴² or spying and recording private affairs.²⁴⁴³ Invasions of territorial privacy could include invasion in a search of a person's home or property.²⁴⁴⁴ A number of previous inquiries in Australia have recommended introducing a statutory cause of action for serious invasions of privacy, including ALRC Report 108, the ACCC's DPI Report, and the AHRC's Human Rights and Technology Final Report.²⁴⁴⁵ Several state review processes have also recommended introducing a statutory cause of action for invasion of privacy.²⁴⁴⁶

The Discussion Paper considered whether there are serious invasions of privacy for which victims are currently unable to seek compensation under the Act and reviewed avenues available in comparable jurisdictions for seeking redress for such actions. It proposed four possible options to provide a legal avenue for compensation for individuals who suffer serious invasions of privacy in Australia.

- **Options involving a statutory tort:**
 1. The statutory tort model recommended in the ALRC Report 123.
 2. A minimalist tort that leaves the scope and application of the tort to be developed by the courts.
- **Options not involving a statutory tort:**
 3. Extending the application of the Act to individuals in a non-business capacity for collection, use or disclose of personal information which would be highly offensive to an objective reasonable person.
 4. States and territories could consider legislating that damages for emotional distress are available in actions for equitable breach of confidence.

Most submitters who addressed this issue supported introducing a statutory tort, with the overwhelming majority preferring the ALRC Report 123 model. Supporters of a statutory tort included academics,²⁴⁴⁷ privacy and consumer advocates,²⁴⁴⁸ the Law Council of Australia,²⁴⁴⁹ the OAIC,²⁴⁵⁰ and the Office of the Information Commissioner Queensland.²⁴⁵¹ A significant minority of submitters opposed any tort, largely from media,²⁴⁵² the health industry,²⁴⁵³ and some businesses.²⁴⁵⁴ Others did not oppose a tort, but expressed caution about its operation and submitted that it would require exceptions.²⁴⁵⁵ The information technology industry was split between supporters²⁴⁵⁶ and opponents.²⁴⁵⁷

There was far less engagement with options 3 and 4 in submissions, although two APP entity submitters who opposed a tort supported extending the Act to individuals.²⁴⁵⁸

²⁴⁴² AHRC, [Ensuring health and bodily integrity: towards a human rights approach for people born with variations in sex characteristics](#) (Report, October 2021) 40-41.

²⁴⁴³ [ALRC Report 123](#), 74.

²⁴⁴⁴ *Ibid*, 142.

²⁴⁴⁵ *Ibid* rec 74-1; ACCC, [DPI Report](#), rec 19; AHRC, [Human Rights and Technology](#) (Final Report, March 2021) rec 21.

²⁴⁴⁶ NSW: New South Wales Law Reform Commission, [Invasion of Privacy](#) (Report 120, April 2009) 4 – and further in the Standing Committee on Law and Justice, Parliament of New South Wales, [Inquiry into remedies for the serious invasion of privacy in New South Wales](#) (Final Report, March 2016) 10. South Australia: South Australian Law Reform Institute, [A statutory tort for invasion of privacy](#) (Final Report 4, March 2016) rec 1 – this report resulted in the Civil Liability (Serious Invasions of Privacy) Bill 2021 (SA) to introduce a statutory cause of action in tort, tabled for consideration in the 54th South Australian Parliament. Queensland: Crime and Corruption Commission Queensland, [Operation Impala: Report on misuse of confidential information in the Queensland public sector](#) (February 2020) 19.

Victoria: Victorian Law Reform Commission, [Surveillance in Public Places](#) (Final Report 18, May 2010) rec 22 – although the discussion was of a statutory tort generally, the recommendation was directed specifically at statutory causes of action for misuse of surveillance.

²⁴⁴⁷ Submissions to the Discussion Paper: [Professor John V Swinson](#), 10; [Eckstein et al.](#), 3; [Kimberlee Weatherall](#), [Tom Manousaridis](#), [Melanie Trezise](#), 6-7; [Prof Barbara McDonald](#) and [Prof David Rolph](#), University of Sydney, 3; [Professor David Lindsay](#), 26; [Graham Greenleaf](#), UNSW Sydney, 8; [Dr Katharine Kemp](#), UNSW Sydney, 19.

²⁴⁴⁸ Submissions to the Discussion Paper: [Privacy 108](#), 47-48; [Access Now](#), 4; [Australian Communications Consumer Action Network](#), 20; [Financial Rights Legal Centre and Financial Counselling Australia](#), 21; [elevenM](#), 71-72; [Australian Council on Children and the Media](#), 11; [Centre for Media Transition](#), 4, 11; [Castan Centre](#), 44-48; [Australian Privacy Foundation](#), 18-19.

²⁴⁴⁹ Submission to the Discussion Paper: [Law Council of Australia](#), 20-21.

²⁴⁵⁰ Submission to the Discussion Paper: [OAIC](#), 211-215.

²⁴⁵¹ Submission to the Discussion Paper: [Office of the Information Commissioner Queensland](#), 4.

²⁴⁵² Submissions to the Discussion Paper: [Commercial Radio Australia](#), 3; [Australia's Right to Know](#), 1; [SBS](#), 9-10, 12-13; [Optus](#), 36-37; [ABC](#), 10-12.

²⁴⁵³ Submissions to the Discussion Paper: [Ramsay Health Care Australia](#), 10; [Australian Medical Association](#), 19; [Medical Insurance Group Australia](#), 12.

²⁴⁵⁴ Submissions to the Discussion Paper: [Business Council of Australia](#), 10-11; [Australian Collectors & Debt Buyers Association](#), 14.

²⁴⁵⁵ Submissions to the Discussion Paper: [Snap Inc.](#), 8-9; [Governance Institute of Australia](#), 8; [Federal Chamber of Automotive Industries](#), 31; [AFP](#), 8-9; [Google](#), 7.

²⁴⁵⁶ Submissions to the Discussion Paper: [Meta](#), 54; [Electronic Frontiers Australia](#), 18; [ADIA](#), 8.

²⁴⁵⁷ Submissions to the Discussion Paper: [Communications Alliance Ltd](#), 20; [Information Technology Industry Council](#), 4; [Internet Association of Australia](#), 4; [BSA | The Software Alliance](#), 12.

²⁴⁵⁸ Submissions to the Discussion Paper: [DIGI](#), 28-29; [Australian Collectors & Debt Buyers Association](#), 14.

27.1 The need for a tort of privacy

The Discussion Paper cited examples given in submissions of the sorts of behaviour that a tort for invasion of privacy would address that are not covered by the Act. The Discussion Paper did not express a view on whether a statutory tort for invasions of privacy is needed and indicated that the issue would continue to be considered following responses to the Discussion Paper.

Salinger Privacy and Privacy 108 submitted that as a tort had been recommended by several inquiries the need for it did not need to be relitigated.²⁴⁵⁹ The OAIC considered that a statutory tort would provide greater coverage and protection to individuals in line with Article 17 of the *International Covenant on Civil and Political Rights*,²⁴⁶⁰ which provides that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

In particular the OAIC considered the Act would not protect the following invasions of privacy:²⁴⁶¹

- peering over a back fence to take a video of someone in their backyard, or other place where there is an expectation of privacy (for example, in a public bathroom)
- recording a private conversation with someone without their knowledge or consent
- interfering with, misusing or disclosing an individual's private correspondence or private written, oral or electronic communication
- disclosing or disseminating sensitive facts relating to an individual's private life
- misusing personal information about another person that was accessed in breach of an employment contract, but for which the employer is not liable because it was misused for a personal purpose (for example blackmail or Family Court proceedings)
- a data breach experienced by a small business or individual not covered by the Act.

In contrast, most submitters opposed to the tort contended that current laws (such as surveillance and family law statutes, or existing torts (including defamation), and breach of confidence) and complaint mechanisms provide adequate protection of individual privacy.²⁴⁶² Media organisations submitted that the co-regulatory regime established by section 123 of the *Broadcasting Services Act 1992* (Cth), which requires industry groups to develop codes of practice, is sufficient.²⁴⁶³ However, these codes, discussed in greater detail in Chapter 9, do not provide for causes of action for individuals to protect their privacy or seek compensation in a court. Others that considered the current protections in the Privacy Act to be sufficient submitted that, if enacted, a tort should only cover entities which are not already regulated by the Act.²⁴⁶⁴

Salinger Privacy highlighted that a broader range of circumstances would be actionable under a statutory tort than would be captured by the Privacy Act, including through any direct right of action for compensation relying on a breach of the Act (See Chapter 26). A tort could extend to actions by:²⁴⁶⁵

- i. entities which are not covered by the Act (e.g. individuals acting in a personal capacity, most small businesses, registered political parties (subject to the removal or modification of exemptions))
- ii. respondents which are covered by the Act but the conduct at issue is exempt from the APPs (e.g. acts or practices subject to an exemption, such as those performed as a contracted service provider to a State or Territory authority)
- iii. rogue employees acting beyond the scope of their authority and whose employers may not be liable under the Act for such conduct
- iv. State and Territory authorities not covered by privacy laws or where the compensable harm exceeds statutory compensation caps (e.g. South Australian and Western Australian state and local government entities, or e.g. NSW public sector agencies are only liable for up to \$40,000 for privacy complaints brought under the *Privacy and Personal Information Protection Act 1998* (NSW), respectively).

²⁴⁵⁹ Submissions to the Discussion Paper: [Salinger Privacy](#), 46-47; [Privacy 108](#), 48.

²⁴⁶⁰ Submission to the Discussion Paper: [OAIC](#), 212.

²⁴⁶¹ *Ibid.*

²⁴⁶² Submissions to the Discussion Paper: [Ai Group](#), 23; [Governance Institute of Australia](#), 8; [ABC](#), 11; [Guardian Australia](#), 21.

²⁴⁶³ Submissions to the Discussion Paper: [SBS](#), 12-13; [Commercial Radio Australia](#), 4.

²⁴⁶⁴ Submission to the Discussion Paper: [Medical Insurance Group Australia](#), 12.

²⁴⁶⁵ Submission to the Discussion Paper: [Salinger Privacy](#), 46.

Submitters in support of a statutory tort did not consider that other laws or causes of action currently available provide redress for the wrong of a serious invasion of privacy. Breach of confidence is concerned with protecting confidentiality in the context of a relationship of confidence. It has been found to extend to intimate images shared in a personal romantic relationship.²⁴⁶⁶ However, it does not protect a person from an invasion of their privacy in the absence of any relationship of confidence such as unwanted observation, or dishonestly obtaining private information from the person under the obligation of confidence.²⁴⁶⁷

The tort of defamation may allow an individual to receive compensation for a defamatory misuse of personal information. However, the complete defence of 'truth',²⁴⁶⁸ means that the law of defamation will only provide protection for private information that is untrue.²⁴⁶⁹ In a privacy setting, it is likely that true information will be more harmful. The ALRC further considered that the law of defamation does not even provide adequate protection for all information that is incorrect.²⁴⁷⁰ If untrue information is misused, but that misuse is not defamatory, the tort of defamation will provide no remedy.

A complaint to the IC may result in an investigation by the IC under section 40 of the Privacy Act and a determination by the IC under section 52, which may include a declaration that the complainant is entitled to an amount by way of compensation. As discussed in Chapters 25 and 26, a determination under section 52 is enforceable in the court.²⁴⁷¹ A direct right of action would allow a more direct route to the court for a breach of the Act than is currently available. However, in either case, the right of an individual to go to court to protect their privacy would be limited by the scope of the Act which does not cover certain entities and does not extend to aspects of 'intrusion upon seclusion' or physical privacy, as the proposed tort would.

Finally, State and Territory surveillance laws do not cover the field in terms of physical privacy. To the extent of overlap (such as installing a device to film someone without their knowledge), most of these statutes criminalise certain conduct and do not provide avenues to seek compensation in the form of damages.²⁴⁷²

An examination of existing frameworks indicates clear gaps in current privacy protection, and the ability of an individual to take steps to protect themselves and seek compensation for invasion of privacy. These gaps would be best addressed through a single privacy tort designed to cover the field.

27.2 Preferred option – ALRC Report 123 model

The OAIC considered that the statutory tort recommended by the ALRC Report 123 would be an important addition to the suite of regulatory measures needed to address gaps in the existing privacy protection framework and current and emerging privacy risks and harms.²⁴⁷³

Professor Barbara McDonald, former ALRC Commissioner who led the Inquiry into Serious Invasions of Privacy in the Digital Era, noted that the model recommended in Report 123 was the culmination of significant targeted research, consultation, analysis, negotiation and compromise.²⁴⁷⁴ The majority of submitters considered that the ALRC's recommended model and reasoning as set out in Report 123 effectively balanced competing interests.²⁴⁷⁵

Many submitters noted the lack of development of the common law in Australia since *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* raised the potential for a tort of privacy in Australia over 20 years ago.²⁴⁷⁶ In *Smethurst v Commissioner of Police*,²⁴⁷⁷ the High Court appeared open to the possibility of the common law recognising a tort of privacy in the future (at [90]), however as the plaintiffs (a *Sunday Telegraph* journalist and the newspaper's publisher) did not raise the question, the Court did not answer it.

²⁴⁶⁶ *Wilson v Ferguson* [2015] WASC 15; *Giller v Procopets* [2008] VSCA 236.

²⁴⁶⁷ Submission to the Discussion Paper: [Dr Jelena Gligorijevic, ANU College of Law](#), 5.

²⁴⁶⁸ *Defamation Act 2004* (NSW) s 25; *Defamation Act 2005* (Qld) s 25; *Defamation Act 2006* (NT) s 22; *Defamation Act 2005* (SA) s 23; *Defamation Act 2005* (Tas) s 25; *Defamation Act 2005* (Vic) s 25; *Defamation Act 2005* (WA) s 25.

²⁴⁶⁹ [ALRC Report 123](#), 84.

²⁴⁷⁰ *Ibid* 84.

²⁴⁷¹ *Privacy Act* s 55A.

²⁴⁷² Submission to the Issues Paper: [New South Wales Information and Privacy Commission](#), 4, discussing the *Crimes Act 1900* (NSW) and the *Surveillance Devices Act 2007* (NSW).

²⁴⁷³ Submission to the Discussion Paper: [OAIC](#), 213.

²⁴⁷⁴ Submission to the Discussion Paper: [Prof Barbara McDonald and Prof David Rolph, University of Sydney](#), 1.

²⁴⁷⁵ Submissions to the Discussion Paper: [Kimberlee Weatherall, Tom Manousaridis, Melanie Trezise](#), 7; [elevenM](#), 72.

²⁴⁷⁶ *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

²⁴⁷⁷ *Smethurst v Commissioner of Police* [2020] HCA 14.

Australia would not be the first jurisdiction to enact a statutory tort of privacy. The Canadian provinces of British Columbia,²⁴⁷⁸ Manitoba,²⁴⁷⁹ Newfoundland and Labrador,²⁴⁸⁰ Quebec²⁴⁸¹ and Saskatchewan²⁴⁸² have enacted statutory torts; as has the State of California in the US.²⁴⁸³

Submitters considered that the lack of development by the courts and lack of litigants raising the prospect of a tort warranted legislative intervention to set the boundaries of the tort and avoid further decades of uncertainty.²⁴⁸⁴

27.2.1 Essential features of the ALRC Report 123 model

The ALRC Report 123 examined the civil causes of action for serious invasion of privacy in New Zealand, the UK, the USA and Canada.²⁴⁸⁵ The model for a statutory tort was recommended in light of analysis of the torts in comparable jurisdictions, with particular focus on the UK and New Zealand.²⁴⁸⁶

The essential features of the ALRC Report 123 tort of serious invasion of privacy cause of action

- the invasion of privacy must be either by:
 - intrusion into seclusion, or
 - misuse of private information
- it must be proved that a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances
- the invasion must have been committed intentionally or recklessly – mere negligence is not sufficient
- the invasion must be ‘serious’
- the invasion need not cause actual damage, and damages for emotional distress may be awarded, and
- it is subject to a ‘balancing exercise’ – the court must be satisfied that the public interest in privacy outweighs any countervailing public interests.²⁴⁸⁷

Recommended defences	Recommended remedies for a plaintiff
<ul style="list-style-type: none"> • a defence of lawful authority • a defence where the conduct was incidental to defence of persons or property • a defence of consent • a defence of necessity • a defence of absolute privilege • a defence for the publication of public documents, and • a defence for fair reporting of public proceedings.²⁴⁸⁸ 	<ul style="list-style-type: none"> • damages, including for emotional distress and, in exceptional circumstances, exemplary damages • an account of profits • injunctions • delivery up, destruction and removal of material • correction and apology orders, and • declarations.²⁴⁸⁹

As noted by the ALRC, adopting similar concepts and tests to overseas jurisdictions would enable Australian courts to draw from jurisprudence from the UK, New Zealand and the US.²⁴⁹⁰

²⁴⁷⁸ *Privacy Act*, RSBC 1996, c 373 (British Columbia).

²⁴⁷⁹ *Privacy Act*, CCSM 1996, c P125 (Manitoba).

²⁴⁸⁰ *Privacy Act*, RSNL 1990, c P-22 (Newfoundland and Labrador).

²⁴⁸¹ *Civil Code of Quebec*, SQ 1991, c 64 ss 3, 35–37.

²⁴⁸² *Privacy Act*, RSS 1978, c P-24 (Saskatchewan).

²⁴⁸³ *California Civil Code* § 1708.8.

²⁴⁸⁴ Submissions to the Discussion Paper: [DIGI](#), 28–29; [Ai Group](#), 23; [Prof Barbara McDonald and Prof David Rolph, University of Sydney](#), 3; [elevenM](#), 72; [NSW Council for Civil Liberties](#), 41–42; [Kimberlee Weatherall, Tom Manousaridis, Melanie Trezise](#), 6–7; [Michael Douglas, UWA Law School](#), 4–5.

²⁴⁸⁵ [ALRC Report 123](#), *inter alia* 22–23; 76–82; 93–94; 112–113; 160–161; 288.

²⁴⁸⁶ *Ibid* 76–82; Chapter 5 generally; 93–94.

²⁴⁸⁷ *Ibid* 123, 19.

²⁴⁸⁸ [ALRC Report 123](#), 19–20.

²⁴⁸⁹ *Ibid* 20.

²⁴⁹⁰ *Ibid* 94.

27.2.2 A fault element of recklessness not negligence

The ALRC recommended that the fault element of the tort of serious invasion of privacy be intention or recklessness.²⁴⁹¹ The OAIC submitted in its response to the Issue Paper that the fault element should include negligence to avoid unnecessarily limiting the application of the tort to different circumstances that may result in serious privacy invasions.²⁴⁹² elevenM in response to the Discussion Paper queried whether it would be appropriate to give further consideration to an additional fault element of negligence.²⁴⁹³ The Public Interest Advocacy Centre and Castan Centre submitted negligence should be part of the fault element of the tort.²⁴⁹⁴ Castan Centre considered that the ALRC model would set the bar too high and noted that the NSW Law Reform Commission and the Victorian Law Reform Commission did not specify fault standards in their recommendations for causes of action in privacy.²⁴⁹⁵ PIAC was concerned to ensure that a victim would have legal recourse for a negligent act, such as negligence in information handling resulting in release of information. PAIC considered some negligent releases of information would not reach the threshold of 'reckless' but may have an equally serious impact.²⁴⁹⁶

The ALRC considered the privacy harms which may be caused by negligence in its Report 123.²⁴⁹⁷ A cause of action in negligence may still be available to plaintiff for these acts if they can demonstrate a duty of care. But absent a relationship establishing a duty of care, extending fault for a serious invasion of privacy to negligence or gross negligence risks being too broad, potentially resulting in organisations adopting an overly cautious approach to many information disclosure activities.²⁴⁹⁸ Adopting a fault element of intention and recklessness would allow an action in tort without proof of damage in line with the torts of assault and false imprisonment. Extending the fault element to negligence would undermine an important justification for making the tort actionable without proof of damage.²⁴⁹⁹ Proof of damage is an essential element of the tort of negligence.

Consistent with the conclusion of the ALRC in Report 123,²⁵⁰⁰ intention or recklessness is considered the appropriate standard of fault. Recklessness would capture circumstances where the parties do not have a pre-existing relationship, but where risk of invasion is known or foreseen.²⁵⁰¹

27.3 Other options are unsuitable

The other options proposed in the Discussion Paper in the alternative to the ALRC Report 123 model tort would not be suitable to adequately address the gap in the law.

27.3.1 A minimalist tort

A small number of academic submitters preferred a minimalist statutory tort as proposed in Option 2 in the Discussion Paper on the basis that it would leave greater room for it to develop through the common law.²⁵⁰² For example, through successive cases it could potentially extend into other areas of privacy interests such as those recognised in the US like 'false light' and dignity.²⁵⁰³ The ALRC considered that what is commonly called 'false light' and 'approbation' could potentially be captured by the Report 123 statutory tort, but those wrongs were not intended to be captured per se. The ALRC noted those wrongs may be addressed by other causes of action and in Australian law should be considered broadly, including in the context of intellectual property law.²⁵⁰⁴

²⁴⁹¹ Ibid 110.

²⁴⁹² Submission to the Issues Paper: [OAIC](#), 136. The OAIC did not repeat this submission in response to the Discussion Paper.

²⁴⁹³ Submission to the Discussion Paper: [elevenM](#), 72.

²⁴⁹⁴ Submissions to the Discussion Paper: [Public Interest Advocacy Centre](#), 21-22; [Castan Centre](#), 56-57.

²⁴⁹⁵ Submission to the Discussion Paper: [Castan Centre](#), 56-57, referring to Victorian Law Reform Commission, *Surveillance in Public Places* (Final Report 18, May 2010) and New South Wales Law Reform Commission, *Invasion of Privacy* (Report 120, April 2009).

²⁴⁹⁶ Submission to the Discussion Paper: [Public Interest Advocacy Centre](#), 21.

²⁴⁹⁷ [ALRC Report 123](#), 119.

²⁴⁹⁸ Ibid; Submission to the Discussion Paper: [Ai Group](#), 23.

²⁴⁹⁹ [ALRC Report 123](#), 117-118.

²⁵⁰⁰ Ibid 124.

²⁵⁰¹ Ibid 110.

²⁵⁰² Submission to the Discussion Paper: [Dr Jelena Gligorijević](#), [ANU College of Law](#), 3.

²⁵⁰³ Submission to the Discussion Paper: [Dr Anna Bunn](#), 1-2.

²⁵⁰⁴ [ALRC Report 123](#), 87-88.

A broad range of other submitters argued that a minimalist tort would result in decades of uncertainty with consequential privacy, business and legal costs.²⁵⁰⁵

27.3.2 Extending the Act to individuals

Two industry submitters considered that the Act should be extended to individuals as per Option 3 of the Discussion Paper as the preferred way of addressing any gap in the law.²⁵⁰⁶ Professor Graham Greenleaf submitted that Option 3 could be introduced in addition to the ALRC statutory tort to enable intimate image abuse and similar misuse of personal information to be addressed under the Act.²⁵⁰⁷ This would provide greater options for a victim including making a complaint to the OAIC or applying to the courts under the direct right of action (see Chapter 26) rather than litigating a tort.

The *Online Safety Act* regulates intimate image abuse and certain other types of conduct which may involve misuse of personal information in online contexts. Extending the Privacy Act into this area runs the risk of increasing complexity for individuals seeking redress in relation to this type of conduct. It may be appropriate to consider the feasibility of a mechanism to enable individuals to seek compensation against perpetrators as part of the eSafety framework to achieve a less fragmented approach.

27.3.3 Damages for emotional distress for equitable breach of confidence

Damages for emotional distress were recognised by the Victorian Court of Appeal in *Giller v Procopets*.²⁵⁰⁸ The ALRC in Report 123 proposed this option in 2014 as an alternative in the event a tort of privacy was not enacted.²⁵⁰⁹ No submitters to the Discussion Paper preferred this option. Submitters who opposed a statutory tort also opposed states and territories legislating that damages for emotional distress should be available for equitable breach of confidence.²⁵¹⁰

Michael Douglas, a senior lecturer at UWA, noted that courts in various jurisdictions had already followed or cited *Giller v Procopets* favourably in equitable breach of confidence cases.²⁵¹¹ It is considered unnecessary for this report to propose that state and territory legislatures enact relevant provisions where the common law is already developing in that direction and, for some states a suitable case may simply not yet have come before the courts.

27.4 Balancing freedom of expression

Media industry submitters were opposed to all options for a statutory tort on the basis that it would have a detrimental or 'chilling' effect on freedom of expression and journalism in Australia.²⁵¹² The Guardian Australia and SBS considered that the privacy benefits of a tort for invasions of privacy would be outweighed by the detriment of negative consequences for transparency and accountability.²⁵¹³ The Guardian Australia also considered that the cost of pursuing litigation is significant and out of reach for many Australians, the tort may therefore likely benefit only a small number of high profile individuals, and pointed to high profile litigation in other jurisdictions.²⁵¹⁴

2505 Submissions to the Discussion Paper: [elevenM](#), 72; [Federal Chamber of Automotive Industries](#), 31; [Michael Douglas, UWA Law School](#), 5; [DIGI](#), 28-29; [Prof Barbara McDonald and Prof David Rolph, University of Sydney](#), 3; [Insurance Council of Australia](#), 18-19.

2506 Submissions to the Discussion Paper: [DIGI](#), 28-29; [Australian Collectors & Debt Buyers Association](#), 14.

2507 Submission to the Discussion Paper: [Graham Greenleaf, UNSW Sydney](#), 8.

2508 *Giller v Procopets* [2008] VSCA 236.

2509 [ALRC Report 123](#), 265, rec 13-1.

2510 Submissions to the Discussion Paper: [DIGI](#), 29; [Medical Insurance Group Australia](#), 12; [ABC](#), 12.

2511 Submission to the Discussion Paper: [Michael Douglas, UWA Law School](#), 5; *Wilson v Ferguson* [2015] WASC 15; *Champions Ride Days Pty Ltd v McFarlane* [2019] QDC 236 at [126].

2512 Submissions to the Discussion Paper: [Australia's Right to Know](#), 1; [Guardian Australia](#), 21; [SBS](#), 12-13; [Commercial Radio Australia](#), 3.

2513 Submissions to the Discussion Paper: [Guardian Australia](#), 21; [SBS](#), 12-13.

2514 Submission to the Discussion Paper: [Guardian Australia](#), 21.

However, the ALRC Report 123 model would expressly require a plaintiff to demonstrate to the satisfaction of a court that the public interest in privacy, in the circumstances of the case, outweigh any countervailing public interest.²⁵¹⁵ Such public interests were expressly considered to include freedom of the media, particularly to responsibly investigate and report matters of public concern and importance.²⁵¹⁶ As the ALRC pointed out, its model slightly preferences other public interests over the public interest in privacy as the test requires that privacy outweigh other interests. Where the public interests are balanced, the test is not met.²⁵¹⁷

Furthermore, the ALRC also recommended defences analogous to defamation defences. These defences would include 'fair report of proceedings of public concern' which the ALRC considered should be co-extensive with the defence in the Uniform Defamation Law.²⁵¹⁸

This means that under the ALRC statutory tort model, a plaintiff would need to prove that the public interest in privacy in their case outweighs the public interest of a particular invasion of privacy by the media done in the interests of transparency or freedom of expression. Further, if a plaintiff's claim did outweigh other public interests, a media defendant could plead a defence on the basis of fair reporting of proceedings of public concern. The protections for journalism in the ALRC model are extensive and any chilling effect on journalism is hoped to be minimal while media familiarise themselves with the content of the tort and the avenues to defend a claim and put a plaintiff to proof.

27.5 Information Commissioner as *amicus curiae*

The statutory tort's protection against 'misuses of private information' would not rely on the definition of 'personal information' in the Act. What is 'private information' for the purpose of the tort would be developed by courts. The Act may provide relevant context for the court when considering this aspect of the tort, but it would not determine the existence of a serious invasion of privacy.

However, because litigation involving the statutory tort may involve circumstances governed by the Act or personal information, the OAIC's submitted that it should be able to assist the court where appropriate.²⁵¹⁹ This submission has merit. The IC should be given the power to seek leave to appear as *amicus curiae* in court proceedings where proceedings have the potential to impact the evolution of the Act and privacy jurisprudence and policy.²⁵²⁰ This power to seek leave would be appropriately located in the *Australian Information Commissioner Act 2010* (Cth). While this reform has been prompted by the statutory tort, the power should not be limited to only such proceedings. This reform would complement the *amicus curiae* role proposed for the Direct Right of Action in Chapter 26.

27.6 Consultation with the States and Territories

A number of state inquiries have considered and recommended introducing a statutory tort. The NSW Standing Committee on Law and Justice and the South Australian Law Reform Institute have recommended enactment of statutory torts of privacy in recent years.²⁵²¹ The Qld Crime and Corruption Commission also recently recommended that a statutory tort for invasion of privacy be introduced.²⁵²² In South Australia, a statutory tort in the Civil Liability (Serious Invasions of Privacy) Bill 2021 was tabled in the South Australian Parliament for consideration in September 2021. The South Australian Bill was based on the 2016 SALRI report which proposed a very similar model to the ALRC Report 123.²⁵²³

²⁵¹⁵ ALRC Report 123, 144.

²⁵¹⁶ Ibid 150, rec 9-2.

²⁵¹⁷ Ibid 149.

²⁵¹⁸ Ibid 206.

²⁵¹⁹ Submission to the Issues Paper: OAIC, 134.

²⁵²⁰ Submission to the Issues Paper: OAIC, 135; Submission to the Discussion Paper: OAIC, 213.

²⁵²¹ Standing Committee on Law and Justice, Parliament of New South Wales, *Inquiry into remedies for the serious invasion of privacy in New South Wales* (Final Report, March 2016) rec 3; South Australian Law Reform Institute, *A statutory tort for invasion of privacy* (Final Report 4, March 2016) rec 1, 2.

²⁵²² Crime and Corruption Commission Queensland, *Operation Impala: Report on misuse of confidential information in the Queensland public sector* (February 2020) rec 17.

²⁵²³ South Australian Law Reform Institute, *A statutory tort for invasion of privacy* (Final Report 4, March 2016) 16.

The ALRC recommended that a statutory tort be enacted in a standalone Commonwealth Act rather than the Privacy Act in the interests of consistency throughout Australia.²⁵²⁴ A statutory tort for serious invasions of privacy would not be limited to APP entities or Commonwealth agencies. It would extend to individuals and state and territory agencies. The ALRC considered the tort would not infringe the implied limitation on the Commonwealth's power to legislate to impose a burden on the exercise of powers and function of the states. In view of the ALRC Report 123 model's defence of lawful authority, government agencies would be immune from liability where conduct is consistent with their statutory powers. The tort would therefore not place any greater burden on a state (or states) than on the Commonwealth itself.²⁵²⁵

An action in the statutory tort should also be able to be commenced in both federal and state and territory courts through cross-vesting of federal jurisdiction.²⁵²⁶ Courts may have variable associated litigation costs and variable jurisdictional limits to hear claims above certain amounts. The ALRC considered there would be considerable benefit for access to justice if these courts could hear privacy actions.²⁵²⁷ The plaintiff would be able to litigate their action in the most appropriate court having regard to the circumstances of their claim.

Consultation should be undertaken with the states and territories given the consideration and steps taken toward introducing statutory torts for invasions of privacy by the states, the need to ensure state agencies have the required lawful authorisations for activities which may be covered by the tort, and potential impacts on state and territory court resourcing.

27.1 Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123.

Consult with the states and territories on implementation to ensure a consistent national approach.

²⁵²⁴ [ALRC Report 123](#), 59.

²⁵²⁵ *Ibid* 67.

²⁵²⁶ *Ibid* 165.

²⁵²⁷ *Ibid* 166.

28. Notifiable data breaches scheme

Under the NDB scheme, organisations and agencies covered by the Act are required to report data breaches both to the OAIC and to the individuals affected by the data breach. The NDB scheme allows individuals whose personal information has been compromised in a data breach to take remedial steps to lessen the adverse impact that might arise from the breach. By arming individuals with the necessary information, they will have the opportunity to take corrective and preventative action to change or otherwise 'resecure' their personal information, such as monitoring their accounts, changing passwords and mobile numbers or cancelling credit cards.

The Discussion Paper sought feedback on the impact of the NDB scheme and whether it is operating effectively.

28.1 The NDB scheme

28.1.1 When notification obligations are triggered

Obligations under the NDB scheme are triggered once the entity is aware that there are reasonable grounds to suspect that there may have been an eligible data breach of the entity. In that event, an entity must conduct a reasonable and expeditious assessment. The notification obligations are triggered once the entity is aware that there are reasonable grounds to believe that there has been an eligible data breach.²⁵²⁸

The definition of 'eligible data breach' has two limbs.²⁵²⁹ These two limbs cover circumstances where there has been unauthorised access to, or unauthorised disclosure of, the information, or the information has been lost in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.²⁵³⁰ In both circumstances, an eligible data breach occurs if a reasonable person would conclude that the access or disclosure would be likely to result in 'serious harm' to any of the individuals to whom the information relates.²⁵³¹

28.1.2 Obligation to prepare a statement to the Commissioner

If an entity determines that an eligible data breach has occurred, it is required to provide a statement to the IC.²⁵³² The statement must set out:

1. the identity and contact details of the entity;
2. a description of the eligible data breach that the entity has reasonable grounds to believe has happened;
3. the kind or kinds of information concerned; and
4. recommendations about steps that individuals should take in response to the eligible data breach that the entity has reasonable grounds to believe has happened.²⁵³³

If the entity has reasonable grounds to believe that the eligible data breach is an eligible data breach of one or more other entities, the statement may also set out the identity and contact details of those other entities.²⁵³⁴

28.1.3 Notification obligations to persons affected by the data breach

After the entity has prepared this statement, the entity is required to notify the contents of the statement to persons affected by the data breach.²⁵³⁵ The contents of the statement notified to the affected individuals include recommended steps that individuals should take in response to the eligible data breach, in line with the purpose of the scheme to provide affected individuals with an opportunity to protect themselves from harm.²⁵³⁶

The IC can direct an entity to notify an eligible data breach if the IC is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity.²⁵³⁷

²⁵²⁸ Privacy Act ss 26WH(1), 26WK(1), 26WKL.

²⁵²⁹ Ibid s 26WE(2).

²⁵³⁰ Ibid.

²⁵³¹ Ibid.

²⁵³² Ibid s 26WK.

²⁵³³ Ibid s 26WK(3).

²⁵³⁴ Ibid s 26WK(4).

²⁵³⁵ Ibid s 26WL.

²⁵³⁶ Ibid s 26WL(2).

²⁵³⁷ Ibid s 26WR.

28.1.4 Recent changes to the NDB scheme

The Privacy Enforcement Act passed the Parliament on 28 November 2022 following several high-profile data breaches.²⁵³⁸ As part of the response to those breaches, the Privacy Enforcement Act introduced some initial reforms to improve the utility of the NDB scheme. Those reforms will:

- provide the IC with new powers to obtain information or documents in relation to an actual or suspected eligible data breaches – this will allow the IC to have a better understanding of the actual or suspected breach to assess the particular risk of harm to individuals;
- expand the IC's power to assess an entity's compliance with the Privacy Act to include notification of eligible data breaches – assessments are an important educative tool, and allow the IC to assess compliance in the absence of a breach of the Privacy Act or a complaint having been made; and
- require entities to set out the particular kind or kinds of information involved in an eligible data breach to ensure the IC has a comprehensive knowledge of the information compromised in a breach in order to assess the particular risk of harm to individuals, and whether the recommendations about the steps that individuals should take in response to the eligible breach outlined in a notification are sufficient.

28.2 Impact of the NDB scheme

The OAIC publishes statistical information about notifications received under the NDB scheme every six months. The Discussion Paper outlined some of the trends by industry and the type of breach. The healthcare and finance sectors account for the most notifications, with malicious and criminal attacks as the largest source of reported data breaches. The majority of these involved cyber incidents such as ransomware, phishing and compromised or stolen credentials. These trends continued in the most recent NDB reports covering the period from July to December 2021 and January to June 2022.²⁵³⁹ The number of data breaches reported has declined in the last reporting period with 464 breaches notified under the scheme in the July to December 2021 period and 396 in January to June 2022.²⁵⁴⁰

Contact information, identity information and financial details continue to be the most common types of personal information involved in data breaches. 84 per cent of breaches in the January to June 2022 period involved contact information, such as an individual's name, home address, phone number or email address. Identity information was exposed in 55 per cent of breaches and includes an individual's date of birth, passport details and driver licence details. Financial details, such as bank account and credit card numbers, were involved in 37 per cent of breaches.²⁵⁴¹

Submissions to the Discussion Paper indicated that the NDB scheme has raised awareness about the importance of effective data security and changed entities' data security practices. The OAIC said the scheme 'has been effective in meeting its key objectives of improving consumer protection, increasing accountability through transparency, and driving better security standards for the protection of personal information'.²⁵⁴² The Australian Government Social Services Portfolio said the scheme was 'vital in raising awareness of the importance of data security, promoting greater transparency and accountability in relation to data breaches, and in minimising harm to individuals affected by a data breach'.²⁵⁴³ The Australian Data and Insights Association said the scheme has worked to heighten awareness and prompt entities to 'establish procedures and preparations for NDB best practice'.²⁵⁴⁴

Some submitters indicated the scheme was achieving its policy rationale without imposing a significant compliance burden on entities. The Federal Chamber of Automotive Industries, for example, said it had not experienced any challenges with the operation of the scheme to date.²⁵⁴⁵ The Australian Collectors & Debt Buyers Association said no changes were necessary to the scheme as the balance between ensuring individuals and the OAIC were aware of data breaches and avoiding notification fatigue had been appropriately struck.²⁵⁴⁶

2538 Such as the Optus, Medibank and other cyber incidents of the same period.

2539 OAIC, [Notifiable Data Breaches Report: July to December 2021](#) (Report, 22 February 2022) 5; OAIC, [Notifiable data breaches report: January to June 2022](#) [Report, 10 November 2022] 3.

2540 OAIC, [Notifiable Data Breaches Report: July to December 2021](#) (Report, 22 February 2022) 5; OAIC, [Notifiable data breaches report: January to June 2022](#) [Report, 10 November 2022] 2.

2541 OAIC, [Notifiable data breaches report: January to June 2022](#) (Report, 10 November 2022) 9.

2542 Submission to the Discussion Paper: OAIC, 216.

2543 Submission to the Discussion Paper: [Social Services Portfolio](#), 33.

2544 Submission to the Discussion Paper: [Australian Data and Insights Association](#), 9.

2545 Submission to the Discussion Paper: [Federal Chamber of Automotive Industries](#), 32.

2546 Submission to the Discussion Paper: [Australian Collectors & Debt Buyers Association](#), 14.

Other submitters were more critical of the scheme. The Law Council of Australia noted that despite an increase in notifications since the NDB scheme was made mandatory in 2018, the rate of reports remains lower than countries subject to the GDPR.²⁵⁴⁷ However, the NDB scheme is not directly comparable to the GDPR scheme because the NDB scheme has a higher threshold of 'serious harm'. Fewer businesses are also generally required to comply with the scheme than overseas schemes due to the exemption for small businesses in Australia.

Some submitters said that although the NDB scheme had been effective at raising awareness following a data breach, more needs to be done to prevent data breaches from occurring. For instance, KPMG said the scheme has assisted breach detection and response, but that there needed to be more focus on the improvement of technical controls regarding breach prevention and protection.²⁵⁴⁸ Ai Group said the government could collaborate with industry to 'co-design workable and practical remedies to increase cyber security capability, such as technological solutions and education and training programs'.²⁵⁴⁹ The Australian Information Security Association said the OAIC should receive funding for more case studies and online learning modules with examples of the breaches that entities have experienced.²⁵⁵⁰

The OAIC noted that resources relevant to prevention are available on its website, including data breach prevention strategies for organisations, developed with the ACSC.²⁵⁵¹ The OAIC also has tailored educational and guidance activities with top reporting sectors, including a healthcare sector-specific guide and webinars developed with the Royal Australian College of General Practitioners and the Tax Practitioners Board.²⁵⁵²

28.3 Effectiveness of the NDB scheme

28.3.1 Harmonising with domestic schemes

The NDB scheme has encouraged mandatory data breach reporting schemes to be developed in other Australian jurisdictions. In NSW, a mandatory notification of data breach scheme applicable to the NSW public sector, which is consistent with the federal scheme, was passed on 16 November 2022.²⁵⁵³ The Queensland Department of Justice and Attorney-General released a Consultation Paper in June 2022 seeking feedback on whether a mandatory NDB scheme, based on the Commonwealth scheme, should be introduced in Queensland.²⁵⁵⁴

However, some submitters are concerned about the alignment of the NDB scheme with other existing and proposed mandatory data breach notification schemes in Australia.²⁵⁵⁵ These submitters referenced the obligations to notify cyber incidents under the *Security of Critical Infrastructure Act 2018* (SOCI Act) and the then Government's proposed mandatory ransomware reporting regime. The Australian Institute of Company Directors said that regulatory complexity presented a 'barrier to directors and organisations understanding existing obligations and building cyber resilience'.²⁵⁵⁶ The Information Technology Industry Council said it recognised that the various schemes may differ in scope or nature, but said the government should consider a single reporting agency and mechanism for all companies to avoid dual reporting.²⁵⁵⁷

A handful of submitters also expressed concern about the overlap between the NDB scheme and the data breach scheme in the *My Health Records Act 2012* (MHR Act). Avant Mutual said the requirements under the two schemes should be aligned.²⁵⁵⁸ Calabash Solutions said the MHR Act scheme should be aligned in favour of the NDB scheme to avoid unnecessary burden due to the broader scope of 'breach' under the former.²⁵⁵⁹

However, there would be challenges with aligning all obligations across the schemes. Specific schemes may require stricter requirements to address particular concerns, including sectoral-specific regulation. The NDB scheme applies to a variety of entities, data breaches and consequent harms, but only covers breaches involving personal information,

2547 Submission to the Discussion Paper: [Law Council of Australia](#), 21.

2548 Submission to the Discussion Paper: [KPMG](#), 33.

2549 Submission to the Discussion Paper: [Ai Group](#), 13.

2550 Submission to the Discussion Paper: [Australian Information Security Association](#), 6.

2551 Submission to the Discussion Paper: [OAIC](#), 217.

2552 Ibid.

2553 Privacy and Personal Information Protection Amendment Bill 2022 (NSW).

2554 Queensland Department of Justice and Attorney-General, [Proposed Changes to Queensland's Information Privacy and Right to Information Framework](#) (Consultation Paper, June 2022) 30.

2555 Submissions to the Discussion Paper: [Business Council of Australia](#), 8; [Information Technology Industry Council](#), 2.

2556 Submission to the Discussion Paper: [Australian Institute of Company Directors](#), 3.

2557 Submission to the Discussion Paper: [Information Technology Industry Council](#), 2.

2558 Submission to the Discussion Paper: [Avant Mutual](#), 21.

2559 Submission to the Discussion Paper: [Calabash Solutions](#), 27-8.

tax file number information and credit information. The MHR data breach scheme is narrower in scope with respect to the entities it covers, but adopts a lower data breach notification threshold than the NDB scheme because its objective is to ensure the security of the network-based MHR system, which connects multiple repositories containing primarily health information. The *Security of Critical Infrastructure Act 2018* SOCI Act scheme imposes short timeframes for reporting cyber incidents (including but not limited to data breaches) in recognition of the potentially immediate and severe downstream effects of compromised critical infrastructure assets, such as impacts on the energy sector.

There has been some effort to align domestic mandatory data breach notification schemes. Under the MHR Act, the IC receives data breach notifications (with the MHR System operator) and as such, eligible breaches do not need to be reported again under the NDB scheme.²⁵⁶⁰ The OAIC observed that although separate schemes are justified in certain circumstances, its general position is to encourage alignment of other domestic schemes with the NDB scheme where possible and particularly in the case of state and territory schemes.²⁵⁶¹ The OAIC also recommended that the NDB scheme should remain the baseline for privacy data breach reporting requirements at the federal level and any separate scheme should seek to increase, not replicate, those reporting requirements where warranted.²⁵⁶² Concerns about the need for further alignment of the Act more broadly with other domestic schemes are discussed further in Chapter 29.

There is also merit in exploring what could be done at a practical level to streamline reporting processes. For example, the OAIC has observed that some entities report data breaches to them in inconsistent ways, which can make it difficult to ensure that the entity has provided them with all the required information. Whilst the OAIC recommend that entities provide the information in a particular format, entities are not required to follow that template. This is different to obligations under the SOCI Act which requires entities to report using an approved form. There is benefit in keeping reporting schemes as consistent as possible and further work should be carried out on a practical level to devise ways to ensure breaches are reported correctly and those with multiple reporting obligations are not unnecessarily burdened.

28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.

28.3.2 Harmonising with international schemes

Submitters to the Discussion Paper also supported consistency with international jurisdictions.²⁵⁶³ The Tech Council of Australia said many Australian companies 'benchmark' themselves by reference to global and overseas standards in addition to the Privacy Act, including the GDPR and ISO 27701.²⁵⁶⁴

Calabash Solutions, on the other hand, said it did not support international harmonisation 'as not every APP entity is subject to or bound by international data scheme notification requirements'.²⁵⁶⁵ It cautioned against the pursuit of harmonisation to the point of increased regulatory burden. While the Governance Institute of Australia and Australian Institute of Company Directors supported the pursuit of GDPR adequacy, they similarly cautioned against imposing regulatory burden on Australian entities as a consequence of that pursuit.²⁵⁶⁶ Western Union said it had good insight into overseas data breach notification schemes due to its operation in almost all countries worldwide and noted it had 'not identified any serious concerns' with its approach of reviewing each data breach incident with a 'focussed review of the specific rules in the relevant jurisdictions'.²⁵⁶⁷

²⁵⁶⁰ *My Health Records Act 2012* [Cth] s 75.

²⁵⁶¹ Submission to the Discussion Paper: [OAIC](#), 217- 19 referencing its submission to the NSW Inquiry into Cybersecurity, which similarly advocated for national consistency across state or territory-based mandatory data breach notification schemes on the basis of alignment with the requirements of the NDB scheme under the Privacy Act: OAIC, [OAIC Submission to NSW Inquiry into Cybersecurity](#), (Web Page, 29 September 2020).

²⁵⁶² Submission to the Discussion Paper: [OAIC](#), 219.

²⁵⁶³ Submissions to the Discussion Paper: [Communications Alliance](#), 4; [BSA | The Software Alliance](#), 1; [Office of the Information Commissioner Queensland](#), 1; [Australian Institute of Company Directors](#), 2; [Governance Institute of Australia](#), 8; [Meta](#), 55.

²⁵⁶⁴ Submission to the Discussion Paper: [Tech Council of Australia](#), 3.

²⁵⁶⁵ Submission to the Discussion Paper: [Calabash Solutions](#), 27.

²⁵⁶⁶ Submission to the Discussion Paper: [Governance Institute of Australia](#), 4; [Australian Institute of Company Directors](#), 2.

²⁵⁶⁷ Submission to the Discussion Paper: [Western Union](#), 12.

Submitters identified that the key areas where the NDB scheme is different from international jurisdictions is the threshold for when a data breach must be notified²⁵⁶⁸ and the controller/processor distinction under the GDPR.²⁵⁶⁹ These issues are discussed further below.

28.3.3 Assigning responsibility for multi-party breaches

There is currently an obligation on all APP entities that hold personal information to notify in relation to an eligible data breach. Therefore, more than one entity can have notification obligations in relation to the same breach, although an entity is relieved of its obligation if another entity has already made a notification in relation to that data breach.²⁵⁷⁰

Some submitters considered that multi-party breaches continue to present a concern for businesses.²⁵⁷¹ For example, KPMG questioned the privacy benefits of the multiple notifications received by individuals and confusion that resulted from the data breach experienced by the online recruitment services organisation, PageUp, which impacted several entities.²⁵⁷² Submitters proposed that one way to address the issue of multi-party breaches was to create a distinction between a data controller and data processor.²⁵⁷³ In contrast, Western Union said that although it agreed 'with the submissions which point out potential challenges with multi-party breaches... in practice this has not created any undue difficulty'.²⁵⁷⁴

28.3.4 The new controller/processor distinction

Proposal 22.1 recommends the introduction of the concepts of APP entity controllers and APP entity processors, which would extend to non-APP entities where they process information on behalf of an APP entity controller. This distinction would apply to the NDB scheme.

The distinction would operate so that only the controller would be responsible for notifying individuals affected by an eligible data breach. This aligns with existing OAIC guidance that the entity with the 'most direct relationship' with the individuals concerned should carry out the notification.²⁵⁷⁵

However, processors would continue to be required to prepare a statement on the breach and provide a copy of that statement to the IC, unless the breach has already been reported by the relevant controller (or another processor).²⁵⁷⁶ This recognises that the circumstances of the breach would determine which entity is best placed to assess the likelihood of serious harm and to set out the details required under section 26WK (or section 26WR). As such, it would continue to be the case that, if neither processor nor controller notifies the IC, both may be in breach of the scheme's requirements.

28.3.5 Ensuring timely assessment and notification

If an entity has reasonable grounds to believe (and not merely suspect) that there has been an eligible data breach, then they must notify the IC and affected individuals under sections 26WK and 26WL 'as soon as practicable'. Entities should be particularly mindful of the speed and ease with which comprised information can be shared and misused by malicious actors.

If the entity has reasonable grounds to suspect (but does not yet believe) that there has been an eligible data breach, it must conduct an expeditious assessment to determine whether there are reasonable grounds to believe there has been an eligible data breach. The entity must take all reasonable steps to complete that assessment within 30 days.²⁵⁷⁷

2568 Submission to the Discussion Paper: [Law Council of Australia](#), 21.

2569 Submission to the Discussion Paper: [BSA | The Software Alliance](#), 5.

2570 Privacy Act ss 26WE(1)(a), 26WJ and 26WM.

2571 Submissions to the Discussion Paper: [Communications Alliance](#), 13; [BSA | The Software Alliance](#), 5; [KPMG](#), 33; [Atlassian](#), 4; [Australian Information Industry Association](#), 7; [Microsoft](#), 2; [Australian Retail Credit Association](#), 3; [Tech Council of Australia](#), 3; [Business Council of Australia](#), 8; [Information Technology Industry Council](#), 2.

2572 Submission to the Discussion Paper: [KPMG](#), 33.

2573 Submissions to the Discussion Paper: [Australian Retail Credit Association](#), 12-13; [Communications Alliance](#), 13; [BSA | The Software Alliance](#), 4-5; [Atlassian](#), 4; [Microsoft](#), 2; [Tech Council of Australia](#), 4.

2574 Submission to the Discussion Paper: [Western Union](#), 12.

2575 OAIC, [Notifiable Data Breach Scheme Guide](#) [Web Page, July 2019].

2576 Privacy Act s 26WK, 26WR.

2577 Privacy Act s26WH.

This is not a default 30-day period for conducting assessments. The OAIC Guidance states that the IC expects that 30 days be treated as a maximum time limit for completing an assessment, and entities should endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time.²⁵⁷⁸ An entity may be in non-compliance with the scheme if it moves too slowly in carrying out an assessment.

The Discussion Paper noted that, in the first half of 2021, 72 per cent of breaches were notified to the OAIC within 30 days of the entity suspecting an eligible data breach. This included the time taken to assess the breach as being eligible for notification. The remaining quarter of breaches were notified after 30 days, with approximately 15 per cent of breaches being notified more than 60 days after the entity became aware of the breach. 27 breaches were notified after 120 days. In the July-December 2021 Report, the number of notifications that took longer than 30 days reduced to 25 per cent.²⁵⁷⁹ In the January to June 2022, this figure increased to 29 per cent of notifications occurring past 30 days. Four entities took more than 12 months from when they became aware of an incident to notify the OAIC.²⁵⁸⁰ Some entities notified individuals at the same time as notifying the OAIC or shortly after. However some entities delayed notifying individuals.

A few submitters to the Discussion Paper supported maintaining the scheme's flexible 'as soon as practicable' requirement for notifying the OAIC and affected individuals of an eligible data breach once they become aware of the breach. The Australian Information Industry Association said 'as soon as practicable' need not be replaced with a specific timeframe as the risk of reputational harm associated with failing to report in a timely manner should alone sufficiently deter delayed notification.²⁵⁸¹ It said 'as soon as practicable' struck the right balance between prompt reporting and 'obtaining sufficient information to better ensure the notification is meaningful and not misleading to the affected individual'.²⁵⁸²

The Australian Government Social Services Portfolio noted that the imposition of rigid timeframes, while perhaps useful for certain types of breaches where individuals are at risk of serious financial or physical harm, could have the unintended effect of undermining reporting because the timeframes may fail to account for the 'type of incident, mitigations taken and to facilitate a trauma informed approach to notification'.²⁵⁸³ Privacy 108 said more attention should be paid to the industries failing to report in a timely manner.²⁵⁸⁴ It also expressed concern that, in the 'absence of comprehensive guidance and support' about the scheme's requirements, many entities have engaged law firms and consultancies 'with mixed results'.²⁵⁸⁵

Western Union similarly supported 'as soon as practicable' over the GDPR's 72-hour timeframe (for notifying the relevant supervisory authority) because it allows for 'more sophisticated and useful reporting'.²⁵⁸⁶ The GDPR notification period contains a specific notice period of 72 hours for notifying the regulator but allows for additional time where information is not available within the time frame. It states that notification should occur to the supervisory authority 'without undue delay, and where feasible, not later than 72 hours after having become aware of it'.²⁵⁸⁷ Further, the GDPR specifies that 'where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay'²⁵⁸⁸ to allow for circumstances where the information required is not immediately available. The communication of a personal data breach to the data subject is then to be done 'without undue delay', which does not contain a specified timeframe.²⁵⁸⁹

In addition to entities currently having some flexibility to determine *when* to notify affected individuals, the scheme also provides entities with three options for *how* to notify individuals. Subsections 26WL(2)(a) and (b) require entities, where practicable, to either notify each of the individuals to whom the relevant breached information relates, or each of the individuals at risk of serious harm from the breach. If neither option applies, the entity is required to take reasonable steps to publish the breach statement on its website and publicise the statement. However, entities should

2578 OAIC, [Notifiable Data Breach Scheme Guide](#) (Web Page, July 2019).

2579 OAIC, [Notifiable Data Breaches Report: July to December 2021](#) (Report, 22 February 2022).

2580 OAIC, [Notifiable data breaches report: January to June 2022](#) (Report, 10 November 2022) 2.

2581 Submission to the Discussion Paper: [Australian Information Industry Association](#), 7.

2582 Ibid.

2583 Submission to the Discussion Paper: [Social Services Portfolio](#), 34.

2584 Submission to the Discussion Paper: [Privacy 108](#), 49.

2585 Ibid, 50.

2586 Submission to the Discussion Paper: [Western Union](#), 12.

2587 GDPR art 33.

2588 Ibid art 33(4).

2589 Ibid art 34.

take care not to undermine the broader rationale of the scheme by pursuing tailored notification at the expense of timely reporting.²⁵⁹⁰ The failure to notify individuals in a timely manner may put them at greater risk of serious harm, particularly as, for example, the threat of identity theft and other such crimes increases the longer that individuals are prevented from taking steps to protect themselves.

It is clear that in light of recent large-scale breaches, community expectation is that individuals will be notified quickly if their personal information has been compromised. A notification to the OAIC should take place *within* 72 hours (with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours) and then a further notification as soon as practicable to the individuals to whom the information relates. A requirement to notify the OAIC within 72 hours of being aware of there being reasonable grounds to believe that there has been an eligible data would align with the requirement under the SOCI Act to notify the ACSC of a cyber security incident.

To further assist an entity to act quickly in the event of a data breach, entities should have a data breach response plan. Although entities may already be required to do this under APP 1 and APP 11, an express provision to this effect in the NDB provisions would provide certainty and ensure that entities proactively plan for how they would respond to a breach, including how they would notify individuals. These proposed requirements would set definitive timeframes and requirements on entities in the event of a breach which would provide greater certainty for APP entities and Australians whose data has been affected. Where applicable, entities would be able to notify relevant regulators under the Privacy Act and SOCI Act at the same time (see above).

28.2

- **Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours.**
- **Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable.**
- **Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.**

28.3.6 Revisiting the serious harm threshold

Of the small number of submissions received on the scheme's 'serious harm' threshold, Microsoft and the Australian Information Industry Association both said the threshold should not be lowered in favour of more breach reports, expressing concern about notification fatigue.²⁵⁹¹ The OAIC agreed with this position, on the basis that the current threshold avoids causing unnecessary distress to individuals who are not at risk, limits notification fatigue and reduces the administrative cost for regulated entities.²⁵⁹²

²⁵⁹⁰ Submission to the Discussion Paper: [OAIC](#), 220.

²⁵⁹¹ Submission to the Discussion Paper: [Microsoft](#), 8; [Australian Information Industry Association](#), 7.

²⁵⁹² Submission to the Issues Paper: [OAIC](#), 221.

The UNSW Allens Hub, Deakin CSRI and IEEE SSIT joint submission took a different view, saying that the threshold did not reflect the expectation of the public who are concerned with breaches of privacy (and not only 'serious harm'). The submission said the threshold should be replaced with a reverse onus requirement to notify 'unless the entity can demonstrate that the risk of harm to an individual and their rights is low'.²⁵⁹³ They said this would allow the scheme to acknowledge situations where an entity underestimates the potential harm to an individual due to a lack of information about the individual's life, such as the threat of intimate partner violence, or where the entity is not aware of other information that may compound the risk to individuals, such as the potential to re-identify otherwise de-identified publicly available information.²⁵⁹⁴

One submitter called for further guidance.²⁵⁹⁵ Professor Swinson said that, in the context of advising entities about their obligations under the scheme, it was not unusual for there to be reasonably differing views on whether a breach was likely to result in serious harm.²⁵⁹⁶ Unlike the UNSW Allens Hub, Deakin CSRI and IEEE SSIT joint submission, Professor Swinson said this confusion could be resulting in overly cautious notification and that, in the absence of case law or other precedent, further guidance would be welcome.²⁵⁹⁷

The current 'serious harm' threshold was developed to avoid the risk of notification fatigue to individuals and to not impose an unreasonable compliance burden on entities. The threshold was devised as an objective test to flexibly suit a variety of data breaches and to avoid the complexity associated with defining every form of harm likely to result from a breach.

An NDB scheme requiring serious harm is flexible enough to extend to breaches which involve less than personal information. A data breach of unidentified or de-identified information which relates to an individual could be subject to the scheme if the breach introduces the information into a new context which risks identification, and the sensitivity of the information when identified means there is a likelihood of serious harm. The identification of an individual as a result of a breach will mean that personal information will have been disclosed (see Chapter 4).

The onus is on the relevant entity to make an assessment of serious harm from the perspective of a reasonable person's position in their circumstances. The entity that experienced the breach would be best-placed to make such an assessment.

While it might not be possible to know with certainty that a data breach will in fact result in serious harm, it is expected that entities will err on the side of caution and notify unless they can demonstrate, for example, that the information subject to an eligible data breach was encrypted and therefore the likelihood of harm was low.²⁵⁹⁸ Section 26WG addresses encryption and other 'relevant matters' to help entities appropriately assess when notification is (or is not) required. The relevant matters also include consideration of the kind and sensitivity of the personal information concerned, which encourages entities to undertake notification where particularly sensitive forms of information are subject to a data breach. The list takes a technology neutral approach but also ensures consistency in that certain important factors will necessarily be considered during assessment.

Addressing the impact of breaches on individuals and mitigating harm

Approximately half of the submissions on the NDB scheme commented on proposal 27.1, which was to 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.

The purpose of the proposal is to ensure that individuals have as much relevant information, including the steps already taken by the relevant entity on their behalf, to protect themselves from the likelihood of serious harm caused by a data breach. For example, it would benefit an at-risk individual to know that the entity has arranged identity document replacement services, or contacted the relevant government agencies about the unauthorised disclosure of their tax file²⁵⁹⁹ or Medicare numbers.²⁶⁰⁰ The entity may also have frozen the individual's accounts, or forced a password reset.

²⁵⁹³ Submission to the Discussion Paper: [UNSW Allens Hub, Deakin CSRI and IEEE SSIT](#), 10.

²⁵⁹⁴ Ibid.

²⁵⁹⁵ Submission to the Discussion Paper: [Social Services Portfolio](#), 34.

²⁵⁹⁶ Submission to the Discussion Paper: [Professor John V Swinson](#), 10.

²⁵⁹⁷ Ibid.

²⁵⁹⁸ Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 78-80; Privacy Act s 26WG(h).

²⁵⁹⁹ The Privacy (Tax File Number) Rule 2015 (Cth) regulates the collection, storage, use, disclosure, security and disposal of an individual's tax file number information

²⁶⁰⁰ Where such disclosures are permitted. See further OAIC, [Notifiable Data Breach Scheme Guide](#) (Web Page, July 2019).

Submitters who commented on this proposal were largely in support of it.²⁶⁰¹ The OAIC said the proposal will 'promote greater transparency and accountability by requiring entities to notify individuals of the steps they have taken or intend to take in response to the breach'.²⁶⁰² The Law Council of Australia said it was 'consistent with the current requirements that a statement about an eligible data breach provides recommendations as to the steps an individual must take in the circumstances'.²⁶⁰³ Some industry representatives also supported the proposal as being feasible and practical.²⁶⁰⁴ CPA Australia said the proposal was reasonable despite its compliance burden because it would 'enhance transparency and public accountability'.²⁶⁰⁵

A handful of submitters opposed the proposal in its entirety. The Australian Information Industry Association said the requirement to set out steps taken in response to an eligible data breach would be 'overly prescriptive' and that existing OAIC guidance should suffice.²⁶⁰⁶

Some submitters were concerned that including detailed information in the statement to the OAIC or in the notice to persons who are at risk from the data breach raised the further risk that commercially sensitive, security or personal information would be released.²⁶⁰⁷ Meta supported the proposal provided 'there will be no requirement to include any confidential information in the notice, or anything else that may compromise any information security procedures that the reporting entity may have in place'.²⁶⁰⁸ The ABC made similar comments that entities should be 'exempt from any requirement to disclose information in relation to confidential cyber security systems or processes, or that could be used to compromise ongoing cyber security'.²⁶⁰⁹ Equifax said the broadness of the proposal should be reconsidered lest it inadvertently mandate the notification of information that 'fraudsters' could use to subvert an entity's 'methods of identifying future attempts to re-access, or exploit, an affected individual's information'.²⁶¹⁰ Equifax said entities should only be required to provide descriptions of action taken to assist affected individuals rather than of preventative methods, which 'may involve having to reveal information about an entity's systems that the notifying entity would not want made public'.²⁶¹¹

There are already existing exceptions under the NDB scheme where entities are not required to notify the OAIC or individuals. These exceptions recognise the balance between the need for transparency with other matters in the public interest. The IC has a broad power under section 26WQ to grant exemptions from the requirement to prepare a statement and notify in certain circumstances, such as while a law enforcement investigation is underway or where the harm in notifying an individual may outweigh the likely harm associated with the breach itself. In granting such a deferral, the IC must be satisfied that it is reasonable in the circumstances and have regard to the public interest. The exemption can be granted either at the IC's own initiative or upon application by the entity.

The proposal would also enable entities to determine the level of detail they include in their statements and notices about the steps they have taken in response to the breach, provided they comply with the essence of the requirement. As is currently the case, there would be no obligation, for instance, to include the personal information of individuals.

The Privacy Enforcement Act has clarified that when an entity prepares a statement for the IC following an eligible data breach under sections 26WK or 26WR, it must include information about the *particular* kind or kinds of information as opposed to just the kind or kinds of information.

In light of the number of recent large-scale data breaches, there is also a question about whether the NDB scheme should go further than what is contemplated in this proposal. The Australian Privacy Foundation said the proposal did not go far enough to address concerns around harm mitigation.²⁶¹² 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 (based on the model under section 36(1) of the DAT Act.²⁶¹³ Some entities are already taking responsibility for the costs and impacts of data breaches and supporting individuals, including by paying for a credit monitoring

2601 Submissions to the Discussion Paper: [OAIC](#), 221; [Calabash Solutions](#), 27; [Michael Douglas](#), 5; [Australian Information Security Association](#), 6; [DIGI](#), 29; [Australian Communications Consumer Action Network](#), 21; [CPA Australia](#), 6; [Social Services Portfolio](#), 34; [Federal Chamber of Automotive Industries](#), 32; [Australian Institute of Health and Welfare](#), 10; [Australian Department of Health](#), 18; [FinTech Australia](#), 17; [Tech Council of Australia](#), 5; [Law Council of Australia](#), 21.

2602 Submission to the Discussion Paper: [OAIC](#), 221.

2603 Submission to the Discussion Paper: [Law Council of Australia](#), 21.

2604 Submissions to the Discussion Paper: [Tech Council of Australia](#), 5; [Federal Chamber of Automotive Industries](#), 32.

2605 Submission to the Discussion Paper: [CPA Australia](#), 6.

2606 Submission to the Discussion Paper: [Australian Information Industry Association](#), 5.

2607 Submissions to the Discussion Paper: [Meta](#), 10; [ABC](#), 12; [Equifax](#), 17-18.

2608 Submission to the Discussion Paper: [Meta](#), 10.

2609 Submission to the Discussion Paper: [ABC](#), 12.

2610 Submission to the Discussion Paper: [Equifax](#), 18.

2611 Ibid.

2612 Submission to the Discussion Paper: [Australian Privacy Foundation](#), 19.

2613 Submission to the Issues Paper: [OAIC](#), 144.

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.

If there was a requirement for entities to take proactive action to mitigate the harm to impacted individuals of the breach, then this would be an extension of the current principle underpinning the scheme, which is that entities should swiftly report breaches so that individuals can take steps to protect themselves. Some entities could perceive this requirement as a pecuniary penalty, particularly if they had taken reasonable steps to protect the personal information and complied with the relevant APPs, but despite this, the personal information was maliciously accessed. The requirement could discourage some entities from reporting the data breach. However, this requirement would align more closely with community expectations that entities need to take at least some responsibility for supporting individuals, particularly during a large-scale breach of the personal information they hold, and could further encourage entities to comply with the APPs under the Act. Given the complexity of this proposed requirement, there would be benefit in considering it further.

28.3 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.

However, this proposal would not require the entity to reveal personal information, or where the harm in providing this information would outweigh the benefit in providing this information.

Consider further a requirement that entities should take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.

28.4 Necessary information sharing after a data breach

The current provisions in the NDB scheme are heavily focussed on the initial reporting and notification of the breach. However, in light of the large scale data breaches that occurred following the release of the Discussion Paper,²⁶¹⁴ there is a question about whether the scheme needs to do more to facilitate the response to a breach.

As part of the Government's response to a large scale data breach of a telecommunications company in late 2022, the Minister for Communications urgently put in place temporary amendments to the *Telecommunications Regulations 2021* to allow telecommunications companies, the financial services sector and relevant Government agencies to work together more effectively, to implement enhanced monitoring and safeguards to protect individuals affected by the breach.²⁶¹⁵

The amendments enable telecommunications companies to temporarily share approved government identifier information (such as driver licence, Medicare and passport numbers of affected customers) with regulated financial services entities to allow them to implement enhanced monitoring and safeguards for customers affected by the data breach. In addition, the amendment enables telecommunications companies to share identifiers to assist Australian Government and State and Territory agencies, to detect and assist in preventing fraud. The regulations have strong privacy and security safeguards to ensure that only limited information can be made available for certain purposes.

²⁶¹⁴ Such as the Optus, Medibank and other cyber incidents of the same period.

²⁶¹⁵ *Telecommunications Amendment (Disclosure of Information for the Purpose of Cyber Security) Regulations 2022* (Cth).

For example, only specified information can be disclosed, and only for the sole purposes of preventing or responding to cyber security incidents, fraud, scam activity or identity theft. Without the amendments to the regulations, telecommunications companies would not be able to safely and securely disclose information to financial institutions and government agencies because there are otherwise strict prohibitions on telecommunications companies from disclosing subscriber information. It is noted that the Australian Government Digital Identity System which enables individuals to prove their identity safely and securely and removes the need for retention of identification documents²⁶¹⁶ would reduce the need for considerable information sharing amongst government bodies.

However, had the breach not related to a telecommunications company, there may have been no immediate way to legally facilitate this information sharing to assist individuals affected. Similar to the emergency declaration provisions that exist under Part VIA of the Act, and discussed in Chapter 5, there would be benefit in providing greater flexibility under the Act to permit the sharing of personal information in limited circumstances to respond to a significant data breach. A new provision could enable the Attorney-General to make a declaration that would enable the sharing of personal information with appropriate entities if doing so would reduce the risk of harm to impacted individuals in the event of an eligible data breach. The provision would need to contain appropriate safeguards including a high threshold for when such a declaration could be made, limits on which entities the information could be provided to and for designated purposes, and a time limit on how long the declaration could be in force.

28.4 Introduce a provision in the Privacy Act to enable the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach. The provision would contain safeguards to ensure that only limited information could be made available for designated purposes, and for a time limited duration.

²⁶¹⁶ Digital Transformation Agency, [About Digital Identity](#) (Web Page).

29. Interactions with other schemes

The Discussion Paper sought feedback on proposals to deal with the interaction between the Act and other Commonwealth schemes that contain privacy protections, between Commonwealth regulators in enforcing matters involving the mishandling of personal information, and with state and territory privacy legislation.

29.1 Interaction between the Act and other Commonwealth schemes

The purpose of the Act is to provide consistent baseline protections for personal information.²⁶¹⁷ While the Act legislates minimum requirements for APP entities, other Commonwealth legislation can authorise the handling of personal information in ways that are different to the APPs. Generally, these separate privacy provisions include specific information handling practices to address clear risks and concerns.²⁶¹⁸ For example, the My Health Records (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.²⁶¹⁹

The Act is one piece of legislation in a broader digital and data regulatory framework.²⁶²⁰ Telstra noted that there is an increasing number of privacy related legislation at the Commonwealth level.²⁶²¹ Submitters raised particular concerns about the interaction between the Act and recent data sharing schemes, such as the DAT Act and the CDR under the *Competition and Consumer Act 2010*. One submitter noted that separate rules under the DAT Act and the CDR increase complexity and compliance costs for APP entities.²⁶²²

Disparate information handling rules can also impact an individual's understanding of how their personal information will be used and disclosed. The Public Interest Advocacy Centre noted that the DAT Act significantly expands the possible use and disclosure of an individual's personal information and in ways that could not reasonably be envisaged by an individual when providing their consent to the initial collection.²⁶²³ Submitters also expressed concerns that the CDR allows disclosures to unaccredited trusted advisers that may not be covered by the Act.²⁶²⁴ Ai Group suggested that the CDR has created a dual regulatory regime with oversight from the OAIC and ACCC, increasing compliance costs for business.²⁶²⁵ However, the OAIC noted that both regulators have published a joint compliance and enforcement policy to provide transparency and certainty to the community.²⁶²⁶

Submitters provided general support for alignment and simplification of privacy and other information related legislation,²⁶²⁷ noting that harmonisation of Commonwealth legislation would assist APP entities to adhere with legislative requirements, reduce the regulatory burden and limit transaction costs.²⁶²⁸

To address concerns raised by submitters regarding inconsistency and overlap between Commonwealth privacy law frameworks, the Discussion Paper proposed the Attorney-General's Department develop a privacy law design guide. This guide would support Commonwealth agencies and legislative drafters when developing new schemes with privacy-related obligations. 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,²⁶²⁹ how additional protections should be drafted, and relevant oversight and enforcement mechanisms recommended to apply to such schemes. Where alternative and additional information handling practices are required, the law design guide would aim to encourage consistency between separate schemes. An example of this type of guide is the Attorney-General's Department's existing Guide to Framing Commonwealth Offences, Infringement Notice and Enforcement Powers, and the New Zealand Legislation Guidelines.²⁶³⁰ Such guides are policyneutral but are intended to guide departments and parliamentary committees on the creation of consistent legislation.

²⁶¹⁷ Submission to the Discussion Paper: [OAIC](#), 222.

²⁶¹⁸ Ibid.

²⁶¹⁹ Submissions to the Issues Paper: [Australian Digital Health Agency](#), 2. See also re credit reporting, [Legal Aid Queensland](#), 17–8.

²⁶²⁰ Submission to the Discussion Paper: [Tech Council of Australia](#), 5.

²⁶²¹ Submission to the Discussion Paper: [Telstra](#), 29.

²⁶²² Submission to the Discussion Paper: [elevenM](#), 17.

²⁶²³ Submission to the Discussion Paper: [Public Interest Advocacy Centre](#), 25.

²⁶²⁴ Submission to the Discussion Paper: [UNSW Allens Hub](#), [Deakin CSRI and IEEE SSIT](#), 6.

²⁶²⁵ Submission to the Discussion Paper: [Ai Group](#), 15–16.

²⁶²⁶ Submission to the Discussion Paper: [OAIC](#), 226.

²⁶²⁷ Submission to the Discussion Paper: [Western Union](#), 13.

²⁶²⁸ Submissions to the Discussion Paper: [Telstra](#), 29; [Western Union](#), 13; Atlassian, p. 2;

²⁶²⁹ See Submission to the Issues Paper: [Legal Aid Queensland](#), 17–8.

²⁶³⁰ Attorney-General's Department, [Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers](#) (9 January 2013); New Zealand Legislation Design and Advisory Committee, [Legislation Guidelines: 2018 Edition](#), (Report, 2018).

There was support for addressing the interaction between the Act and other Commonwealth schemes through the proposed law design guide.²⁶³¹ The Department of Health and Aged Care noted the benefits of increasing awareness of privacy best practice, particularly with Commonwealth agencies tasked with progressing policy and legislation.²⁶³² Telstra suggested that the law design guide place reliance on the APPs where possible, and, suggested different levels of privacy protections should not be created for information already covered by other schemes.²⁶³³

However, the Australian Institute for Health and Welfare noted that a law design guide may only help deal with future inconsistency. It considered a review of existing overlaps and inconsistencies would be beneficial to address existing discrepancies.²⁶³⁴ Optus noted any introduction of new privacy legislation following this Review without the concurrent removal of 'out-of-date and duplicative' sector specific regulation would increase the regulatory burden on APP entities.²⁶³⁵

Other suggestions to remedy inconsistency included placing more reliance on codes under the Act,²⁶³⁶ and OAIC guidance setting out how the Act interacts with other schemes in greater detail.²⁶³⁷ These suggestions acknowledge the importance of clear and transparent legislation, and appropriate guidance to support individuals and entities to understand their rights and obligations.

29.1.1 Proposal – Develop a privacy law design guide

A law design guide would help ensure best practice and reduce inconsistency and overlap between Commonwealth privacy law frameworks into the future. It would acknowledge the role of the Act in providing baseline protections, and provide guidance on when more tailored protections may be needed to address specific policy objectives.

The guide would be a good first step to providing a more structured framework for considering the privacy legislative landscape. Once developed, it would be open for there to be further consideration about whether there would be benefit in reviewing existing legislative schemes to achieve greater harmonisation.

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

29.2 Interactions between the OAIC and other regulators

The intersection between privacy and digital technologies has seen enforcement action in relation to personal information handling practices by regulators other than the OAIC.

The Discussion Paper set out the overlapping issues in data protection, competition and consumer protection. 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. In August 2022, the Federal Court ordered Google to pay \$60 million in penalties for making misleading representations to consumers about the collection and use of their personal location data on Android phones between January 2017 and December 2018, following court action by the ACCC.²⁶³⁸

2631 Submissions to the Discussion Paper: [OAIC](#), 225; [Australian Privacy Foundation](#), 19; [Internet Association of Australia](#), 4; [Department of Health](#), 18.

2632 Submission to the Discussion Paper: [Department of Health](#), 18.

2633 Submission to the Discussion Paper: [Telstra](#), 30.

2634 Submission to the Discussion Paper: [Australian Institute of Health and Welfare](#), 10.

2635 Submission to the Discussion Paper: [Optus](#), 5.

2636 Submission to the Discussion Paper: [OAIC](#), 223.

2637 Submission to the Discussion Paper: [Public Interest Advocacy Centre](#), 25.

2638 ACCC, [Google LLC to pay \\$60 million for misleading representations](#) (Web Page, 12 August 2022); [Australian Competition and Consumer Commission v Google LLC \(No 4\)](#) [2022] FCA 942.

Some of the proposals in this Review will continue to intersect with consumer law. For example, the ACCC's *Digital platforms services inquiry* recommended a general prohibition on unfair trading practices.²⁶³⁹ This prohibition will extend to personal information handling, such as harmful and excessive tracking, collection and use of data.²⁶⁴⁰ These practices would also be captured by the proposed fair and reasonable test (Chapter 12) and proposals to regulate targeted advertising (Chapter 20).

The Discussion Paper proposed that Commonwealth regulators should continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information. Following the release of the Discussion Paper, more work has been done by regulators to facilitate cooperation. In March 2022, the ACMA, the ACCC, the OAIC, and the Office of the e-Safety Commissioner formed the Digital Platform Regulators Forum (DP-Reg). The DP-Reg provides a forum for regulators to share information about, and collaborate on, cross-cutting issues and activities on the regulation of digital platforms, including privacy and data issues.²⁶⁴¹

A number of submissions were supportive of continued cooperation between Commonwealth regulators.²⁶⁴² Submitters provided support for tailored and sector specific regulation. Free TV Australia supported ACMA's regulatory oversight of the Commercial Television Industry Code of Practice.²⁶⁴³ The Commercial Television Industry Code of Practice includes privacy obligations, such as requiring consent or material to be in the public interest before material relating to a person's personal or private affairs or which invades a person's privacy can be broadcast.²⁶⁴⁴ Free TV Australia suggested that ACMA are the appropriate regulator for these privacy protections as they oversee other aspects of broadcasting regulation, and have experience in the relevant public policy considerations.²⁶⁴⁵

However, Ai Group noted that overlap was an inefficient use of government resources, and that there was merit in considering establishing a central regulatory body to coordinate between the existing Commonwealth government regulators.²⁶⁴⁶ Ai Group provided anecdotal evidence of 'double dipping' between regulators where individuals who were unsatisfied with a Telecommunications Industry Ombudsman decision would then file a complaint with the OAIC.²⁶⁴⁷ Similarly, Optus noted that, where possible, regulators should minimise duplicative or overlapping inquiries, and exercising enforcement powers for the same breach.²⁶⁴⁸ Optus suggested this could be done through memoranda of understanding (MoUs) which set out roles and responsibilities of regulators.²⁶⁴⁹ However, the OAIC has already entered into a number of MoUs with other regulators, including ACMA, ADHA, IGIS and ACCC.²⁶⁵⁰

29.2.1 Proposal – Continue to encourage regulatory cooperation

Current methods for collaboration between Commonwealth regulators are commendable, and the OAIC is playing an active role in facilitating regulatory cooperation between Commonwealth regulators. There is merit in the OAIC and other Commonwealth regulators continuing to work collaboratively to ensure enforcement action is brought under the most appropriate framework, lowering the risk of duplicative investigations.

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

²⁶³⁹ ACCC, *Digital platform services inquiry interim report No. 5 – Regulatory reform* (Report, September 2022) 64.

²⁶⁴⁰ Ibid 65.

²⁶⁴¹ ACMA, *Digital Platform Regulators Forum (DP-Reg)* (Web Page, 26 September 2022).

²⁶⁴² Submission to the Discussion Paper: [Australian Privacy Foundation](#), 19; [OAIC](#), 227; [Australian Institute of Company Directors](#).

²⁶⁴³ Submission to the Discussion Paper: [Free TV Australia](#), 3.

²⁶⁴⁴ ACMA, *Commercial television industry code of practice* (2015).

²⁶⁴⁵ Submission to the Discussion Paper: [Free TV Australia](#), 3.

²⁶⁴⁶ Submission to the Discussion Paper: [Ai Group](#), 17.

²⁶⁴⁷ Submission to the Discussion Paper: [Ai Group](#), 17.

²⁶⁴⁸ Submission to the Discussion Paper: [Optus](#), 38.

²⁶⁴⁹ Submission to the Discussion Paper: [Optus](#), 39.

²⁶⁵⁰ Full list of MOUs can be found at OAIC, [MOUs](#) (Web Page, 2022).

29.3 Interaction with state and territory privacy legislation

The Act does not generally cover local, state or territory government agencies. Most Australian states and territories have legislation which covers their public sector agencies. However, it is not always equivalent. The Discussion Paper proposed to establish a Commonwealth, state and territory working group to harmonise privacy legislation, focussing on key issues.

Submissions provided broad support for this proposal,²⁶⁵¹ noting that harmonisation could reduce the compliance burden on APP entities operating in multiple Australian jurisdictions,²⁶⁵² such as contactors who work to both Commonwealth, and state and territory governments.²⁶⁵³ The OAIC noted that there would be benefit in ensuring that the privacy protections in states and territories laws are commensurate with those under the Act, such as mandatory data breach notification requirements.²⁶⁵⁴

29.3.1 Health information

The Act applies to all private sector health service providers anywhere in Australia. It does not apply to state and territory public sector health service providers, such as public hospitals.

Submissions provided strong support for the proposed working group to focus on treatment of health information.²⁶⁵⁵ This is particularly important given the increase in telehealth services following the COVID-19 pandemic.²⁶⁵⁶

Health privacy legislation is complex. However, it is also an area where harmonisation may have the greatest benefit to individuals due to the risk of harm and discrimination if health information is disclosed without authorisation.²⁶⁵⁷ Some proposed focus areas included the classification of genomic information,²⁶⁵⁸ coverage of the deceased,²⁶⁵⁹ and the interaction between genomic information and deceased individuals or at-risk relatives.²⁶⁶⁰ Relatedly, Commonwealth, state and territory governments are currently undergoing a consultation process about access to social media accounts and digital records upon death or incapacity.²⁶⁶¹

There were also concerns raised about each Australian jurisdiction having separate legislation for mental health.²⁶⁶² It was noted that this can complicate treatment, particularly for people who may have need to seek mental health care across jurisdictions and families who may live in other jurisdictions to the person they care about.²⁶⁶³

29.3.2 Contractors

Another key issue raised was the treatment of contractors. Submitters noted there are gaps in coverage between contractors that work for both Commonwealth, and state and territory governments. Specifically, concerns were raised about subsection 7B(5) of the Act under which contractors under state or territory contracts are exempt from the APPs to the extent of that contract, even if there is no relevant state or territory privacy legislation that applies.²⁶⁶⁴ Salinger Privacy noted that this meant contractors may sometimes be bound by the Act, sometimes by state or territory privacy principles (either directly or via contract), and sometimes by no privacy legislation at all.²⁶⁶⁵

2651 Submissions to the Discussion Paper: [OAIC](#), 227-8; [Western Union](#), 13; [Atlassian](#), 1; [Australian Privacy Foundation](#), 19; [Avant Mutual](#), 21; [Australian Information Industry Association](#), 7; [Salinger Privacy](#), 47; [Department of Health](#), 18; [Australian Institute of Health and Welfare](#), 11; [Australia Research Data Commons](#), 2; [Australian Retail Credit Association](#), 14; [Justice Connect](#), 7; [Research Australia](#), 4; [Lived Experience Australia](#), 5; [The Benevolent Society](#), 7; [Medical Software Industry Association](#), 4-5; [Population Health Research Network](#), p. 5.

2652 Submissions to the Discussion Paper: [Western Union](#), 13; [Australian Institute of Health and Welfare](#), 11; [Australian Information Industry Association](#), 7; [Justice Connect](#), 7.

2653 Submission to the Discussion Paper: [Australian Information Industry Association](#), 7.

2654 Submission to the Discussion Paper: [OAIC](#), 218.

2655 Submissions to the Discussion Paper: [Australia Research Data Commons](#), 2-3; [Research Australia](#), 4; [Medical Software Industry Association](#), 4; [Royal Australian and New Zealand College of Psychiatrists](#), 4.

2656 Submission to the Discussion Paper: [Royal Australian and New Zealand College of Psychiatrists](#), 4.

2657 Submission to the Discussion Paper: [Research Australia](#), 4.

2658 Submission to the Discussion Paper: [Department of Health](#), 18.

2659 Submission to the Discussion Paper: [Avant Mutual](#), 21.

2660 Submission to the Discussion Paper: [Department of Health](#), 18.

2661 Attorney-General's Department, [Standing Council of Attorneys-General communique](#) (Web Page, 9 December 2022).

2662 Submission to the Discussion Paper: [Lived Experience Australia](#), 5.

2663 Submission to the Discussion Paper: [Lived Experience Australia](#), 5.

2664 Submission to the Discussion Paper: [Salinger Privacy](#), 47.

2665 Submission to the Discussion Paper: [Salinger Privacy](#), 48.

29.3.3 Proposal – Establish a Commonwealth, state and territory working group

The development of digital technologies requires all Australian jurisdictions to seek to continually improve their privacy legislation. Commonwealth, state and territory governments are increasingly working together on national initiatives that involve sharing information across jurisdictions.²⁶⁶⁶

Subject to the agreement of States and Territories, proceeding with the recommendation for a Commonwealth, state and territory government working group would provide a forum to focus on aligning privacy legislation in areas of key concern, such as the handling of health information and contractors. As suggested in Proposal 21.6, the working group could also review and consider alignment of Australian law that requires entities to retain personal information. The working group would not seek to achieve complete uniformity, and could initially focus on ensuring there are agreed principles for any federal, state or territory laws that purport to address privacy issues. However, a model for longer-term harmonisation could be considered by the working group.

Existing national structures, such as the Standing Council of Attorneys-General, could provide a framework under which the working group could be established. There would also need to be appropriate consultation with those entities who would be affected by harmonisation.

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

²⁶⁶⁶ Submission to the Discussion Paper: [OAIC](#), 218.

30. Further review

The proposals in this Report, if implemented, would amount to significant reforms to Australia's privacy framework. It would be judicious to ensure that the operation and effectiveness of the reforms are evaluated after the provisions have been in effect for an appropriate period of time. This would ensure the continued effectiveness of Australia's privacy framework in the future, and enable further consultation on the impact and effectiveness of the changes. Accordingly, a statutory review should commence within three years of the commencement of the amendments to the Act which implement the proposals put forward in this Review.

30.1 Conduct a statutory review of any amendments to the Act which implement the proposals in this Report within three years of the date of commencement of those amendments.

Attachment A – Consultation

Consultation process

The Review commenced in October 2020 with the release of Terms of Reference and an Issues Paper. The Issues Paper outlined the current provisions of the Act and sought feedback on areas for potential reform. The department received 200 written submissions in response to the Issues Paper. Consent was obtained to publish 166 submissions on the department's website.

A Discussion Paper was released in October 2021. The Discussion Paper put forward 67 proposals designed to elicit feedback and ideas. The department received 235 submissions in response to the Discussion Paper. Consent was obtained to publish 207 submissions on the department's website.

Between October 2020 and November 2022, 162 consultation meetings took place with 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. These meetings included meetings with stakeholders on specific issues and stakeholder consultation roundtables.

Further detail on stakeholder consultation roundtables convened by the Review is set out below.

Stakeholder consultation roundtables

Roundtable	Date of consultation
Academics and children's privacy advocates	19 November 2021
Australian Government Commissioners: Information Commissioner, eSafety Commissioner, National Children's Commissioner and Disability Discrimination Commissioner	23 November 2021
Academics, research centres and civil society	24 November 2021, 2 December 2021, 3 December 2021, 8 December 2021, 13 December 2021
Social media platforms	25 November 2021
Technology companies and data brokers	29 November 2021, 30 November 2021
Media organisations	1 December 2021
General industry	9 December 2021, 15 December 2021
Finance, banking and insurance sector	10 December 2021
Medical and research sector	16 December 2021
Government research agencies	1 April 2022
Children and young people (organised by Reset Australia)	18 January 2022, 20 January 2022, 27 January 2022
Small business representatives	30 March 2021, 4 February 2022
Employer representatives	8 February 2022
Employee representatives	9 February 2022
Industry: CBPR and domestic privacy certification	23 March 2022

* The stakeholder roundtables with technology companies, data brokers and social media platforms were convened in relation to the lapsed Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (OP Bill). However, the feedback obtained was considered by the Review.

Issues Paper submissions published

1.	ABC	42.	Business Council of Australia
2.	ACCC	43.	Calabash Solutions
3.	Adobe	44.	Castan Centre for Human Rights Law – Monash University
4.	AGL Energy Limited	45.	Centre for AI and Digital Ethics and Melbourne Law School, University of Melbourne
5.	Ai Group	46.	Centre for Cyber Security Research and Innovation
6.	Anonymous submission 1	47.	Centre for Media Transition, University of Technology Sydney
7.	Anonymous submission 2	48.	CHOICE
8.	Anonymous submission 3	49.	Clubs Australia
9.	Anonymous submission 4	50.	Commercial Radio Australia Limited
10.	Anonymous submission 5	51.	Communications Alliance
11.	Anonymous submission 6	52.	Consumer Policy Research Centre
12.	ANZ	53.	CrowdStrike
13.	Arts Law Centre of Australia	54.	CSIRO
14.	Association for data-driven marketing and advertising	55.	Cyber Security Cooperative Research Centre
15.	Assured Support	56.	Data Republic
16.	Atlassian	57.	Data Synergies
17.	auDA	58.	Database Consultants Australia
18.	AusPayNet	59.	Deloitte
19.	Australia's Right to Know Coalition (ARTK)	60.	Department of Health of Western Australia
20.	Australian Association of National Advertisers	61.	Department of Justice and Community Safety, Victoria
21.	Australian Banking Association	62.	Department of Veterans' Affairs
22.	Australian Chamber of Commerce and Industry (ACCI)	63.	DIGI
23.	Australian Communications and Media Authority (ACMA)	64.	Digital Rights Watch
24.	Australian Communications Consumer Action Network	65.	Digital Rights Watch – Joint comments with Access Now, Centre for Responsible Technology Australia, Fastmail, Reset Australia
25.	Australian Council on Children and the Media	66.	Dr Caitlin Curtis, Prof Nicole Gillespie and Dr Steve Lockey (University of Queensland)
26.	Australian Department of Health	67.	Dr Chris Culnane and Associate Professor Ben Rubinstein
27.	Australian Digital Health Agency	68.	Dr Jelena Gligorijevic
28.	Australian Finance Industry Association	69.	Dr John Zerilli
29.	Australian Financial Markets Association	70.	Dr Kate Mathews Hunt
30.	Australian Information Security Association	71.	Dr Katharine Kemp
31.	Australian Institute of Health and Welfare	72.	Dr Kerin Robinson
32.	Australian Medical Association	73.	Dr Kimberlee Weatherall
33.	Australian Privacy Foundation	74.	Electronic Frontiers Australia
34.	Australian Retail Credit Association	75.	elevenM
35.	Australian Small Business and Family Enterprise Ombudsman	76.	Energy and Water Ombudsman, New South Wales
36.	Australian Society of Archivists	77.	Experian
37.	Avant Mutual	78.	Facebook
38.	Benevolent Society	79.	Fastmail
39.	Bennett + Co	80.	Federal Chamber of Automotive Industries
40.	Blanco	81.	Felix Harvey
41.	BSA The Software Alliance		

82. Financial Planning Association of Australia
83. Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia
84. Financial Services Council
85. Fintech Australia
86. FreeTV Australia
87. Fundraising Institute Australia
88. Gadens
89. Global Data Alliance
90. Google
91. Griffith University
92. Ground Up
93. HIV AIDS Legal Centre
94. Humanising Machine Intelligence Project, Australian National University
95. ID Exchange
96. IDCARE
97. illion
98. Information Technology Industry Council
99. Institute for Cyber Investigations and Forensics, University of the Sunshine Coast
100. Insurance Council of Australia
101. Integral GRC Pty Ltd
102. Interactive Games and Entertainment Association (IGEA)
103. James Scheibner (Department of Health Sciences and Technology ETH Zurich) and Dianne Nicol (Centre for Law and Genetics Faculty of Law University of Tasmania)
104. Karen Meohas
105. KPMG
106. Law Council of Australia
107. Law Institute of Victoria
108. Legal Aid New South Wales
109. Legal Aid Queensland
110. Lockstep Consulting
111. Maurice Blackburn
112. McAfee
113. Medical Insurance Group Australia (MIGA)
114. Michael Douglas, University of Western Australia Law School
115. Microsoft Australia
116. Minderoo Tech and Policy Lab, University of Western Australia Law School
117. Murdoch Children's Research Institute
118. MyCRA Lawyers
119. National Archives of Australia
120. National Health and Medical Research Council
121. New South Wales Council for Civil Liberties
122. New South Wales Information and Privacy Commission
123. New York Times
124. Nine
125. Obesity Policy Coalition
126. Office of the Australian Information Commissioner
127. Office of the Information Commissioner Queensland
128. Office of the Victorian Information Commissioner
129. Openly Australia
130. Optus
131. Oracle
132. Palo Alto Networks
133. Privacy 108
134. Privcore
135. Public Interest Advocacy Centre
136. Queensland Council for Civil Liberties
137. Queensland Law Society
138. Queensland University of Technology Faculty of Law
139. Ramsay Australia
140. Records and Information Management Professionals of Australasia
141. Reset Australia
142. Rights in Records by Design (Monash University)
143. Roche
144. Roxanne Quinlan
145. Royal Australian College of General Practitioners
146. Salesforce
147. Salinger Privacy
148. SBS
149. Shaun Chung and Rohan Shukla
150. Shogun Cybersecurity
151. Shopping Centre Council of Australia
152. Snap Inc.
153. Superchoice
154. Telecommunications Industry Ombudsman Ltd
155. Telstra Corporation Ltd and Telstra Health Pty Ltd
156. The Allens Hub for Technology, Law and Innovation
157. The Guardian Australia
158. The Painter and The Writer Gallery
159. United States Chamber of Commerce
160. Uniting Church of Australia
161. University of Technology Sydney, Faculty of Engineering and IT
162. Vanessa Teague
163. Western Union
164. William Delaforce
165. Woolworths
166. Workday

Discussion Paper submissions published

167.	ABC	204.	Australian Federal Police (AFP)
168.	Access Now	205.	Australian Financial Markets Association
169.	ACT The App Association	206.	Australian Genomics
170.	ACTU	207.	Australian Information Industry Association
171.	Ai Group	208.	Australian Information Security Association
172.	Amazon Web Services	209.	Australian Institute of Company Directors
173.	Anna Bunn	210.	Australian Institute of Health and Welfare
174.	Anonymous submission 1	211.	Australian Medical Association
175.	Anonymous submission 10	212.	Australian Nuclear Science and Technology Organisation, ANSTO
176.	Anonymous submission 11	213.	Australian Privacy Foundation
177.	Anonymous submission 12	214.	Australian Research Data Commons (ARDC)
178.	Anonymous submission 2	215.	Australian Retail Credit Association
179.	Anonymous submission 3	216.	Australian Services Roundtable
180.	Anonymous submission 4	217.	Australian Society of Archivists
181.	Anonymous submission 5	218.	Australian Super
182.	Anonymous submission 6	219.	Australia-New Zealand Chapter, Association of Professional Genealogists
183.	Anonymous submission 7	220.	Australia's Right to Know (ARTK)
184.	Anonymous submission 8	221.	Avant Mutual
185.	Anonymous submission 9	222.	BSA The Software Alliance
186.	ANZ	223.	Business Council of Australia
187.	Association for Data-driven Marketing & Advertising (ADMA)	224.	Calabash Solutions
188.	Association of Australian Medical Research Institutes (AAMRI)	225.	CARE Australia
189.	Association of Heads of Independent Schools Australia	226.	Castan Centre for Human Rights Law and the Centre for Commercial Law and Regulatory Studies, Monash University (Castan Centre)
190.	AssuranceLab Pty Ltd	227.	Centre for Artificial Intelligence and Digital Ethics (Melbourne University)
191.	Atlassian	228.	Centre for Media Transition
192.	AusPayNet	229.	Certis Security Australia
193.	Australian Association Of National Advertisers (AANA)	230.	Chartered Accountants ANZ
194.	Australian Banking Association	231.	CHOICE
195.	Australian Banking Association, Consumer Action Law Centre, Financial Rights Legal Centre, Economic Abuse Reference Group, COTA Australia, WEstjustice	232.	Civic Data
196.	Australian Chamber of Commerce and Industry (ACCI)	233.	Clubs Australia
197.	Australian Collectors & Debt Buyers Association	234.	Commercial Radio Australia
198.	Australian Communications Consumer Action Network	235.	Commissioner for Children and Young People
199.	Australian Competition and Consumer Commission (ACCC)	236.	Commonwealth Bank of Australia
200.	Australian Computer Society (ACS)	237.	Communications Alliance Ltd
201.	Australian Council on Children and the Media	238.	Consumer Action Law Centre
202.	Australian Data and Insights Association (ADIA)	239.	Consumer Policy Research Centre
203.	Australian Digital Health Agency	240.	CPA Australia
		241.	CrowdStrike
		242.	CSIRO
		243.	Deloitte Australia
		244.	Department of Health
		245.	Department of Health - Western Australia
		246.	DIGI
		247.	Digital Law Association

248.	Digital Rights Watch	292.	IoT Alliance Australia (IoTAA)
249.	Dr Ben Egliston, Lucinda Nelson and Dr Marcus Carter	293.	Justice Connect
250.	Dr Henry Fraser	294.	KarlsGate
251.	Dr Jelena Gligorijevic, ANU College of Law	295.	Kimberlee Weatherall, Tom Manousaridis, Melanie Trezise
252.	Dr Katharine Kemp, UNSW Sydney	296.	KPMG
253.	Education Services Australia	297.	Law Council of Australia
254.	Electrical Trades Union of Australia	298.	Lisa Eckstein (Eckstein et al)
255.	Electronic Frontiers Australia	299.	Lived Experience Australia
256.	elevenM	300.	Marcelo Ulvert ; Malcolm Treanor
257.	Emin Hasic	301.	Mark Nottingham
258.	Energy & Water Ombudsman NSW (EWON)	302.	Mark Thomson
259.	Energy and Water Ombudsman (Victoria)	303.	Medical Insurance Group Australia (MIGA)
260.	Energy and Water Ombudsman Queensland	304.	Medical Software Industry Association Ltd
261.	Energy and Water Ombudsman SA	305.	Megan Richardson
262.	Equifax	306.	Meta
263.	European Commission	307.	Michael Douglas, UWA Law School
264.	Experian Australia	308.	Microsoft
265.	Federal Chamber of Automotive Industries	309.	Minderoo Tech & Policy Lab, UWA Law School
266.	Financial Rights Legal Centre and Financial Counselling Australia	310.	Murdoch Children's Research Institute
267.	Financial Services Council	311.	National Archives of Australia
268.	FinTech Australia	312.	National Australia Bank
269.	Foundation for Alcohol Research and Education	313.	National Health and Medical Research Council
270.	Free TV Australia	314.	Niall Gillmor, Ben Clapin, Vukasin Sokic, Myles Allen, and Thea Harpley Green
271.	Fundraising Institute Australia and Public Fundraising Regulatory Association	315.	Nine
272.	Garvan Institute of Medical Research and Garvan Research Foundation	316.	NSW Council for Civil Liberties
273.	Geoffrey Stafford	317.	Obesity Policy Coalition
274.	Geoscience Australia	318.	Office of the Australian Information Commissioner
275.	Global Data Alliance	319.	Office of the Information Commissioner Queensland
276.	Google	320.	Office of the Victorian Information Commissioner
277.	Governance Institute of Australia	321.	Optus
278.	Graham Greenleaf, UNSW Sydney	322.	Paul Salanitri
279.	Guardian Australia	323.	Peter Holland
280.	Heart Research Australia	324.	Peter Kovesi
281.	Helen Gregorczyk, University of Queensland	325.	Peter Leonard, Data Synergies
282.	Housing Industry Association Ltd	326.	Pharmaceutical Society of Australia
283.	IIS Partners & Ground Up Consulting	327.	Phil Eckert
284.	IKEA Australia	328.	Population Health Research Network
285.	Illion	329.	Privacy 108
286.	Information Technology Industry Council	330.	Privcore
287.	Insurance Council of Australia	331.	Prof Barbara McDonald and Prof David Rolph, University of Sydney
288.	Interactive Advertising Bureau (IAB)	332.	Professor David Lindsay
289.	Interactive Games & Entertainment Association (IGEA)	333.	Professor John V Swinson
290.	International Fund for Animal Welfare (IFAW) Australia	334.	Public Health Association of Australia
291.	Internet Association of Australia	335.	Public Interest Advocacy Centre

336.	QUT Digital Media Research Centre	357.	Telecommunications Industry Ombudsman
337.	Ramsay Health Care Australia	358.	Telstra
338.	Research Australia	359.	The Australia Institute – Centre for Responsible Technology
339.	Reset Australia	360.	The Australian Communications and Media Authority (ACMA)
340.	ResMed	361.	The Benevolent Society
341.	Retail Drinks Australia	362.	The Hon Bruce Billson, Australian Small Business and Family Enterprise Ombudsman
342.	Rob Lake	363.	Twilio
343.	Rob Marsh	364.	Uniting Church in Australia, Synod of Victoria and Tasmania
344.	Royal Australian and New Zealand College of Psychiatrists	365.	UNSW Allens Hub, Deakin CSRI and IEEE SSIT joint submission
345.	Russell Blackford	366.	UWA Law School Students: Sophie Archibald, Samantha Hopson, Sarah Jones, Gar-Hou Tran and Emma Young
346.	Salesforce	367.	Victor Chang Cardiac Research Institute
347.	Salinger Privacy	368.	Western Union
348.	Samantha Gavel, Information and Privacy Commission NSW	369.	Woolworths Group
349.	Services Australia	370.	Workday
350.	Shopping Centre Council of Australia	371.	World Animal Protection
351.	Snap Inc.	372.	Xero
352.	Social Services Portfolio	373.	yourtown
353.	Society Of Australian Genealogists		
354.	Special Broadcasting Service (SBS)		
355.	Sylvia Else		
356.	Tech Council of Australia		

Attachment B – 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 NDB 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.

