Australian Government

Attorney-General's Department

Privacy Act Review

Issues Paper

October 2020

Terms of Reference

Objective

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

Context

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

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

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

Matters to be considered by the review

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

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

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

Matters that will not be considered

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

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

Conduct and outcomes of the review

Consultation and evidence

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

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

Reviewer

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

Timing and outcomes

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

Foreword

The *Privacy Act 1988* (Privacy Act) is the primary Australian legislation that protects the privacy of individuals, and restricts how government and industry can collect, use and disclose individuals' personal information. In 2019, the Government made a commitment to conduct a review of the Privacy Act.

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

This review takes account of, and builds upon the Australian Competition and Consumer Commission's (ACCC's) *Digital Platforms Inquiry* final report ('DPI report').[1] The DPI report, published in July 2019, considered the impact of online platforms on advertising and the media, together with a number of related privacy issues from a consumer perspective. The DPI report proposed broad reform of the Privacy Act and several specific reforms.[2]

As part of the Government's response to the DPI Report, the Government agreed to consult on the following specific reforms which the Government supported in-principle, subject to consultation and design of specific measures:

- updating the definition of 'personal information' to capture technical data and other online identifiers (Recommendation 16(a))
- strengthening existing notification requirements (Recommendation 16(b))
- strengthening consent requirements and pro-consumer defaults (Recommendation 16(c)), and
- introducing a direct right of action to enforce privacy obligations under the Privacy Act (Recommendation 16(e)).[3]

The review will consider these issues, as well as other recommendations in the DPI report, including whether a statutory tort for serious invasions of privacy should be introduced, and whether the Privacy Act should include a 'right to erasure'[4]. The review will build on reforms announced by the Government in March 2019 to increase the maximum civil penalties under the Privacy Act and to develop a binding privacy code to apply to social media platforms and other online platforms that trade in personal information.[5]

In establishing this review of the Privacy Act, the Australian Government recognises that the issues raised in the DPI report apply beyond digital platforms. The digital economy is vital to Australia's economic growth and prosperity. The ability to communicate and transact with individuals online has led to rapid improvements in the provision of goods and services by businesses and government.

---

[1] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019).
[2] Ibid Recommendations 16-19.
[3] Department of the Treasury, *Regulating in the digital age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Government Response, December 2019).
[4] ACCC, *Digital Platforms Inquiry* (n 1) Recommendations 19 and 16(d).
[5] These reforms constitute the Government response to ACCC, *Digital Platforms Inquiry* (n 1) Recommendation 18.

New and emerging technologies present new opportunities to realise further benefits. To achieve these benefits, individuals must have trust and confidence that their privacy is respected and protected.

In light of these developments, the review will consider whether the scope of the Privacy Act and its enforcement mechanisms remain fit for purpose.

About the review

The review is being conducted by the Australian Attorney-General's Department.

This issues paper is the first of two papers seeking public input. This paper outlines the current law and seeks feedback on potential issues relevant to reform. A discussion paper will be released in early 2021, seeking more specific feedback on preliminary outcomes, including any possible options for reform.

Call for submissions

The Government invites submissions in response to the questions in this issues paper or any other matter relevant to the terms of reference.

We may publish your submission, unless you request for it to remain confidential, or if we consider (for any reason) that it should not be made public. We may redact parts of published submissions, as appropriate. Refer to our privacy policy to find out more.[6]

Submissions should be returned by **29 November 2020** to PrivacyActReview@ag.gov.au. For further information about the consultation process for this review, please visit **Review of the Privacy Act 1988**.

[6] Attorney-General's Department, *Privacy Policy* (Web Page, accessed 15 October 2020).

Table of Contents

Abbreviations

2020 ACAP survey	OAIC Australian Community Attitudes to Privacy Survey 2020
AAT	Administrative Appeals Tribunal
ABS	Australian Bureau of Statistics
ACCC	Australian Competition & Consumer Commission
ACMA	Australian Communications and Media Authority
ACT	Australian Capital Territory
ADHA	Australian Digital Health Agency
AFCA	Australian Financial Complaints Authority
AFP	Australian Federal Police
AHRC	Australian Human Rights Commission
ALRC	Australian Law Reform Commission
APEC	Asia-Pacific Economic Cooperation
APPs	Australian Privacy Principles
APRA	Australian Prudential Regulation Authority
Archives Act	*Archives Act 1983* (Cth)
ASIO	Australian Security Intelligence Organisation
CBPR	Cross-Border Privacy Rules
CCA	*Competition and Consumer Act 2010* (Cth)
CCPA	*California Consumer Privacy Act of 2018*
CDPP	Commonwealth Director of Public Prosecutions
CDR	Consumer Data Right
CIIs	Commissioner Initiated Investigations
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DPI report	ACCC Digital Platforms Inquiry: Final Report
DPI response	Government Response and Implementation Roadmap for the Digital Platforms Inquiry
EU	European Union
FOI Act	*Freedom of Information Act 1982* (Cth)
GDPR	*General Data Protection Regulation* (European Union)
ICCPR	International Covenant on Civil and Political Rights
IGIS	Inspector-General of Intelligence and Security
IMEI	International Mobile Equipment Identity
Commissioner	Information Commissioner
IoT	Internet of Things
IPP	Information Privacy Principles
IP address	Internet Protocol address
MAC address	Media Access Controller address
MOU	Memorandum of Understanding
NDB Scheme	Notifiable Data Breaches Scheme
NPP	National Privacy Principles
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Co-operation and Development
ONDC	Office of the National Data Commissioner
RIS	Regulation Impact Statement
Tel Act	*Telecommunications Act 1997* (Cth)
the Act	*Privacy Act 1988* (Cth)
TIA Act	*Telecommunications (Interception and Access) Act 1979* (Cth)
UN	United Nations

Complete list of questions for consideration

Objectives of the Privacy Act

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

Definition of personal information

2. What approaches should be considered to ensure the Act protects an appropriate range of technical information?
3. Should the definition of personal information be updated to expressly include inferred personal information?
4. Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?
5. Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?

Flexibility of the APPs in regulating and protecting privacy

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

Exemptions

Small business exemption

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

Employee records exemption

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

Political parties exemption

16. Should political acts and practices continue to be exempted from the operation of some or all of the APPs?

Journalism exemption

17. Does the journalism exemption appropriately balance freedom of the media to report on matters of public interest with individuals' interests in protecting their privacy?
18. Should the scope of organisations covered by the journalism exemption be altered?
19. Should any acts and practices of media organisations be covered by the operation of some or all of the APPs?

Notice of Collection of Personal Information

Improving awareness of relevant matters

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

Third party collections

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

Limiting information burden

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

Consent to collection and use and disclosure of personal information

Consent to collection, use and disclosure of personal information

26. Is consent an effective way for people to manage their personal information?
27. What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?

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

Exceptions to the requirement to obtain consent

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

Pro-consumer defaults

32. Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?

Obtaining consent from children

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

The role of consent for IoT devices and emerging technologies

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

Inferred sensitive information

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

Direct marketing

37. Does the Act strike the right balance between the use of personal information in relation to direct marketing? If not, how could protections for individuals be improved?

Withdrawal of consent

38. Should entities be required to refresh an individual's consent on a regular basis? If so, how would this best be achieved?
39. Should entities be required to expressly provide individuals with the option of withdrawing consent?
40. Should there be some acts or practices that are prohibited regardless of consent?

Emergency declarations

41. Is an emergency declaration appropriately framed to facilitate the sharing of information in response to an emergency or disaster and protect the privacy of individuals?

Regulating use and disclosure

42. Should reforms be considered to restrict uses and disclosures of personal information? If so, how should any reforms be balanced to ensure that they do not have an undue impact on the legitimate uses of personal information by entities?

Control and security of personal information

Security and retention

43. Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?
44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?

Access, quality and correction

45. Should amendments be made to the Act to enhance:
    a. transparency to individuals about what personal information is being collected and used by entities?
    b. the ability for personal information to be kept up to date or corrected?

Right to erasure

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

Overseas data flows and third party certification

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

Enforcement powers under the Privacy Act and role of the OAIC

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

Direct right of action

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

Statutory tort

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

Notifiable Data Breaches scheme – impact and effectiveness

63. Have entities' practices, including data security practices, changed due to the commencement of the NDB Scheme?
64. Has the NDB Scheme raised awareness about the importance of effective data security?
65. Have there been any challenges complying with the data breach notification requirements of other frameworks (including other domestic and international frameworks) in addition to the NDB Scheme?

Interaction between the Act and other regulatory schemes

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

Privacy in Australia

The *Privacy Act 1988* was enacted by the Australian Parliament as the primary piece of Commonwealth privacy law. The Privacy Act created a legal framework to regulate how Commonwealth departments and agencies handled personal information. The Privacy Act also reflects the Organisation for Economic Co-operation and Development (OECD) framework of data protection principles.[7]

The Privacy Act was drafted to be principles based and technologically neutral and supported by detailed regulatory guidance. This is demonstrated in the second reading speech of the then Attorney General, the Hon Lionel Bowen MP who stated that:

> *'the enormous developments in technology for the processing of information are providing new, and in some respects, undesirable opportunities for the greater use of personal information and that these developments have focused attention on the need for the regulation of the collection and use of personal information by government agencies.'*[8]

Until 2001, the Privacy Act only applied to Commonwealth departments and agencies. In 2000, the Australian Government passed the *Privacy Amendment (Private Sector) Act 2000* (Cth) which extended the application of the Privacy Act to the private sector. At the time of its introduction, the then Attorney General, the Hon Daryl Williams QC stated:

> *'The Privacy Amendment (Private Sector) Bill 2000 is the most significant development in the area of privacy law in Australia since the passage of the Privacy Act in 1988… For the first time, Australians can be confident that information held about them by private sector organisations will be stored, used and disclosed in a fair and appropriate way. For the first time, Australians will have a right to gain access to that information and a right to correct it if it is wrong.'*[9]

After the commencement of the *Privacy Amendment (Private Sector) Act 2000* (Cth), both Commonwealth Government departments and agencies and private sector organisations to whom the Act applied were subject to separate privacy principles.[10] This changed with the passage of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), when all entities covered by the Privacy Act became subject to a single set of privacy principles known as the Australian Privacy Principles (APPs).

The Privacy Act has been subject to numerous reviews which have influenced its development including the Australian Law Reform Commission's 'For Your Information, Australian Privacy Law and Practice Report 108' which resulted in the government passing the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth). Also, since the enactment of the Privacy Act, some states and territories have passed privacy laws that cover the management of personal information by entities not covered by the Privacy Act including state government agencies. Other regulatory frameworks

[7] Explanatory Memorandum, Privacy Bill 1988 (Cth) 2.
[8] Commonwealth, *Parliamentary Debates*, House of Representatives, 1 November 1988, 2117 (Lionel Bowen, Attorney-General).
[9] Commonwealth, *Parliamentary Debates*¸ House of Representatives, 12 April 2000, 15749 (Daryl Williams, Attorney-General).
[10] The Information Privacy Principles applied to Commonwealth departments and agencies and the National Privacy Principles applied to private sector organisations.

also have a role in protecting individuals' privacy, including the Consumer Data Right under the *Competition and Consumer Act 2010* (Cth) and the *Enhancing Online Safety Act 2015* (Cth).

A brief history of the Privacy Act is at **Appendix B**.

Australian attitudes to privacy

The results of the OAIC *Australian Community Attitudes to Privacy Survey 2020* (2020 ACAP survey) show that privacy is a major concern for 70 per cent of survey participants, with almost 9 in 10 respondents indicating they want more choice and control over their personal information.[11]

Data privacy was a top consideration for survey respondents when choosing a digital service ahead of reliability, convenience and price.[12] More than half of survey respondents reported experiencing a problem with how their data was used during the 12 months leading up to the survey, such as unwanted marketing communications, or personal information being collected when it was not required.[13] The results suggest Australians are increasingly questioning data practices where the purpose for collecting personal information is unclear, and that trust in organisations to protect personal information is declining.[14] 66 per cent of respondents to the Deloitte's Privacy Index 2020 had backed out of purchasing a product or using a service, or closed an account completely, due to privacy concerns in the past.[15]

[11] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020* (September 2020) 7.
[12] Ibid 51.
[13] Ibid 21.
[14] Ibid 7, 56.
[15] Deloitte *Opting-in to meaningful consent: Deloitte Australian Privacy Index 2020* (Report, June 2020).

Objects of the Act

Section 2A sets out the objects of the Act. These are:

- to promote the protection of the privacy of individuals;
- to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities;
- to provide the basis for nationally consistent regulation of privacy and the handling of personal information;
- to promote responsible and transparent handling of personal information by entities;
- to facilitate an efficient credit reporting system while ensuring that the privacy of individuals is respected;
- to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected;
- to provide a means for individuals to complain about an alleged interference with their privacy; and
- to implement Australia's international obligation in relation to privacy.[16]

The objects of the Act emphasise that the protection of privacy of individuals needs to be balanced against the interests of entities when carrying out their functions and activities.[17] However, the requirement to balance the protection of privacy with the interests of businesses can be difficult in the context of businesses whose core activity is acquiring and dealing in personal information.

The DPI report recognised that technological developments have led to data analytics becoming increasingly integrated into everyday business practices.[18] The ability to identify patterns in data sets, provide recommendations, and to predict the next best action relies on powerful processing platforms, and rich information sources.[19] This makes data, particularly personal information and the insights drawn from it, an important resource for a wide range of entities – not just digital platforms. Under the Act's objectives, the protection of individual privacy is required to be balanced against entities' functions and activities which may include these broad new functions and activities deployed for commercial interests.

Acknowledging this tension, the DPI report recommended that the Government consider whether the objectives of the Act should place a greater emphasis on privacy protections for consumers, to empower them to make informed choices.[20] Specifically, the DPI report recommended considering whether it remains appropriate for the objectives to require the protection of privacy to be balanced with the interests of business in carrying out their functions or activities.[21]

Questions

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

[16] *Privacy Act 1988* (Cth) ('Privacy Act') s 2A.
[17] Ibid s 2A(b).
[18] ACCC, *Digital Platforms Inquiry* (n 1) 87.
[19] International Banker, *Why data is the new commodity in the global economy* (Web Page, accessed 21 September 2020); The Economist, *Regulating the internet giants* (Web Page, accessed 21 September 2020).
[20] ACCC, *Digital Platforms Inquiry* (n 1) 439, 477.
[21] Ibid 477.

Scope and Application of the Privacy Act

Definition of personal information

The current Australian law

APP entities must comply with the requirements set out in the APPs in respect of personal information. Failure to do so may give an individual grounds to complain to the OAIC and to seek a remedy.[22]

Definition of personal information

Subsection 6(1) of the Act defines personal information to mean '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 material form or not'.

The Act also defines subsets of personal information, such as sensitive information and health information,[23] which are subject to additional protections.

Background to the definition

The definition of personal information is intended to be expansive. The Explanatory Memorandum to the Privacy Bill 1988 noted that the range of information or opinions that fall within the scope of the definition was 'infinite', and could include information about a person's physical description, residence, place of work, business and business activities, employment, occupation, investments, property holdings, relationship to other persons, recreational interests and political, philosophical or religious beliefs.[24]

In response to a recommendation in ALRC Report 108, the definition of personal information was amended in 2012.[25] This amendment substituted the requirement that personal information be about an individual whose 'identity is apparent, or can be reasonably ascertained,' for the phrase 'identified or reasonably identifiable.' The Explanatory Memorandum stated that whether an individual is reasonably identifiable must be 'based on factors which are relevant to the context and circumstances,'[26] and that the amendment was necessary 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.' This focus on 'identifiability' rather than 'identity' allows it to capture a broader range of information, including some online identifiers.

Guidance on the scope of "personal information"

The definition of personal information was considered by the Full Federal Court in *Privacy Commissioner v Telstra Corporation Ltd* (the Grubb case).[27] In the Grubb case, the issue was whether telecommunications metadata was personal information which Mr Grubb had a right to access under the Act. The Full Federal Court held that, in this case, it was not personal information on the

[22] Privacy Act (n 16) s 13.
[23] Ibid s 6FA.
[24] Explanatory Memorandum, Privacy Bill (n 7) 11-12.
[25] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).
[26] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 53.
[27] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4.

basis that it failed to satisfy the threshold question of whether the information was 'about' an individual.[28] Whether information is about an individual will depend on the facts of any individual case.[29] Some technical data may be about a device or service in the circumstances, rather than an individual. An implication of the Grubb case is that there are no set categories of technical data that ordinarily fall within the definition of 'personal information'.[30]

The APP Guidelines also provide advice on what is meant by the definition of personal information.[31] The Guidelines state that certain types of information will generally constitute personal information.[32] Where it is unclear whether an individual is reasonably identifiable, APP entities should take a cautious approach and treat the information as personal information.[33]

Whether an individual is 'reasonably identifiable' will depend on the context and the circumstances in which information is held, including the nature and amount of the information, who will hold and access it, and the other information available to that entity.[34] Information can also be characterised as joint personal information if it is about more than one 'reasonably identifiable' individual.[35]

The definition of 'personal information' does not include de-identified information, from which an individual is no longer reasonably identifiable,[36] information about households or groups of people, where no one person is reasonably identifiable, or information about deceased individuals (provided the information is not also about a living individual), because 'an individual' means a living, natural person.[37]

DPI report recommendations relating to personal information

The ACCC noted the 'considerable legal uncertainty on the issue of whether technical data collected in relation to individuals is within the scope of the definition of personal information'.[38] It also noted the position under EU law, under which technical data such as dynamic IP addresses clearly constitute personal information if they can be used to indirectly identify an individual when combined with other data.[39] In light of the advancements in data analytics technologies and the volume of technical data that is collected, used and shared in digital markets, the ACCC considered it

[28] Ibid [63]
[29] Ibid.
[30] Note that certain types of metadata must be treated as personal information in the context of Australia's metadata retention scheme: *Telecommunications (Interception and Access) Act* (Cth) s 187LA.
[31] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (July 2019) B.85-B.96.
[32] Such as an individual's name, signature, home address, email address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person: Ibid B.86.
[33] Ibid B.94.
[34] E.g. a common surname may not be personal information that would reasonably identify a particular individual, however combined with other information such as an address, it may be personal information: Ibid B.92.
[35] *Privacy Commissioner v Telstra Corporation Ltd* (n 28) [63]; See also Office of the Australian Information Commissioner, *What is personal information?* (Web Page, 5 May 2017).
[36] Privacy Act (n 16) s 6(1).
[37] OAIC, *Australian Privacy Principles Guidelines* (n 32) B.95.
[38] ACCC, *Digital Platforms Inquiry* (n 1) 458.
[39] Ibid 459; see also *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 ('General Data Protection Regulation'), art 30.

important to clarify that technical data relating to an identified individual is considered personal information within the scope of the Act.[40] Recommendation 16(a) proposed that:

> The definition of personal information in the Act be updated to clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual.[41]

The rationale for this recommendation is to ensure the definition is aligned with consumer expectations and reflects the realities of how data is used in digital markets.[42] The Government supported this recommendation in principle, subject to consultation and design of specific measures.[43]

The ACCC also recommended that broader reforms to the Act should have specific regard to:

- whether the Act should offer protection for inferred information, particularly where inferred information includes sensitive information, such as information about an individual's health, religious belief, or political affiliations.[44]
- whether there should be protections or standards for de-identification, anonymization and pseudonymisation of personal information to address the growing risk of re-identification as datasets are combined and data analytic technologies become more advanced.[45]

Key issues

Technical information

The application of the definition of personal information is unclear in relation to technical data and online identifiers. Online identifiers are informational traces that a person leaves when operating online that can be used to identify an account, a device, a browser or other behaviour. Examples of online identifiers can include files embedded on devices such as pixel tags and cookies and device fingerprints that record information about website access such as IP addresses. Lack of clarity regarding the application of the definition of personal information to these categories of information may increase the risk of APP entities breaching the Act and expose individuals to privacy risks.

It has been suggested that a clear, contemporary definition of personal information may be achieved by aligning it with the definition of personal information in the GDPR.[46] Article 4(1) of the GDPR stipulates that 'personal data means any information relating to an identified or identifiable natural person' and provides a non-exhaustive list of identifiers by which an identifiable natural person may be referenced. The DPI report noted that adoption of the GDPR definition could address challenges posed by the large scale processing of data and address the privacy risks associated with correlating technical information such as IP addresses and URLs with social media profiles.[47]

---

[40] ACCC, *Digital Platforms Inquiry* (n 1) 459.
[41] Ibid 458.
[42] Ibid 460.
[43] Department of the Treasury, *Regulating in the digital age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (n 3) 17.
[44] ACCC, *Digital Platforms Inquiry* (n 1) 476.
[45] Ibid 476.
[46] Office of the Australian Information Commissioner, Submission to Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (17 April 2018) 11.
[47] ACCC, *Digital Platforms Inquiry* (n 1) 460.

Inferred personal information

Inferred personal information is information collated from a number of sources which reveals something new about an individual.[48] For example, information collected about an individual's activity on digital platforms, such as interactions, purchases and 'likes' can be sold to data analytics companies if on-selling was included in the purposes for which consent was obtained or notice given, or if the information is de-identified. In the hands of the third party company, information may be combined with information from other sources, such as data from fitness trackers and other 'smart' devices. Together, this information can be aggregated to reveal information such as an individual's age, friendships, health or sexual orientation.[49] Inferred information can meet the definition of 'personal information' or 'sensitive information' even if it is inferred from de-identified information or technical data.

53 per cent of respondents to the 2020 ACAP survey were uncomfortable with a business combining data about its customers (for example, loyalty card transaction history) with other data (for example, IP address, type of browser used) to better profile their customers.[50] 48 per cent of respondents to a 2018 ACCC survey of digital platform users considered inferred tastes and preferences to be their personal information.[51] The results suggest Australians are split in their views about inferred personal information. APP entities may find it difficult to practically determine the point at which the inferences they generate become personal information – triggering notice and (in the case of sensitive information) consent requirements.[52]

De-identified, anonymous and pseudonymous information

Under APP 2, APP entities must give individuals the option of not identifying themselves, or the option to use a pseudonym, unless an exception applies. APP entities must also regularly consider how to de-identify personal information. For example, APP 11.2 requires APP entities to either destroy or de-identify any personal information they hold when it is no longer required for any purpose.[53]

Personal information will be 'de-identified' if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.[54] De-identified information may technically be able to be re-identified, but it will not be 'reasonably identifiable' if there is almost no likelihood of identification occurring.[55] Common de-identification processes include deleting or masking identifiers within data, such as names, and suppressing or generalising other information which may identify someone.

If information is not reasonably identifiable, APP entities can retain the information and are not constrained by the APPs in how they deal with it, provided they manage any risk of identification or re-identification and comply with any other applicable laws. This de-identified or anonymous data is

[48] Ibid 378.
[49] Productivity Commission, *Data Availability and Use* (Inquiry Report No 82, March 2017) 10.
[50] OAIC, *Australian Community Attitudes to Privacy Survey 2020* (n 11) 32.
[51] Roy Morgan, *Consumer Views and Behaviours on Digital Platforms* (Final Report, November 2018) 19.
[52] Privacy Act (n 16), sch 1, cl 3-5.
[53] Ibid sch 1, cl 11.
[54] Ibid s 6(1).
[55] Office of the Australian Information Commissioner, *De-identification and the Privacy Act* (Web Page, 21 March 2018).

often used for statistical and analytical purposes. Entities can de-identify any personal information at their discretion and do not need to notify individuals that de-identification can occur.[56]

To support robust de-identification practices and the management of re-identification risks, the OAIC and CSIRO's Data61 have released a non-binding de-identification decision-making framework.[57] The OAIC's guidelines on de-identification also encourage APP entities to consider the APPs which relate to use and disclosure, overseas transfers, and information security to mitigate any remaining privacy risks when handling de-identified information (APPs 6, 8 and 11).[58]

In 2016, the Privacy Amendment (Re-identification Offence) Bill was introduced to Parliament. The Bill sought to amend the Act to impose criminal and civil penalties relating to the re-identification of de-identified information released by Commonwealth entities. The Bill recognised that technological advances have enhanced re-identification risks associated with the release of de-identified information.[59] Although introduced to the Senate, the Bill was not passed by the Senate or considered by the House of Representatives and lapsed in 2019.[60]

In contrast to Australia, privacy laws in other jurisdictions dictate that personal information must be anonymised rather than de-identified for the definition of personal information (or personal data) to no longer apply.[61] Anonymisation is the process of irreversibly treating data so that no individual can be identified, including by the holders of the data.[62] This may be more difficult for data holders to achieve. However, it may protect individuals better against the privacy risks posed by potential re-identification.

Information about deceased individuals

The protections under the Act apply to personal information of living, natural persons.[63] Information about deceased individuals will only be personal information if it is also about a living person, (for example, information about genetic diseases of a deceased individual may be personal information of their living genetic relatives – indicating their vulnerability to developing that disease),[64] or in cases where an emergency declaration has been made under Part VIA of the Act.[65]

Affording protection only to living persons is consistent with the notion that only living people have privacy rights since 'dead people can feel no shame or humiliation'.[66] It is consistent with international instruments including the OECD Privacy Guidelines, the ICCPR, and the application of

[56] Ibid.
[57] CSIRO, *The De-identification Decision-Making Framework* (Web Page, accessed 2 October 2020).
[58] OAIC, *De-identification and the Privacy Act* (n 55).
[59] Explanatory Memorandum, Privacy Amendment (Re-identification Offence) Bill 2016 (Cth), [2].
[60] Parliament of Australia, *Bills and Legislation: Privacy Amendment (Re-identification Offence) Bill 2016* (Web Page, accessed 8 September).
[61] General Data Protection Regulation (n 39), recital 26.
[62] European Commission, *What is personal data* (Web Page, accessed 18 September).
[63] *Acts Interpretation Act 1901* (Cth) s 2B.
[64] OAIC, *Australian Privacy Principles Guidelines* (n 31) B.95.
[65] Privacy Act (n 16) s 80G.
[66] Paul Roth, 'Privacy Proceedings and the Dead' (2004) 11 *Privacy Law and Policy Reporter* 50 quoted in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 1, 355.

the GDPR, which leaves the creation of rules regarding the processing of personal data of deceased persons to member states.[67]

Some Australian states and territories extend privacy protection to the handling of information about deceased individuals by state public sector agencies and require these agencies to comply with privacy principles when handling information about deceased individuals. The extent of protection varies. In New South Wales, personal information is subject to privacy protection for up to 30 years following an individual's death,[68] whereas in the Northern Territory protection is extended for five years.[69]

Personal information of the deceased is also protected from disclosure through other statutes, such as the secrecy provisions in the *Social Security (Administration) Act*.[70] The *Freedom of Information Act* and the *Archives Act* protect against unreasonable disclosure of personal information of deceased individuals in response to requests for access to government documents.[71]

ALRC Report 108 recommended new privacy requirements apply to private sector organisations regulated under the Act in relation to the handling of information about deceased individuals for up to 30 years after their death.[72] The ALRC considered there are legitimate public policy reasons for extending some privacy protection to the personal information of deceased individuals, noting that obligations of confidence do not necessarily end when the person who has provided the information dies.[73] Access to digital records after death was recently examined more generally by New South Wales Law Reform Commission, which recommended changes to the ways in which NSW privacy laws deal with requests to access and manage personal information of deceased individuals.[74]

Questions

2. What approaches should be considered to ensure the Act protects an appropriate range of technical information?
3. Should the definition of personal information be updated to expressly include inferred personal information?
4. Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?
5. Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?

[67] Organisation for Economic Co-operation and Development, *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, 2013, para 6; *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17; General Data Protection Regulation (n 39).
[68] *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(a).
[69] *Information Act 2002* (NT) s 4 "person".
[70] *Social Security (Administration) Act 1999* (Cth) s 202.
[71] *Freedom of Information Act 1982* (Cth) s 47F; *Archives Act 1983* (Cth) s 33(1)(g).
[72] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 66) 377.
[73] Ibid 367.
[74] New South Wales Law Reform Commission, *Access to digital records upon death or incapacity* (Report No 147), December 2019) 74.

Flexibility of the APPs in regulating and protecting privacy

A key objective of the APPs is to balance the protection of the privacy of individuals, with the interests of public and private sector entities in carrying out their lawful and legitimate functions and activities.

Scalability of the APPs to a wide range of entities, acts and practices

The APPs enable the personal information of an individual to be collected, used and disclosed in certain circumstances where it is 'reasonably necessary' or directly related to, one or more of the entity's functions or activities. 'Reasonably necessary'[75] is an objective test, and it is the responsibility of an APP entity to justify that the particular collection, use or disclosure is reasonably necessary. Likewise, the use or disclose requirements in APP 6 rely on an interpretation of the 'reasonable expectation' of the individual whose personal information is being used or disclosed.[76]

This approach allows the APPs to be scalable to entities of various sizes and capabilities, and to be adapted to different acts and practices of those entities. However, by taking this broad-based approach, there are limited opportunities for the APPs to prescribe specific requirements or treatments in relation to certain classes of entities, information, or acts and practices.

Legislative flexibility to adapt the APPs

Exempt entities (or classes of entities), or acts and practices can be brought within the regulatory remit of the APPs through delegated legislation, where there is a public interest in doing so.[77] For example, the *Privacy Regulation 2013* requires that small business operators that operate residential tenancy databases comply with the APPs in relation to their conducting of that practice.[78]

There is also the power under Part IIIB of the Act to create an APP code. An APP Code can set out how the APPs are complied with, and may impose additional requirements to those imposed by the APPs.[79] Any additional requirements must not be contrary to, or inconsistent with the APPs.[80] A code can be targeted at:

- a specified type of personal information;
- a specified activity or specified class of activities of an APP entity;
- a specified industry or profession, or specified class of industries or professions; or
- APP entities that use technology of a specified kind.[81]

An APP code may be developed by the Information Commissioner if the Commissioner considers that it is in the public interest to do so. The Commissioner may also request that a private entity (for example, a peak industry group) develop a code for a relevant sector to be approved and subsequently registered by the Commissioner.[82] The public must have an opportunity to engage in the creation of any new or amended code. There are currently two codes that are in force, one

[75] OAIC, *Australian Privacy Principles Guidelines* (n 31) B.114.
[76] Privacy Act (n 16) sch 1, cl 6.2.
[77] Ibid div 1, part 2.
[78] *Privacy Regulation 2013* (Cth) s 7(1).
[79] Privacy Act (n 16) Part IIIB.
[80] Ibid s 26C(3)(a).
[81] Ibid s 26C(4).
[82] Ibid s 26E.

which applies to Commonwealth Government Agencies, and the other applying to market and social research.[83]

Questions

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

[83] *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth)*; Privacy (Market and Social Research) Code 2014* (Cth).

Exemptions from the Privacy Act

When the Act was extended to the private sector in 2000, it exempted small business operators, organisations in relation to employee records, media organisations and registered political parties.[84] The ACCC recommended that regard should be had to whether the Act should apply to some of these exempt entities.[85] It noted that there is a high risk associated with privacy violations in relation to employee records, due to human resources data often containing sensitive information. It also noted that media reports on the collection and use of personal information by political parties raise the issue of whether a broad exemption for 'registered political parties' remains appropriate.[86]

Small business exemption

The small business exemption was introduced in recognition of the potentially unreasonable compliance costs for certain small businesses, which were considered to pose little or no risk to the privacy of individuals.[87] 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 the low privacy risk.[88]

The exemption was based on the premise that not all private sector organisations pose the same risk to privacy. Many small businesses did not have significant holdings of personal information – they may have held customer records that were used for their own business purposes; however they did not sell or otherwise deal with customer information in a way that posed a high risk to the privacy interests of those customers. 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.[89]

In the 20 years since the small business exemption was introduced, technology has changed the way that small businesses operate. These advancements may mean that small businesses are increasingly handling personal information and may now pose a higher privacy risk than previously. Consumer attitudes to privacy may also have evolved since the introduction of the private sector amendments. The results of the 2020 ACAP survey show 71 per cent of survey participants think small businesses should be covered by the Privacy Act.[90]

The current law

A business is a 'small business' if its annual turnover for the previous financial year is $3 million or less.[91] Annual turnover is defined to include all income from all sources, but does not include assets held, capital gains or proceeds of capital sales.[92] However the small business exemption does not apply to a business that:

---

[84] *Privacy Amendment (Private Sector) Act 2000* (Cth).
[85] ACCC, *Digital Platforms Inquiry* (n 1) 476.
[86] Ibid 479.
[87] Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (Daryl Williams, Attorney-General).
[88] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 36.
[89] Ibid 74.
[90] OAIC, *Australian Community Attitudes to Privacy Survey 2020* (n 11) 60.
[91] Privacy Act (n 16) s 6D.
[92] Ibid s 6DA; see also Office of the Australian Information Commissioner, *Small business* (Web Page, accessed 14 September 2020).

- is a health service provider
- trades in personal information
- provides services under a Commonwealth contract
- is a credit reporting body
- operates a residential tenancy database
- 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 system
- is related to a business that is an APP entity.[93]

A business can also be brought into the scope of the Act if it is prescribed through regulation.[94] The regulation-making power allows small businesses to be brought within the scope of the Act where the Attorney-General is satisfied that it is in the public interest to do so. Regulations can also be made to prescribe certain acts or practices of small business operators to be subject to the Act. There is also a mechanism which allows small businesses to voluntarily opt-in to the Act.[95] This provides small businesses with the opportunity to benefit from any increase in consumer confidence and trust that may be derived from operating under the Act.

$3 million threshold

Before arriving at the $3 million figure, alternative thresholds of $1 million and $10 million were considered. A $10 million threshold was identified as unreasonable because it would carve out a significant portion of all businesses, which had the potential to adversely affect the efficacy of the legislation.[96] An Exposure Draft of the legislation proposed a threshold of $1 million, which would have exempted approximately 93.8 per cent of business categorised as small businesses by the ABS.[97] The ABS defines a small business as one with less than 20 employees.[98]

The $3 million threshold was adopted based on estimates that 98.9 per cent of businesses categorised as small businesses by the ABS would be captured by the $3 million threshold and exempted from the requirements of the Act.[99] The Explanatory Memorandum stated that the $3 million figure would be reviewed from time to time to ensure that it remained appropriate.[100]

---

[93] Privacy Act (n 16) ss 6D(4)(b)-(f), 6E(1A)-(1D), 6D(9); *Privacy Act Regulation 2013* (Cth) s7.
[94] *Privacy Regulation 2013* (Cth) s 7; the Regulation currently prescribes small business operators that operate residential tenancy databases and Aussie Farms Inc.
[95] Privacy Act (n 16) s 6EA; the OAIC maintains a register of small business operators that have opted-in to the Privacy Act. As at 14 September 2020, the register contained the names of 641 businesses.
[96] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 37.
[97] House of Representatives Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (Report, June 2000) ch 2, 11.
[98] Geogg Gilgillan, 'Definitions and data sources for small businesses in Australia: A Quick Guide' (Research Paper, Parliamentary Library, Parliament of Australia, 1 December 2015).
[99] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 37; House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (n 97) 11.
[100] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 37.

In other contexts, the Australian Government defines a small business by reference to other factors such as its number of employees and the value of its assets. In addition to the ABS definition above, the *Fair Work Act 2009* (FW Act) defines a small business as one that employs less than 15 employees[101] and the Australian Taxation Office defines a small business as one that has annual aggregate turnover of less than $10 million.[102] This inconsistency reflects that there is no generally accepted definition of what constitutes a small business.

When the $3 million threshold was considered by the House of Representatives Standing Committee on Legal and Constitutional Affairs, the committee was of the view that the use of employee numbers to determine whether a business was a small business could have unintended consequences in relation to internet-based businesses, where high privacy risk businesses could have low numbers of staff. The committee concluded that any form of threshold would appear arbitrary in some circumstances and that if access to the exemption was determined by addressing issues of privacy risk, with high risk businesses unable to access the exemption, the use of a turnover threshold was of reduced significance.[103]

In 2005, the then Office of the Privacy Commissioner recommended that the ABS definition of small business should be adopted in place of the annual turnover threshold.[104] The report concluded that the $3 million threshold was arbitrary and that reference to a number of employees would be more easily understood by consumers. The Government did not agree with this recommendation, noting that redefinition could capture some small operators not required to comply with the Act, which would increase compliance costs for these businesses and would be inconsistent with the aims of cutting red tape.[105]

The current threshold of $3 million is fixed rather than indexed, meaning that with inflation over time, the 'real' value of the threshold is declining.

Balancing privacy risks and compliance costs

In its Advisory Report on the private sector reforms to the Act, the House of Representatives Standing Committee on Legal and Constitutional Affairs (Standing Committee) took the view that, from the perspective of protecting privacy, the nature of the information being handled and how it was used was important, rather than the size of the business involved. For example, a business with a small turnover could nonetheless handle particularly sensitive data while a large business may not.[106]

The Standing Committee recognised the importance of an equitable regulatory regime for business, particularly where technology allowed small and large businesses to compete in the same markets

---

[101] *Fair Work Act 2009* (Cth) ('Fair Work Act') s 23.
[102] Australian Taxation Office, *Small business entity concessions – eligibility* (Web Page, 15 September 2017).
[103] House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (n 97) 12.
[104] Office of the Privacy Commissioner, *Getting in on the Act: the Review of the Private Sector Provisions of the Privacy Act 1988* (Report, March 2005) 185.
[105] Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006).
[106] House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (n 97) 12.

with little consumer differentiation as to the size of the entity they were dealing with. It concluded that an effective regulatory balance had to be achieved in order to avoid overly burdening small businesses that posed low privacy risks and this could not be achieved without some form of exemption for small business.

In its report '*The real Big Brother: Inquiry into the Privacy Act 1988*' the Senate Legal and Constitutional References Committee (Senate Committee) recommended the removal of the small business exemption on the basis that the exemption inconsistently regulates businesses and adds to the complexity of the Act.[107] It considered that individual's privacy rights should be protected irrespective of the size of the business they were dealing with and that protecting privacy rights made commercial sense for all businesses. The Government did not agree with this recommendation and noted that the exemption struck the right balance between risk of privacy breaches and regulation of small businesses, and the recommendation would be inconsistent with cutting red tape.[108]

In ALRC Report 108, the ALRC recommended the removal of the small business exemption, concluding that its removal would have substantial benefits for the protection of privacy.[109] The ALRC noted that no other comparable jurisdiction (the United Kingdom, New Zealand, Canada and the European Union) exempts small businesses from the general privacy law.[110] The Senate Committee inquiry further recommended the removal of the exemption given the privacy regimes in overseas jurisdictions have operated effectively without a small business exemption and that the existence of the exemption was one of the key outstanding issues preventing Australia from seeking adequacy with the EU.[111] The EU restricts the export of personal data from an EU member state to a recipient country that does not have an adequate level of privacy protection.

Consent provisions

The consent provisions of the small business exemption provide that a small business that trades in personal information may still be exempt from the Act if it has the consent of individuals to collect or disclose their personal information.[112] The Privacy Commissioner's review of the small business provisions, recommended the removal of these consent provisions on the basis the provisions were 'clumsy and complicated'. This review also noted there was a considerable lack of certainty for small business that trade in personal information because it was not clear whether a single failure to gain consent would change the exempted status of the small business.[113] The review also recommended the removal of the consent provisions to ensure that all organisations that trade in personal information would be regulated by the Act.[114] The Government response disagreed with the

---

[107] Senate Legal and Constitutional References Committee, Parliament of Australia, *The Real Big Brother: Inquiry into the Privacy Act 1988* (Report, June 2005) 157.
[108] Australian Government Attorney-General's Department, *Government Response to the Senate Legal and Constitutional References Committee Report: The Real Big Brother: Inquiry into the Privacy Act 1988* (2006).
[109] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 2, 1358.
[110] Ibid 1319.
[111] Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (n 107) 68.
[112] Privacy Act (n 16) s 6D(7)-(8).
[113] Office of the Privacy Commissioner, *Getting in on the Act: the Review of the Private Sector Provisions of the Privacy Act 1988* (n 104) 185.
[114] Ibid 62.

recommendation to remove the consent provisions on the basis that the Act provides an appropriate mechanism for dealing with situations in which the consent provisions should not operate.[115]

Questions

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

[115] Australian Government Attorney-General's Department, *Government Response to the Privacy Commissioner's Report: Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (n 105).

Employee records exemption

The employee records exemption applies to acts or practices of 'organisations', which broadly covers non-public sector entities, in their capacity as employers or former employers.[116] While personal information about employees typically held on personnel files was regarded as 'deserving of privacy protection', the exemption was included on the basis that the 'handling of employee records is a matter better dealt with under workplace relations legislation'.[117]

This rationale reflected the largely state responsibility for workplace relations laws at that time. In the Government's response to recommendations of the 2000 House of Representatives Standing Committee on Legal and Constitutional Affairs to narrow the employee records exemption in the Bill, it noted that:

> *the regulation of employee records is an area that intersects with a number of State and Territory laws on workplace relations, minimum employment conditions, workers' compensation and occupational health and safety, some of which already include provisions protecting the privacy of employee records. The Government considers that to attempt to deal with employee records in the Bill might result in an unacceptable level of interference with those State and Territory laws, and a confusing mosaic of obligations*.[118]

Commonwealth, state and territory workplace relations laws include provisions which require employers to maintain certain employee records. The basis for these provisions is to ensure records are available for inspection by workplace inspectors and authorised union officials to ensure compliance with workplace laws. Some also provide employees, and former employees, with a right to access records held about them.

The findings of the 2020 ACAP survey show that 72 per cent of respondents considered employers requesting access to an employee's social media account to be a misuse of personal information. Of those respondents who were aware of the employee records exemption, 64 per cent believed that businesses collecting work-related information about employees should be covered by the Act.[119]

Scope of the exemption

The exemption applies to an organisation acting in its capacity as an employer or former employer of an individual, in relation to acts or practices that are directly related to the employment relationship, where the act or practice directly relates to an 'employee record'.[120] 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.[121]

A relationship between a job applicant and a prospective employer does not constitute a 'current or former employment relationship'. Personal information collected from prospective employees who

---

[116] 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; Privacy Act (n 16) s 7B(3).
[117] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 4-5; Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15752 (Daryl Williams, Attorney-General).
[118] Australian Government Attorney-General's Department, *Government Response to House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (September 2000) 4.
[119] OAIC, *Australian Community Attitudes to Privacy Survey 2020* (n 11) 39 and 60.
[120] Privacy Act (n 16) s 7B(3).
[121] *'QF' & Others and Spotless Group Limited (Privacy)* [2019] AICmr 20.

are subsequently not employed by an organisation, such as unsuccessful job applicants, will not be covered by the employee records exemption.[122]

An employee record under the Act is a record of personal information relating to the employee.[123] There is no distinction for the purpose of the exemption between personal information and sensitive or health information. The Act provides examples of personal information relating to an employee as including health information and personal information about the employee's engagement, training, disciplining or resignation, the termination of the employee, terms and conditions of employment, performance or conduct, hours of employment, salary or wages, memberships of professional or trade associations, leave and financial information.

The exemption therefore covers a diverse range of employer-held records which may contain personal information, such as details of next of kin, addresses, date of birth, banking information, medical information, details of disciplinary processes including opinions about an employee's performance or conduct and employees' emails and browsing histories.

Current privacy protection for employees

The employee records exemption does not apply to 'agencies' as defined in the Act. This means that Commonwealth departments and other agencies governed by the *Public Service Act 1999* (Cth) are bound by the Act in their handling of personal information about employees.

The FW Act requires national system employers to make and keep employee records of the kind prescribed by the regulations in relation to each employee for a period of 7 years.[124] The coverage of the FW Act includes all employees located in Victoria (with limited exceptions), the Northern Territory (except law enforcement officers), Tasmania (except state government employees) and the Australian Capital Territory; employees employed by private enterprise in New South Wales, Queensland, and South Australia; and employees of constitutional corporations in Western Australia.[125]

The *Fair Work Regulations 2009* (Cth) require employers to keep a record in respect of each employee about basic employment details such as the name of the employer and the employee and other matters relating to their employment including the nature of their employment (e.g. part-time or full-time, permanent, temporary or casual), pay, overtime hours, leave entitlements, superannuation contributions and the manner of termination of employment (where applicable). Employers must ensure the records are legible and must make a copy of an employee record available for inspection and copying on request by the employee or former employee to whom the record relates. An employer is also required to correct an employee record as soon as the employer becomes aware that it contains an error.

Privacy legislation has been enacted in all states and territories apart from South Australia and Western Australia which regulates the handling of employees' personal information by state and territory public sector employers.[126] There are limited exemptions in state and territory privacy

---

[122] Office of the Australian Information Commissioner, *Employee records exemption* (Web Page, accessed 19 September 2020).
[123] Privacy Act (n 16) s 6(1).
[124] Fair Work Act (n 101) s 535.
[125] Fair Work Commission, *What is a national system employer* (Web Page, accessed 19 September 2020).
[126] *Privacy and Personal Information Protection Act 1998* (NSW); *Privacy and Data Protection Act 2014* (Vic); *Information Privacy Act 2009* (Qld); *Personal Information and Protection Act 2004* (Tas); *Information Privacy*

legislation for personal information relating to employees.[127] Some states and territories have also enacted legislation which regulates the handling of health information by the public and private sector.[128] Some states and territories have also legislated to restrict surveillance of employees.[129]

Key issues

Sensitive information

The higher levels of protection afforded to sensitive information, including health information, under the Act do not apply where the employee records exemption applies. This is in contrast to the small business exemption which does not apply to small businesses that provide health services and hold any health information, except in an employee record.[130]

In 2003, the ALRC recommended that the Act be amended to ensure that employee records are subject to the protections of the Act, to the extent that they contain genetic information, and that the Government consider whether to amend the Act to ensure that employee records are subject to the protections of the Act, to the extent that they contain health information other than genetic information. [131] It further recommended that employers should not collect or use genetic information of job applicants or employees, except in limited circumstances where this is consistent with privacy, anti-discrimination, and occupational health and safety legislation.[132]

Genuineness of employees' consent

A recent decision by a Full Bench of the Fair Work Commission considered the employee records exemption in the context of an unfair dismissal claim under the FW Act.[133] It was held that an employer's direction to an employee to submit to fingerprint scanning to record his attendance contravened his right under APP 3 to withhold consent to the employer's request to collect his sensitive information. The Full Bench found that the employee records exemption did not operate to exempt the employer from its obligations under the Act and APPs as the exemption only applies once the employee record has been generated.[134] The direction was therefore not lawful and the employee's refusal to allow his personal information to be collected was not a valid reason for dismissal.[135] The Full Bench also commented that any consent the employee might have given once

---

Act 2014 (ACT); *Information Act 2002* (NT). The Western Australian government is currently consulting on privacy and responsible information sharing legislation for the WA public sector.

[127] For example, s 10 of the *Personal Information Protection Act 2004* (Tas) exempts employee information from specific Personal Information Protection Principles.

[128] *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT). Section 5(3)(n) of the *Health Records and Information Privacy Act 2002* (NSW) excludes information held in an employee record (within the meaning of the Privacy Act) by a private sector employer from the definition of personal information for the purposes of that Act.

[129] Examples of legislation regulating workplace surveillance include the *Privacy and Personal Protection Act 1988* (NSW), *Surveillance Devices Act 1999* (Vic) and the *Surveillance Devices Act 1998* (WA); *Workplace Privacy Act 2011* (ACT).

[130] Privacy Act (n 16) s 6D(4)(b).

[131] Australian Law Reform Commission, *Essentially Yours: The Protection of Human Genetic Information in Australia* (Report 96, 28 March 2003) 69.

[132] Ibid 67.

[133] *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946; 286 IR 368.

[134] Ibid [55].

[135] Ibid [58].

told he faced disciplinary action or dismissal would not have been genuine consent at it would be likely to be vitiated by the threat.[136]

Although this case concerned a claim under the FW Act rather than a claim for breach of the Act or APPs, it raises questions for employers about the application of the employee records exemption to the act of employers' soliciting employees' personal information, as well as employees' ability to genuinely consent to the collection of their sensitive information by their employer.

Balancing employers' ability to manage and compliance burden with employee privacy

In the ALRC's consideration of the employee records exemption in Report 108, it noted concerns by submitters that removing the employee records exemption would undermine the ability of businesses to manage their human resources effectively.[137]

In recommending the exemption be removed, the ALRC considered that rather than undermining the ability of businesses to manage their human resources effectively, 'good information-handling practices would assist in ensuring that organisations would be making sound business decisions based on accurate and up-to-date information that is held securely within the organisation'. The ALRC considered that the application of the privacy principles need not interfere with the management interests of employers or the employment relationship.[138] It also highlighted that aspects of the employment relationship, such as its ongoing nature and mutual trust and confidence, reinforce rather than negate the need to ensure that the privacy of employees is protected. It also noted that the United Kingdom does not exempt employee records and that removing the exemption may facilitate recognition of the adequacy of Australian privacy law by the EU.[139]

Questions

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

[136] Ibid.
[137] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1383.
[138] Ibid 1392.
[139] Ibid.

Political exemption

Personal information is widely used in the democratic process, including in the management of party registrations, communications between Members of Parliament (MPs) and their constituents, the provision of AEC-certified voter lists to MPs and candidates,[140] and the construction of voter databases by political parties for electoral purposes.[141]

Registered political parties and political acts and practices engaged in by specified entities are currently exempt from the operation of the Act. The political exemption was designed to "enhance the freedom of political communication in Australia and to prevent restrictions on the democratic process".[142]

Following recent controversies overseas about data misuse by political consultancies and digital platforms[143], there have been renewed calls to re-examine the status of the political exemption.[144] The findings of the 2020 ACAP survey indicate support for a re-examination, with 74 per cent of respondents stating that political parties should be subject to the Act.[145]

The current law

Section 6C expressly excludes "registered political parties" from the definition of an Organisation for the purposes of the Act. Registered political parties are therefore not required to comply with the APPs or other requirements of the Act in how they collect, use, disclose or store personal information.

Section 7C exempts political acts or practices done in connection with an election, a referendum or another aspect of the political process by political representatives (MPs and local government councillors), contractors and subcontractors for political parties and representatives, as well as volunteers for registered political parties. Acts or practices in relation to personal information for a purpose unconnected with an election, referendum or other participation in the political process is subject to the Act.[146]

Breadth of the exemption

In 2000, the House of Representatives Standing Committee on Legal and Constitutional Affairs recommended that the section 7C exemption should be altered in scope from excluding acts and practices for the purpose of 'participation in the political process' to the 'parliamentary or electoral process'.[147] The Government did not accept the recommendation on the basis that incorporating the proposed wording would have the effect of narrowing the exemption which was not what the Committee had intended in making the recommendation.

---

[140] *Commonwealth Electoral Act 1918* (Cth) ss 90B, 91A, 91B.
[141] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1416-1417.
[142] Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (Daryl Williams MP).
[143] Cecelia Kang and Sheera Frenkel, 'Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users', *New York Times* (online, 4 April 2018).
[144] ACCC, *Digital Platforms Inquiry* (n 1) 479.
[145] OAIC, *Australian Community Attitudes to Privacy Survey 2020* (n 11) 60.
[146] Privacy Act (n 16) s 7C.
[147] House of Representatives Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (Report, June 2000) ch 5, Recommendations 11-12.

The ALRC in its Report 108, acknowledged that any reform of the exemption must take into account the strong public interest in promoting Australia's system of representative democracy. It considered removing the exemption altogether, providing limited exceptions for political acts and practices or requiring registered political parties and other entities engaging in political acts and practices to develop information-handling guidelines, in consultation with the then Office of the Privacy Commissioner.[148]

The ALRC ultimately recommended removing the political exemption as it would be 'in the interests of promoting public confidence in the political process, [that] those who exercise or seek power in government should adhere to the principles and practices that are required of the wider community'.[149] The ALRC also noted that removing the exemption would accord with comparable overseas jurisdictions which do not exempt political parties, including the United Kingdom and New Zealand.

Implied freedom of political communication and parliamentary privilege

The operation of the political exemption may be subject to the implied constitutional freedom of political communication and parliamentary privilege. The implied freedom of political communication has been recognised by the High Court as an essential element of representative democracy, operating as a restriction on legislative and executive powers.[150] Similarly, the freedom of speech and debate privilege which provides MPs with immunity for anything they may say or do in the course of parliamentary proceedings or anything incidental to those proceedings, has been described as the single most important parliamentary privilege.[151]

To accommodate this, the ALRC recommended inserting a provision into the Act to expressly provide that the Act would not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication.[152]

Questions

16. Should political acts and practices continue to be exempted from the operation of some or all of the APPs?

[148] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1426.
[149] Ibid 1428.
[150] *Theophanous v Herald & Weekly Times Ltd* (1994) 182 CLR 104, 168; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 561; cited in ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1417.
[151] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1418.
[152] Ibid 1433.

Journalism exemption

The purpose of exempting media organisations from the Act was 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.[153] This exemption is considered critical to maintaining a democratic society.[154]

While the need to safeguard the media's role remains, the evolving nature of data and communications has greatly influenced the production and distribution of news. Emerging forms of journalism – driven by the rise of social media – have elevated the role of individuals as sources, content providers and even reporters.

Scope of the exemption

Subsection 7B(4) of the Act exempts acts and practices of 'media organisations' engaging in the course of journalism from the operation of the Act, provided the organisation is publicly committed to observing published privacy standards that deal with privacy in the context of the activities of a media organisation. A media organisation is therefore bound by the privacy standards applicable to media organisations and not the standards in the Act. For example, most journalists who are members of the Media, Entertainment & Arts Alliance are bound by its *Journalist Code of Ethics*; print or online media organisations that are members of the Australian Press Council are bound by its *Standards of Practice* which include the *Statement of Privacy Principles*; and radio and television industry groups develop codes of practice in accordance with the *Broadcasting Services Act*.[155]

A 'media organisation' is one whose activities consist of or include the collection, preparation for dissemination or dissemination to the public of material having the character of news, current affairs, information or a documentary or commentary or opinion on, or analysis of, news, current affairs, information or a documentary.

Although subsection 7B(4) of the Act refers to 'journalism', this word is not defined in the Act. The Privacy Amendment (Private Sector) Bill 2000 had initially included a definition. However this was removed on the basis that the ordinary meaning of the word should apply, after concerns were raised that the proposed definition would have covered activities beyond the commonly understood activities of journalism. The term 'journalism' was intended to apply in a technology-neutral way.[156]

Re-defining journalism and media organisations

Although the rationale for this exemption is widely accepted, questions have been raised about whether its scope is too wide and, as a consequence, it is being improperly claimed.[157] The ALRC has previously recommended narrowing the scope of the exemption by including a definition of journalism.[158]

The ALRC's consideration of a definition of journalism was based on concerns that the lack of a definition – combined with the wide definition of the term 'media organisation' – may allow a range

[153] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 4.
[154] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1439.
[155] Ibid 1453-1454.
[156] Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 2.
[157] Office of the Privacy Commissioner, *Getting in on the Act: the Review of the Private Sector Provisions of the Privacy Act 1988* (n 104) 197-198.
[158] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1452-1453.

of parties to claim the exemption even though they may not ordinarily be considered to be engaging in journalism. It was of the view that including a definition would limit the scope of the exemption to acts and practices that are associated with a clear public interest in freedom of expression.[159]

With the emergence of non-traditional media including reporting by citizen journalists and production of news content involving the application of big data[160], it is also important to consider if these types of journalism should be covered by the journalism exemption and how this may impact on how the exemption is framed.

Media privacy standards

The 2020 ACAP survey indicates there are strong community expectations that the media behaves in a manner respectful of individual privacy. 72 per cent of survey respondents expressed a view that media organisations should be subject to the Privacy Act and 61 per cent of respondents who were aware of the journalism exemption expressed the same view.[161]

In 2017-18, the Australian Press Council responded to 94 complaints relating to intrusions on privacy.[162] The Council may reprimand an organisation and explicitly call for apologies, retractions, corrections or other remedial action from its members, but has no power to order enforceable compensation, fines or other financial sanctions.[163]

In 2012, the Report of the Independent Inquiry into the Media and Media Regulation recommended the establishment of a new body to set journalistic standards for the news media in consultation with the media industry, which would handle complaints made by the public when those standards are breached.[164] While the recommendations did not directly relate to the journalism exemption under the Privacy Act, the report highlighted shortcomings with the regulatory model which applies to journalists in the place of the privacy principles in the Act.

Questions

17. Does the journalism exemption appropriately balance freedom of the media to report on matters of public interest with individuals' interests in protecting their privacy?
18. Should the scope of organisations covered by the journalism exemption be altered?
19. Should any acts and practices of media organisations be covered by the operation of some or all of the APPs?

[159] In 2005, the then Office of the Privacy Commissioner also recommended defining the term 'in the course of journalism' to ensure the exemption operates according to the public interest: Office of the Privacy Commissioner, Office of the Privacy Commissioner, *Getting in on the Act: the Review of the Private Sector Provisions of the Privacy Act 1988* (n 104) 198-199.

[160] Chris Atton, 'Separate, supplementary or seamless? Alternative news and professional journalism', in Chris Peters and MJ Broersma (eds), *Rethinking Journalism: Trust and Participation in a Transformed News Landscape* (Taylor & Francis Group, 2012) 131; Seth Lewis, 'Journalism in an Era of Big Data', (2015) 3(3) *Digital Journalism* 321.

[161] OAIC, *Australian Community Attitudes to Privacy Survey 2020* (n 11) 58-60.

[162] Australian Press Council, *Annual Report 2017-2018* (Annual Report No 42, June 2018) 21.

[163] Australian Press Council, *Handling of Complaints* (Web Page, accessed 30 September 2020).

[164] The Hon Raymond Finkelstein QC, *Report of the Independent Inquiry into the Media and Media Regulation: Report to the Minister for Broadband, Communications and the Digital Economy* (Report, February 2012) 8.

Protections

Notice of collection of personal information

The Act requires that regulated entities that collect personal information about individuals take reasonable steps to notify that individual about the collection of their personal information. Notice is a key component of privacy as it provides the basis for individuals to understand why an entity is collecting their personal information and to make an informed decision about whether to consent to a proposed collection of certain types of personal information and to the use or disclosure of their personal information for certain purposes.

The current Australian law

Legal requirement

APP 5.1 requires that at the time of collection, or if that is not practicable, as soon as is practicable after collection, the APP entity must take such steps (if any) as are reasonable in the circumstances, to notify, or otherwise ensure that the relevant individual is aware of certain matters.[165]

The matters which an APP entity must take reasonable steps to notify the individual of are listed in APP 5.2. They include, for example, the identity and contact details of the APP entity; the purposes for which the APP entity is collecting the personal information; and other persons or APP entities to whom the collecting entity normally discloses personal information. Chapter 5 of the APP Guidelines provides advice about compliance with APP 5.[166]

Background to the requirement

In its Report 108, the ALRC considered it appropriate for an entity to only take such steps, if any, as are reasonable in the circumstances as this would enable the notification principle to be sufficiently high-level and flexible to be applied in a wide variety of circumstances.[167]

This view is reflected in APP 5, which requires that entities take such steps as are "reasonable in the circumstances". The explanatory memorandum to the introduction of the APPs into the Privacy Act in 2012 explained that:

> The phrase 'reasonable in the circumstances' is an objective test that ensures that the specific circumstances of each case have to be considered when determining the reasonableness of the steps in question. This flexibility is necessary given the different types of APP entities and functions/activities that are to be regulated under the APPs. In many cases, it would be reasonable in the circumstances for an APP entity to provide the information outlined in APP 5.2.[168]

The concepts of 'reasonableness' and 'practicability' are central to the model of notice under APPs. This flexibility extends to the manner in which notice is communicated to the individual. An APP entity is required to "notify…or otherwise ensure that the individual is aware of any such matters".[169]

---

[165] Privacy Act (n 16) sch 1, cl 5
[166] OAIC, *Australian Privacy Principles Guidelines* (n 31).
[167] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 778.
[168] Privacy Amendment (Enhancing Privacy Protection) Bill (Cth) 2012.
[169] Privacy Act (n 16) sch 1, cl 5.1(a)-(b).

ACCC Digital Platform Inquiry Final Report recommendations

The DPI report recommended that the notification requirements be strengthened. Recommendation 16(b) proposes that:

- All collection of personal information (whether directly or indirectly) be accompanied by a notice from the APP entity collecting the personal information unless the individual already has the information or there is an overriding legal or public interest reason;
- The notice must be concise, transparent, intelligible and easily accessible and must clearly set out how the APP entity will collect, use and disclose the information. The notice should be able to be readily understood by persons of the minimum age of the permitted platform user; and
- To reduce information burden, it may be appropriate to implement these requirements with measures such as layered notices or the use of standardised icons or phrases.[170]

The ACCC considered that APP entities currently have significant discretion about whether they notify consumers about collection of their personal information and how that notice is provided. This creates "information asymmetry" between the APP entity and the person whose information is being collected such that the person is not fully informed or does not fully understand the scope of information that is being collected and how the APP entity may use their information. This impacts on individuals' ability to make informed choices about whether to engage with a business.[171]

The ACCC also considered that the regulatory burden associated with increased notice requirements would be unlikely to outweigh the benefits of strengthened notification requirements, particularly as the ACCC was of the view that the requirement would be commensurate with the extent to which the APP entity collects, uses and discloses an individual's personal information.[172]

Key issues

Ensuring individuals are aware of relevant matters

Notice will only be effective in assisting an individual to make an informed decision where the notice is presented in a way that can be easily understood by an individual. 63 per cent of respondents to the 2020 ACAP survey indicated they do not read privacy policies. The main reason for this being that they are too long and complex.[173] Additionally, only five per cent of respondents felt very confident they understood a privacy policy after reading it.[174] The importance of presenting information about entities' practices with regard to personal information is highlighted by the finding that 64 per cent of those who read a privacy policy took specific actions (such as declining to use, or discontinuing a service; or changing their privacy settings) in relation to their personal information provided under that policy.[175]

Not every person has the same capacity to engage with, and absorb information. This is particularly relevant to children and other vulnerable persons. To ensure children and other vulnerable groups are appropriately notified, consideration must be given to whether requirements should ensure that

[170] ACCC, *Digital Platforms Inquiry* (n 1) 461.
[171] Ibid 448.
[172] Ibid 462.
[173] OAIC, *Australian Community Attitudes to Privacy Survey 2020* (n 11) 48.
[174] Ibid.
[175] Ibid 72.

notice is provided in a way that is widely accessible, especially where a product or service is targeted at a vulnerable group.

Third party collections

There is an added layer of complexity where an individual's personal information is collected by a third party. APP 3 requires entities to collect personal information directly from an individual unless it is unreasonable or impracticable to do so. However where individual's personal information is collected by a third party, it often occurs without their knowledge, and so the individual is not in a position to make any decisions about how the collecting entity handles (or does not handle) their personal information.

The ACCC's view is that an individual should always be provided with notice when their personal information is collected, regardless of whether the collection is direct or indirect. However, there is the question of how this could be implemented where the entity does not have the individual's contact information.

Limiting information burden

It is important that an individual is able to engage with, and absorb the information being presented to them. According to a poll of 3,419 adults living in the US, the average American has an average of 27 online accounts.[176] This provides a snapshot of the number of different entities collecting and handling one individual's personal information in just the online sphere.

Any consideration of increasing notification requirements needs to be accompanied by discussion of how best to communicate notice to individuals in a way that will promote engagement, reduce information overload and reduce the risk of consent fatigue. The ACCC suggested layered notices or standardised icons or phrases could be used to assist individuals to comprehend and process the data handling practices of entities.[177]

Questions

Improving awareness of relevant matters

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

Third party collections

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

Limiting information burden

24. What measures could be used to ensure individuals receive adequate notice without being subject to information overload?

[176] Jason Aten, 'Google Says 66% of Americans Still Do This One Thing That Puts Their Personal Information at a Huge Risk', *Inc* (online, 2 October 2019); citing Google and Harris Insights & Analytics, '*The United States of Passwords*', *Google/Harris Poll* (Web Page, October 2019).
[177] ACCC, *Digital Platforms Inquiry* (n 1) 403.

25. Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?

Consent to collection and use and disclosure of personal information

The key way individuals exercise control over their personal information is through granting consent for entities to collect, use and disclose their personal information for different purposes.

The current Australian law

Legal requirement

Under the APPs, there are limited circumstances where an individual's consent is required for entities to be able to collect, use or disclose personal information. Consent can be 'express or implied'.[178]

When an entity collects personal information, APP 3 and APP 4 require that the collection be 'reasonably necessary for, or directly related to, one or more of an entity's functions or activities.[179] An APP entity must collect personal information only by lawful and fair means and only from the individual unless it is unreasonable or impractical to do so or another legislative exception applies.

Personal information that is not sensitive information can be collected without the individual's consent. APP 6 permits an entity to use or disclose the collected personal information without obtaining consent provided it is for the primary purpose for which it was collected, or for a secondary purpose if the individual would reasonably expect the entity to use or disclose their personal information for the secondary purpose and the secondary purpose is related to the primary purpose for which the personal information was collected. Other uses or disclosures are prohibited unless consent is obtained or another legislative exception applies. [180]

An individual must consent to the collection of their sensitive information. An entity can use or disclose the collected sensitive information without obtaining further consent provided it is for the primary purpose for which it was collected or for a secondary purpose if the individual would reasonably expect the entity to use and disclose the information for the secondary purpose and where that purpose is *directly* related to the primary purpose of collection. Other uses or disclosures are prohibited unless consent is obtained or another legislative exception applies. [181]

The exceptions to the requirement of obtaining consent to collect sensitive information and to the use or disclosure of personal information or sensitive information for a purpose other than a primary or secondary purpose include law enforcement purposes, legal proceedings, permitted general situations and permitted health situations.[182] These exceptions recognise that there are circumstances where there is an overriding public interest which is of greater importance than the individual's rights in relation to their personal information.

The Act also contains a mechanism to allow for an emergency declaration to be made to facilitate the response to an emergency or disaster of national significance. A declaration can be made by the Attorney-General or the Prime Minister. The effect of an emergency declaration is to allow entities

[178] Privacy Act (n 16) s 6(1).
[179] See ibid sch 1, cl 3 for solicited collection and cl 4 for unsolicited collection.
[180] Privacy Act (n 16) sch 1, cl 6.
[181] Ibid sch 1, cl 6.
[182] See ibid sch 1, cl 3.4 in relation to collection, and cl 6.2 in relation to use and disclosure.

to collect, use and disclose personal information without obtaining consent, where the purpose for that handling is to respond to the emergency or disaster.[183]

Guidelines for interpreting consent

In its Report 108, the ALRC considered that what is required to demonstrate that consent has been obtained is highly dependent on the context in which personal information is collected, used and disclosed.[184] The ALRC considered that the privacy regulator should provide guidance on the context of consent rather than providing greater specificity in legislation.

Chapter B of the APP Guidelines state that consent should have the following characteristics:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

ACCC Digital Platform Inquiry Report recommendations relating to consent

In the DPI report, the ACCC recommended that consent requirements should be strengthened. Recommendation 16(c) proposes that:

- Entities should be required to obtain consent in relation to any collection, use or disclosure unless the personal information is necessary for the performance of a contract to which the individual is party, is required by law, or an overriding public interest reason applies;
- Valid consent should require a clear affirmative act that is freely given, specific; unambiguous and informed. This includes de-bundling consents and any settings for data practices relying on consent to be pre-selected to 'off'; and
- Measures should be considered to reduce consent fatigue. This could include the use or standardised icons or phrases to facilitate comprehension and aid decision-making.

The ACCC considered that stronger consent requirements will increase the transparency of information processing and significantly reduce the effects of the bargaining power imbalance between consumers and the entities processing their personal information.[185]

The ACCC also recommended that privacy reforms should have specific regard to whether the Act should offer protection for inferred information, particularly where inferred information includes sensitive information, such as information about an individual's health, religious belief, or political affiliations.[186]

Key issues

Consent as a condition of service

As noted in the DPI report, digital platforms require wide ranging consents from an individual to the collection, use and disclosure of their personal information as a condition of accessing the service or

[183] Privacy Act (n 16) Part VIA.
[184] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 683.
[185] ACCC, *Digital Platforms Inquiry* (n 1) 465.
[186] Ibid 394.

product. A key finding was that 'click-wrap agreements with take-it-or-leave-it terms that bundle a wide range of consents … leverage digital platforms bargaining power and deepen information asymmetries, preventing consumers from providing meaningful consents to digital platforms' collection, use and disclosure of their user data'.[187]

This practice raises concerns that consumers may be required to consent to the use of their personal information for a purpose that is against their interests in order to access a product or service. The DPI report noted that:

> This could include circumstances where personal information is used and disclosed to provide the consumer with a service, such as using location information to provide navigational assistance. However, it could also include the use and disclosure of personal information for purposes that may not be in the consumer's interests, such as disclosure to third parties for targeted advertising or online profiling purposes.[188]

While the trade-off between providing personal information to an entity in return for accessing a product or service without a monetary charge may be in that individual's interest, it is desirable that the individual has a proper understanding of the purposes for which their personal information may be used and disclosed and that their consent to such an arrangement is meaningful.

Consent to wide ranging and multiple purposes for collection, use and disclosure

The DPI report also noted that digital platforms may collect personal information without an individual's consent for wide-ranging purposes on the basis that such collection is necessary for the digital platform's functions or activities, even where such practices may not meet consumer expectations.[189] It cited the example of digital platforms collecting web-browsing data of users on third party websites for the platform's advertising related functions.[190]

It also noted the practice of digital platforms describing 'numerous broadly-expressed purposes for their collection of personal information' which means there is no requirement for any additional consent to the use of disclosure of that information because the multiple purposes for collection may be construed as the primary purposes for collection, such that no further consent is required to use or disclosure for those purposes.[191] Due to often lengthy and complex terms of service, and evidence that individuals do not read these notices, individuals are often unaware of what they are consenting to. The results of the 2020 ACAP survey indicate that three quarters of survey respondents do not read most or all privacy policies, with one third of Australians reading few or no policies.[192]

Pro-consumer defaults

The DPI report recommended, in light of the preference of the majority of users that digital platforms should only collect information needed to provide their products or services, that default

[187] Ibid 394.
[188] Ibid 465.
[189] Ibid 382: 85 per cent of respondents to a consumer survey on digital platforms indicated that they should only collect information needed to provide their products or services.
[190]Ibid 438: 83 per cent of respondents to a consumer survey on digital platforms considered monitoring and collection of their online activities without their express consent to be a misuse of their personal information.
[191] Ibid.
[192] OAIC, *Australian Community Attitudes to Privacy Survey 2020* (n 11) 117.

settings enabling data processing for a purpose other than the performance of a contract should be pre-selected to 'off'.[193]

The APP Guidelines endorse a similar approach:

> How broadly a purpose can be described will depend on the circumstances and should be determined on a case-by-case basis. In cases of ambiguity, and with a view to protecting individual privacy, the primary purpose for collection, use or disclosure should be construed narrowly rather than expansively.[194]

The advantage of requiring pro-consumer defaults is that individuals can be confident that when they engage with an entity, their data settings will be addressed in a way that best protects their personal information. This provides an additional protection for individuals who may not be aware of, or taken the time to, adjust their settings to meet their preferences.

The results of the 2020 ACAP survey show that 32 per cent of respondents are more likely to change their default privacy settings after reading an entity's privacy policy. This is more than double the percentage of those who would not make any further changes after reading an entity's privacy policy.[195] This suggests that when people understand how their personal information is being collected, used and disclosed, and are aware of their options for exercising control over their data, that people are more likely to update their settings. The Deloitte Privacy Index 2020 notes that as individuals are placing greater importance on their privacy, "organisations that adopt pro-consumer defaults through singular and express consent should be able to differentiate themselves in the market, likely expanding their commercial presence".[196]

Obtaining consent from children

The Act does not have different requirements for consent where the individual has a limited capacity to understand the implications of that consent, such as children. The DPI report noted that digital platform users often include children who are likely to lack the capacity to understand how their personal information is being collected, used and disclosed. It therefore considered that consent to collect the personal information of children by entities must be obtained from the child's guardian. [197] Given the impracticability of requiring a guardian to provide consent or the ability for such a requirement to be circumvented in an online setting, the DPI report recommended that additional requirements regulating children's interaction with digital platforms be addressed in an online privacy code of practice (recommendation 18). This is being progressed by the Government separate to this review.

However, as the review is considering the role of consent for the protection of privacy economy-wide, it is necessary to consider whether additional privacy protections in relation to children should apply to all APP entities.

Consent fatigue

Strengthening consent requirements may result in an increased burden on individuals to make more decisions about whether they should agree to an entity collecting, using and disclosing their personal

[193] ACCC, *Digital Platforms Inquiry* (n 1) 468.
[194] OAIC, *Australian Privacy Principles Guidelines* (n 31) B.101.
[195] OAIC, *Australian Community Attitudes to Privacy Survey 2020* (n 11) 73.
[196] Deloitte, *Opting-in to meaningful consent:* *Deloitte Australian Privacy Index 2020* (n 15).
[197] ACCC, *Digital Platforms Inquiry* (n 1) 468.

information in different ways. Individuals may also be affected by longer administrative processes when signing up for products or services.

The DPI report considered options to address this risk of consent fatigue and suggested that:

- Consumers only be required to provide consent where the entity is intending to collect personal information that falls outside of a contract to which the consumer is a party
- Using standardised icons or phrases to facilitate consumers comprehension and decision-making
- Supplementing consent with a higher standard of protections to shift some of the burden for management of personal information from consumers to the entities collecting their personal information.[198]

Inferred sensitive information

Entities must collect personal information about an individual from that individual unless it is unreasonable or impracticable to do so.[199] In relation to sensitive information, an entity must obtain the individual's consent unless a specified exception applies.[200] With new technologies such as web scraping, which is the automated extraction of data from websites, combined with sophisticated algorithms, there are likely to be scenarios where entities are generating inferred personal information, including sensitive information.

The APP Guidelines anticipate that APP entities may generate personal information and considers that such a practice constitutes collection of that personal information.[201] Where an entity generates inferred sensitive information about an individual with whom the entity has no relationship or ability to contact, sensitive information is being collected in circumstances where it is impossible to obtain the individual's consent.

As sensitive information is becoming easier to generate from other information, it is desirable to consider whether there are certain activities that should be completely prohibited without the direct express consent of the individual.

Consent in relation to Internet of Things

The Internet of Things (IoT) can be described as devices through which the "internet extends into the real world including everyday objects. Physical elements are no longer disconnected from the virtual world, but can be controlled remotely and serve as physical access points to internet services."[202] This extends to wearable devices including fitness trackers, and smart-home devices such as virtual assistants.

IoT devices can collect a broad range of personal information, including from multiple people, some of whom may not have consented to, or even realise, that their information is being collected. This may occur, for example, with a virtual assistant in a household in relation to other members of the

[198] Ibid 35.
[199] Privacy Act (n 16) sch 1, cl 3.6.
[200] Ibid sch 1, cl 3.3.
[201] OAIC, *Australian Privacy Principles Guidelines* (n 31) B.28.
[202] Chahid Yassine, Benabdellah Mohammed and Abdelmalek Azizi 'Internet of things security' Paper presented at the International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), 2017.

household, or visitors. It is widely expected that the IoT industry will continue to expand rapidly, and that this will lead to a dramatic increase in data collected and generated by IoT devices.[203]

In September 2020, the Australian Government released the voluntary code of practice 'Securing the Internet of Things for Consumers".[204] Principle 5 – ensure personal data is protected - states that "Personal data should only be collected if necessary for the operation of the device, and privacy settings on a device should be set to privacy protective by default."[205]

A recent issues paper by the Office of the Victorian Information Commissioner on the interaction of IoT devices and privacy concluded that "traditional methods used to protect privacy and better inform individuals about how their personal information is collected, used and disclosed are largely incompatible or insufficient for IoT devices."[206] This has significant privacy implications, particularly given the increasing collection and generation by IoT devices of sensitive information, such as health information.

Use of personal information for direct marketing

The APPs set out specific requirements where personal information is used for direct marketing purposes. The APP Guidelines suggest that direct marketing may be interpreted as being as broad as "displaying an advertisement on a social media site that an individual is logged into, using personal information, including data collected by cookies relating to websites the individual has viewed".[207]

APP 7 requires that an entity must not use or disclose personal information for the purpose of direct marketing unless the individual has consented to such use and the individual must be provided with a simple means of opting out of direct marketing that uses their personal information. The DPI report noted that because of the intertwined nature of consents through the use of terms of service, multiple primary purposes, and 'click-wrap' agreements which bundle together multiple consents, it is often difficult for individuals to be able to understand how their personal information is being used to market products or services to them, and subsequently, are unable to make informed decisions about whether they agree to acts or practices by the entity that result in direct marketing to that individual.[208]

Additionally, under APP 7, entities may use or disclose individuals' personal information to a third party for direct marketing by the third party where the information has been obtained from someone other than the individual to whom the information relates and it is impracticable to obtain the individual's consent. While there are requirements for entities to provide details to individuals in relation to how to opt out of further marketing from that entity, this may be burdensome on the individual, particularly if their personal information has been disclosed to multiple entities.

Withdrawal of consent

The APP Guidelines state that consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely. It is good practice to inform the individual of the period for which

[203] Office of the Victorian Information Commissioner, *The Internet of Things and Privacy* (Issues Paper, February 2020) 3.
[204]Australian Government, *Code of Practice: Securing the Internet of Things for Consumers* (Web Page, accessed on 14 September 2020).
[205] Ibid 5.
[206] Ibid 11.
[207] OAIC, *Australian Privacy Principles Guidelines* (n 31) 7.11.
[208] ACCC, *Digital Platforms Inquiry* (n 1) 465.

the consent will be relied on in the absence of a material change of circumstances. They further state that if the consent did not cover a proposed use or disclosure, an entity should seek the individual's consent at the time of the use or disclosure.[209]

The APP Guidelines state that an individual may withdraw their consent and this should be an easy and accessible process. However, an individual often has limited opportunity to reconsider their initial consent given, with implications for an individual's privacy where their information is subsequently used or disclosed for purposes the individual may not have envisaged at the time they gave their consent.

Use of personal information in responses to an emergency or disaster

An emergency declaration allows entities to collect, use and disclose personal information without the consent of individuals where the purpose for that handling is to respond to the emergency or disaster. The power to make an emergency declaration was inserted into the Act in 2006 in response to the 2004 Indian Ocean earthquake and tsunami.[210] The Explanatory Memorandum to the Bill inserting the emergency declaration provisions stated that:

> "Part VIA establishes a clear and certain legal basis for the management of the collection, use and disclosure of personal information about deceased, injured and missing individuals involved in an emergency or disaster, whether it occurs in Australia or overseas… [and] places beyond doubt the capacity of the Australian Government and others to lawfully exchange personal information in an emergency or disaster situation. Part VIA ensures that agencies make clear and timely decisions on information exchange in order to deliver necessary services to victims of tragedies".[211]

Emergency declarations have been used three times since the provisions were inserted into the Act, each time was in response to a natural disaster. The most recent declaration was in January 2020 to facilitate the response to the Australia bushfires in the summer of 2019-20.

Where an emergency declaration is made, regulated entities may collect, use or disclose personal information for a permitted purpose in relation to the emergency or disaster where the entity reasonably believes that the individual may be involved in the emergency or disaster. A 'permitted purpose' is one that directly relates to the Commonwealth's response to the declared emergency or disaster.[212] Disclosure of personal information by an agency or organisation under these provisions is limited to certain entities and individuals.[213]

There are some limitations with the current emergency declaration provisions. For example, an emergency declaration cannot be restricted in its application to specific acts or practices. In addition, the provisions currently facilitate disclosure of personal information to a state or territory authority by a Commonwealth agency, but not by an organisation.[214]

Regulating use and disclosure

In light of the challenges in relation to individuals' capacity to freely provide informed consent it is useful to consider whether there is a role for enhanced protections in relation to the use and disclosure of personal information that do not rely on consent.

---

[209] OAIC, *Australian Privacy Principles Guidelines* (n 31) B.51.
[210] *Privacy Legislation Amendment (Emergencies and Disasters) Act* 2006 (Cth).
[211] Ibid.
[212] Privacy Act (n 16) s 80H.
[213] Ibid s 80P.
[214] Ibid.

This concept was considered in a 2016 discussion paper by the Canadian privacy regulator in relation to the Canadian privacy framework which, like Australia's, features consent as a central component of its model.[215] The paper considered that there may be a role for accountability mechanisms that have broader notions of fairness and ethics in the assessment of proposed uses of personal information as a way to supplement, or in some circumstances, substitute consent.[216]

Similarly, the Consultative Group to Assist the Poor (CGAP), a global partnership of development organisations focused on financial inclusion of those in poverty, maintains that consent models place an unreasonable burden on low income consumers and suggest that a legitimate purpose test for the use of data; or fiduciary duty owing to those to whom the personal information pertains may be beneficial to protecting the interests of individuals.[217]

A requirement on entities to act fairly exists currently within the APPs. APP 3.5 requires that APP entities must collect personal information only by 'lawful and fair means'.[218] The APP Guidelines state that 'fair means' depend on the circumstances, and that it would usually be 'unfair to collect personal information covertly without the knowledge of the individual'.[219]

While there is no similar obligation in relation to use and disclosure, it is useful to consider whether the Act should place greater obligations on entities to handle personal information in a manner which is consistent with the interests of the individual, particularly in relation to those who may have vulnerabilities which limit their ability to provide meaningful consent.

The Canadian privacy regulator also describes as 'no-go zones' certain acts or practices that are so contrary to the individual or public interest that they should be designated.[220] Such uses would be prohibited based on a variety of criteria, including the sensitivity of the type of data, the nature of the proposed use or disclosure, or vulnerabilities associated with the class of person whose personal information was being used or disclosed.[221] This could be supplemented with 'proceed with caution zones', or enhanced protections for certain categories of information, or acts or practices that pose a high risk to privacy. This is already the case in Australia in relation to sensitive information, and to an extent, certain activities such as direct marketing.

Issues for comment

Consent to collection, use and disclosure of personal information

26. Is consent an effective way for people to manage their personal information?
27. What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?
28. Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?

---

[215] Office of the Privacy Commissioner of Canada, *A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act* (Discussion Paper, May 2016).
[216] Ibid 10.
[217] Consultative Group to Assist the Poor, *Making Data Work for the Poor: New Approaches to Data protection and Privacy* (Report, January 2020).
[218] Privacy Act (n 16) sch 1, cl 3.5.
[219] OAIC, *Australian Privacy Principles Guidelines* (n 31) 3.60.
[220] Office of the Privacy Commissioner of Canada, *A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act* (n 215) 17.
[221] Ibid.

29. Are the existing protections effective to stop the unnecessary collection of personal information?
    a. If an individual refuses to consent to their personal information being collected, used or disclosed for a purpose that is not necessary or central to providing the relevant product or service, should that be grounds to deny them access to that product or service?
30. What requirements should be considered to manage 'consent fatigue' of individuals?

Exceptions to the requirement to obtain consent

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

Pro-consumer defaults

32. Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?

Obtaining consent from children

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

The role of consent for IoT devices and emerging technologies

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

Inferred sensitive information

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

Direct marketing

37. Does the Act strike the right balance between the use of personal information in relation to direct marketing? If not, how could protections for individuals be improved?

Withdrawal of consent

38. Should entities be required to refresh an individual's consent on a regular basis? If so, how would this best be achieved?
39. Should entities be required to expressly provide individuals with the option of withdrawing consent?
40. Should there be some acts or practices that are prohibited regardless of consent?

Emergency declarations

41. Is an emergency declaration appropriately framed to facilitate the sharing of information in response to an emergency or disaster and protect the privacy of individuals?

Regulating use and disclosure

42. Should reforms be considered to restrict uses and disclosures of personal information? If so, how should any reforms be balanced to ensure that they do not have an undue impact on the legitimate uses of personal information by entities?

Control and security of personal information

The proliferation of digital services is rapidly expanding the amount of data and personal information collected in return for the use of those services. Yet once 'consent' is given, individuals can have little say in how their information is subsequently used. 87 per cent of respondents to the 2020 ACAP survey indicated they want more control and choice over the collection and use of their personal information. In line with this, 84 per cent of respondents believe they should have the right to ask a business to delete their personal information and 64 per cent believe they should have the right to ask a government agency to delete their personal information.[222]

The current law

Security of personal information

APP 11 requires APP entities that collect or hold personal information to protect it from misuse, interference, loss, unauthorised access, modification or disclosure. The purpose of these security requirements is to ensure APP entities take reasonable and appropriate measures to protect personal information held by the entity.

APP 11 requires that APP entities take such steps as are reasonable in the circumstances. The OAIC APP Guidelines provide that this allows the requirement to be scalable to reflect the entity's 'size, resources, the complexity of its operations and its business model'.[223] The entity should also take account of the 'amount and sensitivity of information held'.[224] There are no specific requirements as to how specific types or classes of information should be protected.

Adequate security of personal information is important for a number of reasons. Proper security measures can reduce instances of identity fraud and scams that expose individuals to reputational damage, emotional distress and financial loss. Data breaches also impact the organisations involved through the costs of remedial measures, legal action, reputational damage and loss of consumer trust and confidence.[225]

Retention of personal information

APP 11 also sets out obligations which apply when it is no longer appropriate for an entity to retain personal information. Entities are required to destroy or de-identify personal information if the entity no longer needs the information for any purposes for which the information may be used or disclosed under the APPs.

Given the broad interpretation of primary and secondary purposes for collection of personal information, there are no strict requirements on entities to delete personal information after an individual ceases or concludes interactions with that entity as a secondary use for that information may continue to apply under the APPs. While an individual may withhold consent in relation to the collection of any further personal information, beyond the requirements of APP 11, this does not impact an entity's obligations in relation to personal information that the entity already holds.

---

[222] OAIC, *Australian Community Attitudes to Privacy Survey 2020* (n 11) 7.
[223] OAIC, *Australian Privacy Principles Guidelines* (n 31) 11.7.
[224] Ibid.
[225] ACCC, *Digital Platforms Inquiry* (n 1) 444.

Access to, and correction of personal information

For individuals to make informed decisions about their interaction with entities, they need to be able to understand what data an entity holds about them. This is particularly relevant with technological advances that allow entities to derive or aggregate data to generate inferred personal information about an individual. APP 12 requires entities to give individuals access to their personal information upon request, subject to certain exceptions.

Under APP 13, entities have an ongoing obligation to take reasonable steps to ensure that personal information collected, used or disclosed is accurate, up-to-date and complete. An individual may make a request to have their own personal information corrected under this principle. APP 13 overlaps with APP 10, which requires APP entities to take reasonable steps to ensure the personal information it collects, uses or discloses is accurate, up to date and complete.

ACCC Digital Platform Inquiry Final Report

The DPI report recommended that entities should be required to 'erase the personal information of a consumer without undue delay on receiving a request for erasure from the consumer, unless the retention of 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'.[226]

The ACCC's stated rationale for this recommendation is that it would give consumers greater control over their personal information and help mitigate the bargaining power imbalance between consumers and digital platforms.[227] It considered that a right of erasure is a critical complement to strengthened consent requirements by providing consumers with a mechanism for withdrawing their consent if they are no longer comfortable with an APP entity collecting, using or sharing their personal information.[228]

The ACCC noted that such a requirement is supported by the existing right to access personal information under APP 12. The ALRC has also noted that the Information Commissioner already has the power to issue declarations to require APP entities to take certain steps which may include deleting, removing or de-identifying personal information.[229] The DPI report did not recommend the introduction of a mandatory deletion obligation once data is no longer necessary. It considered that such a duty could create a significant regulatory burden and would be unreasonably onerous for small businesses that only partially operate in the digital space.[230]

Key issues

Countervailing public interest considerations

The ACCC proposed that a right to erasure should not override existing obligations to retain personal information for legal reasons, such as industry-specific laws, tax requirements, healthcare purposes and law enforcement requirements.[231] The ACCC also indicated that it would not apply to small businesses exempted from the Act. The right would also be counterbalanced by any competing

[226] Ibid 470.
[227] Ibid 471.
[228] Ibid 472.
[229] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report No 123, September 2014) 313.
[230] ACCC, *Digital Platforms Inquiry* (n 1) 473.
[231] Ibid 472.

public interest reasons, which could include matters such as freedom of speech, freedom of the media, public health and safety, and national security.[232] For example, it would not be in the public interest for personal information in online chat logs containing evidence of the grooming of children to be erased such that law enforcement could not investigate or prosecute that activity.

Another consideration is whether a right to erasure could negatively impact freedom of expression and the free flow of information. The ALRC has warned that such a mechanism may have an 'undesirably chilling effect' on freedom of expression if the interests of the person requesting erasure are not properly balanced against broader public interests.[233] Others highlight that the potential for this impact depends on the framing of the right, noting it is minimal where the right can only be exercised in limited and justified circumstances, such as when the information is outdated, irrelevant or when a person withdraws consent for data to be published.[234]

International examples of a right to erasure

Article 17 of the GDPR provides EU citizens with a right to erasure of their personal data without undue delay in various circumstances, including where it is no longer necessary for the purpose for which it was originally collected and processed, the data subject has withdrawn consent where consent is the basis for the data being held, or there is no overriding legitimate interest in the continued processing of the data.[235] This is also known as the 'right to be forgotten'.[236] The requirement applies to commercial data but not to information used for journalistic purposes; academic, artistic or literary expression; or statistical, scientific or historical research purposes.[237] Commercial entities do not have to comply with a request for erasure under all circumstances.[238]

In recent privacy reforms overseas, a 'right to erasure' has not been implemented consistently. The UK has enacted a right of erasure consistent with the GDPR in the UK *Data Protection Act 2018*. However neither Canada[239] nor New Zealand[240] have an equivalent law. In California, the CCPA allows consumers to request that businesses delete personal information collected directly from the consumer subject to various exceptions – a more limited right than that afforded by the GDPR.[241]

Questions

Security and retention

43. Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?
44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?

---

[232] Ibid.
[233] ALRC, *Serious Invasions of Privacy in the Digital Era* (n 229) 313.
[234] Eugenia Georgiades, 'Down the rabbit hole: Applying right to be forgotten to personal images uploaded on social networks' (2020) 30(4) *Fordham Intellectual Property, Media & Entertainment Law Journal* 1133.
[235] General Data Protection Regulation (n 39) art 17.
[236] Information Commissioner's Office (UK), *Right to Erasure* (Web Page, accessed 2 October 2020).
[237] Alexander Tsesis, 'Data subjects' privacy rights: Regulation of personal data retention and erasure' (2019) 90(2) *University of Colorado Law Review* 604.
[238] General Data Protection Regulation (n 39) art 17.
[239] In 2018, the Office of the Privacy Commissioner of Canada released a draft position supporting the introduction of similar provisions however this has not yet occurred. See, Office of the Privacy Commissioner of Canada, *Draft OPC Position on Online Reputation* (Web Page, 26 January 2018).
[240] New Zealand's *Privacy Act 2020* will come into effect from 1 December 2020 and does not have provisions resembling a right to erasure. See New Zealand Ministry of Justice, *Privacy* (Web Page, 1 July 2020).
[241] *California Consumer Privacy Act of 2018* (California) 178.105.

Access, quality and correction

45. Should amendments be made to the Act to enhance:
    a. transparency to individuals about what personal information is being collected and used by entities?
    b. the ability for personal information to be kept up to date or corrected?

Right to erasure

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

Overseas data flows

Overseas (or cross-border) data flows refer to the movement of data (including personal information) across national borders. Cross-border flow of information is an increasingly important component of international trade and digital service models.[242] By some estimates, cross-border data flows contribute $2.8 trillion (USD) to global economic activity.[243] There is growing uncertainty from individuals about how their personal information is being used.[244] As a result, consumers are increasingly asking for assurances that their data is being handled appropriately.[245] The 2020 ACAP survey results showed that 92 per cent of respondents were concerned about their personal information being sent overseas and 41 per cent thought that sending personal information overseas was one of the biggest privacy risks.[246]

There is currently no single global standard to regulate cross-border data flows. The EU and the APEC have adopted frameworks aimed at facilitating the cross-border flow of information between members while upholding privacy protections. The APEC CBPR system certifies the information handling practices of businesses that voluntarily opt into the scheme. Australia's participation in the CBPR system was endorsed by APEC in late 2018, although the system has not yet been implemented domestically. The EU GDPR, which applies to all member states, aims to give individuals' control of their personal data and to simplify the regulatory environment for businesses offering goods or services or monitoring the behaviour of persons in the EU.

The Act implements a system for dealing with cross-border data flows through APP 8 and section 16C. It also regulates acts or practices engaged in overseas by agencies and organisations with an 'Australian link' through the extra-territorial operation of the Act.[247] The DPI report recommended reforming the Act with regard to whether it should be revised to facilitate the flow of information to and from overseas jurisdictions such as the EU, and whether an independent privacy certification scheme should be introduced.[248]

The accountability approach

The aim of APP 8 and section 16C is to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected.[249] When APP 8 was adopted, there were two internationally accepted approaches to dealing with cross border data flows: the adequacy approach, adopted by the EU in the Data Protection Directive of 1995 and carried through to the GDPR, and the accountability approach, adopted by the APEC Privacy Framework in 2004 and carried through to the CBPR.[250] Prior to the introduction of APP 8, cross border data flows were prohibited

[242] W Gregory Vodd, 'Cross-border data flows, the GDPR, and data governance' (2020) 29 *Washington International Law Journal* 485.
[243] McKinsey Global Institute, *Digital globalization: the new era of global flows* (March 2016) 10.
[244] Office of the Australian Information Commissioner, *OAIC international strategy* (March 2020) 2.
[245] Francesca Casalini and Javier Lopez Gonzalez, 'Trade and cross-border data flows' (2019) 220 *OECD Trade Policy Papers* 6.
[246] OAIC, *Australian Community Attitudes to Privacy Survey 2020* (n 11) 39.
[247] Privacy Act (n 16) s 5B(1)-(1A). For the purposes of this paper 'overseas' means outside Australia and the external territories.
[248] ACCC, *Digital Platforms Inquiry* (n 1) 476.
[249] Privacy Act (n 16) s 2A(f).
[250] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 70; Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (Report, August 2017) 22.

unless there were adequate protections in place.[251] The Act was subsequently amended to adopt the accountability approach, consistent with the APEC Privacy Framework.[252]

Liability for acts of overseas recipient

APP 8.1 provides that before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.[253] What are 'reasonable steps' will depend on the circumstances and may include requiring an overseas entity to enter into contractual obligations and monitoring compliance with any contract.[254]

When an APP entity discloses personal information to an overseas recipient, the entity must also comply with APP 6 and must only disclose the personal information for the primary purpose for which it was collected unless a legislative exception applies.[255] The aim of APP 8 is to permit cross-border disclosure of personal information and to ensure any information that is disclosed is treated in accordance with the Act.[256]

Section 16C provides that an APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs. That is, the act or practice engaged in by the overseas recipient that would be a breach of the APPs is taken to have been done by the APP entity and to be a breach of the APPs by the APP entity.[257]

Under the accountability approach, an APP entity may be liable for the acts or practices of the overseas recipient, and an individual will have a means of redress, even where the entity took reasonable steps to ensure the overseas recipient complies with the APPs, although any steps may be taken into account as mitigation for the breach.[258]

Obligations apply only to 'disclosures'

APP 8 explicitly adopts the term 'disclosure' rather than 'transfer' or 'use'. 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.[259] APP 8 is not intended to apply where personal information is routed through servers outside Australia. However, entities are still required 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.[260]

The chain of accountability for APP entities is not broken by an overseas entity engaging a subcontractor. The requirements of APP 8 will still apply where an organisation contracts a function to an overseas entity, and that overseas entity then engages a subcontractor. In practice, the

[251] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 70.
[252] Ibid.
[253] Privacy Act (n 16) sch 1 cl 8.1. Note APP 8.1 refers to a breach of the APPs with the exception of APP 1.
[254] OAIC, *Australian Privacy Principles Guidelines* (n 31) 8.17.
[255] Ibid 8.4.
[256] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 83.
[257] Privacy Act (n 16) s 16C.
[258] OAIC, *Australian Privacy Principles Guidelines* (n 31) 8.58.
[259] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 83.
[260] Ibid.

concept of taking 'such steps as are reasonable in the circumstances' will usually require an entity to enter into a contractual relationship with the overseas recipient.[261]

Where an APP entity engages a contractor located overseas to perform services on its behalf, in most circumstances, the provision of personal information to that contractor is a disclosure. This means that the entity will need to comply with APP 8 before making that disclosure. Where a subcontractor may be engaged, the entity should also take reasonable steps to ensure the subcontractor does not breach the APPs in relation to the personal information.[262]

In limited circumstances, providing personal information to an overseas contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure. This occurs where the entity does not release the subsequent handling of personal information from its effective control. For example, where an APP entity provides personal information to a cloud service provider located overseas for the limited purpose of performing the services of storing and ensuring the entity may access the personal information. [263]

While the Act requires APP entities to take steps to protect personal information they 'disclose' overseas, transfers of personal information that are not 'disclosures' raise questions about privacy. 74 per cent of respondents to the 2020 ACAP survey considered an organisation sending consumers' data to an overseas processing centre to be a misuse of personal information. Questions have also been raised about personal information being transferred and stored overseas. For example, when the Act was amended to implement privacy protections for information collected by the COVIDSafe App, specific provisions were introduced to ensure data was stored within Australia and to prohibit the overseas transfer of COVID app data.[264]

Exception - overseas recipient is subject to substantially similar laws

There are exceptions to the requirement in APP 8.1 to take reasonable steps and to the accountability provision in s 16C. In particular, an APP entity will not be accountable if the disclosing entity reasonably believes that the recipient is subject to a law, or binding scheme, that has the effect of protecting personal information in a way that is substantially similar to the APPs.[265]

When the entity has a reasonable belief that the overseas recipient is subject to legal or binding obligations to protect information in at least a substantially similar way to the protection provided by the APPs, APP 8.1 will not apply. For this exception to apply, there must be accessible mechanisms which allow the individual to enforce those protection obligations.[266]

The requirement on APP entities to determine whether another country's laws are sufficient to attract this exception is an issue which has been raised in previous reviews. Stakeholders, especially small businesses, have criticised the system, arguing that they neither have the expertise or the resources to assess a foreign country's privacy laws'.[267]

---

[261] OAIC, *Australian Privacy Principles Guidelines* (n 31) 8.16.
[262] Ibid 8.12.
[263] Ibid 8.14.
[264] Privacy Act (n 16) s 94F.
[265] Ibid sch 1 cl 8.2(a).
[266] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 83.
[267] Office of the Privacy Commissioner, *Getting in on the Act: the Review of the Private Sector Provisions of the Privacy Act 1988* (n 104) 77.

Countries with substantially similar laws

ALRC Report 108 recommended that the Australian Government develop and publish a list of laws and binding schemes in force outside Australia that provided privacy protections that were substantially similar.[268] The ALRC considered this would assist individuals to make choices based on where their personal information may be transferred, and how it would be handled.[269] The Government response agreed with this recommendation and acknowledged that a Government list of laws and binding schemes outside Australia which were substantially similar to the Act would provide guidance to agencies and organisations.[270]

Standard contractual provisions

The Office of the Privacy Commissioner's review also considered publishing approved standard contractual provisions for use by Australian companies and international trading partners.[271] Contractual provisions could provide details on how the international company must protect information when the information collected in Australia is transferred to organisations overseas.[272] However, the review ultimately decided instead to recommend that further guidance be provided to assist organisations to comply with their obligations.[273]

Extraterritorial application of the Act

The extraterritorial application of the Act is intended to capture multinational corporations based overseas with offices in Australia as well as entities with an online presence (but no physical presence in Australia) that 'carry on business in Australia' and collect or hold personal information of people in Australia.[274] The Act stipulates that an act or practice overseas will not breach an APP or a registered APP code if the act or practice is required by an applicable law of a foreign country and where engaged in by an organisation it will not constitute an interference with an individual's privacy.[275] Where an overseas recipient of personal information does an act or practice that is required by an applicable foreign law, this will not breach the Act and the disclosing entity will not be held accountable.[276]

This exception recognises that in some situations, compliance with the APPs or an APP code overseas may breach a local law or regulation, and in this situation an organisation is not required to comply with the Act to the extent of the conflict. The intention is to ensure that the Act does not require organisations to act in contravention of laws operating in the country in which the act or practice occurs.[277]

In *E v Money Transfer Service*, the Information Commissioner noted that the exception does not authorise the collection of personal information within Australia and its transfer to an overseas

---

[268] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1122.
[269] Ibid.
[270] Australian Government, '*First stage response to the Australian Law Reform Commissioner Report 108*' (2009) 79.
[271] Office of the Privacy Commissioner, *Getting in on the Act: the Review of the Private Sector Provisions of the Privacy Act 1988* (n 104) 78.
[272] Ibid 79.
[273] Ibid 80.
[274] Privacy Act (n 16) s 5B(3). See also *Australian Information Commissioner v Facebook Inc (No 2)* [2020] FCA 1307.
[275] Privacy Act (n 16) ss 6A(4), 6B(4) and 13D.
[276] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 89.
[277] Ibid 71.

country for the purpose of complying with a foreign law.[278] The exception is only applicable where relevant personal information is already located outside Australia and, pursuant to the legal process in the country where it is located, it has to be disclosed to someone in that jurisdiction.[279]

APEC Cross-Border Privacy Rules system

The APEC CBPR System operates as a regional certification scheme and provides a mechanism for governments and business stakeholders to safeguard the free flow of data while protecting the privacy rights of individuals.[280] It requires certified businesses to demonstrate compliance with a commonly understood set of privacy standards, establishing a level of certainty and assurance for the individuals providing their data.[281]

The CBPR is a voluntary certification scheme which assesses personal information handling practices in relation to notice, collection, use, choice, integrity and security of personal information, access and correction and accountability.[282] Entities seeking certification must submit to an audit of their privacy practices and procedures by an APEC-certified Accountability Agent. The scope of the certification is flexible and may be defined by the applying organisation to be broad or narrow. It may cover the operations of an entire organisation, or a particular data type or business process.

Australia's participation in the CBPR system

The APEC Joint Oversight Panel of the Data Privacy Subgroup endorsed Australia's application to participate in the CBPR system in November 2018. In order to implement the CBPR system in Australia, the CBPR program requirements must be incorporated and an Accountability Agent must be appointed.

One way of incorporating the CBPR system requirements is through a Code under Part IIIB of the Act. A Code would operate in addition to the APPs and reconcile how the CBPR program requirements would interact with the APPs.[283] The development of a Code would require a private sector code developer to be identified, who would be responsible for developing the Code in consultation with relevant stakeholders and the OAIC, and for ensuring that effective public consultation also occurs.[284] A Code would set out the class of businesses to be covered by its provisions, which in this case would be businesses with CBPR certification status.

Accountability Agents conduct audits based on the CPBR's Intake Questionnaire and Program Requirements, as well as provide individuals with a cost-effective, accessible dispute resolution mechanism. [285] Under the CBPR, an individual that has a privacy complaint must first contact the CBPR certified business to seek to resolve the matter, but may later escalate the matter to the relevant Accountability Agent or government regulator, respectively. At present there are no Accountability Agents operating in the Australian market. Entities that wish to apply to be an Accountability Agent must complete an Accountability Agent Application which is reviewed by the

[278] *E v Money Transfer Service* [2006] PrivCmrA (1 April 2006).
[279] Ibid.
[280] APEC, *APEC Privacy Framework* (n 250) 30.
[281] Ibid 8.
[282] Asia-Pacific Economic Cooperation, *Cross-Border Privacy Rules System Program Requirements* (Report, November 2019).
[283] Privacy Act (n 16) Part IIIB.
[284] Ibid s 26E.
[285] Asia-Pacific Economic Cooperation, *Cross-Border Privacy Rules System Documents* (Web Page, accessed 1 October 2020).

APEC Joint Oversight Panel, and then sent to the APEC Data Privacy Sub-group for further endorsement.[286] Accountability Agents undergo annual reviews to ensure that they meet ongoing requirements, including that no conflicts of interest exist, that they undertake ongoing monitoring of organisations they have certified, as well as reporting to privacy enforcement authorities.

Participating economies must also have a 'back-stop' regulator that can bring the force of law to the enforcement of breaches.[287] An individual that has a privacy complaint against a CBPR certified business, would first contact the business to seek to resolve the matter. If the individual was not satisfied with the response, they would then be able to contact the relevant Accountability Agent. In the event that a complaint could not be resolved through the Accountability Agent, the dispute could be escalated to the relevant government regulator.

Costs of Certification

An important factor for potential uptake of CBPR is the cost to certify businesses. Costs could vary depending on which Accountability Agency conducts the certification, the size of the organisation to be certified, and scope of the certification. Certifications are granted on a yearly basis, and there may be additional fees to maintain the certification on an ongoing basis.

Japan's Accountability Agency, JIPDEC, currently charges an average of $AU8,700 for the initial certification audit. JIPDEC also charges for an annual certification management fee, which is dependent on the certified entity's yearly revenue. Singapore's IMDA charges an initial application fee of ~$AU550, and additional assessment fees are paid to the relevant Assessment Body that conducts the audit, which may range from ~$AU1,000 to ~$AU8,000.

Domestic privacy certification schemes

Some participating economies in the CBPR system maintain a domestic certification alongside the CBPR, including Singapore's Data Protection Trustmark Certification and Japan's PrivacyMark. Beyond facilitating overseas transfers of personal information, privacy certification schemes can enhance consumer trust in the collection, use and storage of personal information.

The ACCC noted the benefit of privacy certifications in the DPI report as a mechanism that '…seeks to address issues arising from consumers not reading or being able to understand digital platforms' privacy policies by outsourcing the potentially complex and time-consuming assessment to a qualified and independent third-party'.[288]

Certifications may also provide benefits for APP entities including improving their privacy practices, procedures and systems, streamlining compliance requirements and providing them with the competitive advantage of being a privacy-respecting choice for consumers and businesses. [289]

[286] Asia-Pacific Economic Cooperation, *Accountability Agent APEC Recognition Application* (November 2019).
[287] APEC, *Cross-Border Privacy Rules System Program Requirements* (n 282).
[288] ACCC, *Digital Platforms Inquiry* (n 1) 480.
[289] For example, Japan's Privacy Mark is often a prerequisite for the awarding of government contracts. More broadly, privacy and information security certifications can provide assurances for commercial business partners in a vendor selection process.

Australian privacy certification scheme proposals

In 2000, the Senate Select Committee on Information Technologies recommended that the Federal Privacy Commissioner develop a privacy webseal as a consumer empowerment measure.[290] In its Report 108, the ALRC proposed that the concept of a privacy trustmark in Australia should be explored further, but found that it was premature without further consideration of how it could be implemented.[291]

Key issues for any Australian certification scheme

Developing a privacy certification scheme requires consideration of whether criteria should be based on regional standards, such as the requirements of the CBPR or standards that have been developed by a private standard-setting organisation.[292]

Another consideration is the extent to which a certification scheme could operate consistently with existing accreditations in Australia that incorporate privacy safeguard requirements, such as the Consumer Data Right and the proposed Data Availability and Transparency scheme. A privacy certification ought to be interoperable with existing Australian accreditations to the extent possible, in order to minimise the fragmentation of privacy certifications and accreditations for which regulated entities may wish to apply.

A further consideration is whether any certification scheme should be voluntary or mandatory. Generally, voluntary certifications rely on businesses having an incentive to seek certification in order to establish a competitive advantage as a compliant and trusted handler of personal information. Internationally, most existing privacy certifications are voluntary, including the CBPR and the GDPR's data protection certification scheme.

General Data Protection Regulation

The objectives of the GDPR are to harmonise and strengthen privacy laws across the EU. The GDPR was introduced in response to growing concerns from the public and regulators that many companies were not doing enough to protect customers' personal information.[293] Under the GDPR, individuals are given rights to manage how their data is collected, used and shared. European regulators, known as data protection authorities have strong enforcement powers, including the power to sanction companies with fines of up to 20 million Euros or 4 per cent of annual worldwide revenue for serious contraventions.[294]

Under the GDPR, personal data can only be transferred outside the EU to countries or organisations that provide an adequate level of privacy protection.[295] Unlike the Australian approach, which

---

[290] Senate Select Committee on Information Technologies, Parliament of Australia, *Cookie Monsters? Privacy in the Information Society* (Report, November 2000), 123-4 [5.125]-[5.143].
[291] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1079.
[292] Privacy certifications established and administered by private-sector bodies include the International Organisation for Standardization, British Standards Institution and the Japanese Industrial Standards.
[293] Elizabeth Englezos, 'A new world standard? Why Australian businesses should be ensuring their compliance with the EU 'General Data Protection Regulation'' (2019) 115 *Intellectual Property Forum: Journal of the Intellectual Property Society of Australia and New Zealand* 39.
[294] Ibid.
[295] General Data Protection Regulation (n 39) art 45.

requires entities to determine if a potential recipient has appropriate privacy protections in place, the European Commission (EC) designates which countries provide adequate protections.[296]

In the absence of an adequacy decision, overseas transfers of personal data are permitted on the condition that individual rights under the GDPR are enforceable and effective remedies are available.[297] In addition, the transferring entity is required to comply with Article 46, which outlines the safeguards that must be in place when transferring personal information to a non-white listed country, such as Australia.

Australian businesses and the GDPR

When the Act was extended to the private sector in 2000, the intention was to facilitate trade with European countries by having the privacy protections in the Act deemed adequate for the purposes of the former EU Directive.[298] Following the introduction of the private sector reforms, the EU released an opinion expressing concern about the sectors and activities excluded from the protection of the Act and mentioned, in particular, the small business and employee records exemptions.[299] In evidence to the Senate Legal and Constitutional References Committee, it was 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.[300]

When does an Australian business need to comply with the GDPR

The GDPR has broad extraterritorial application and captures the activities of businesses without an establishment in the EU if the business either offers goods or services to persons in the European Economic Area, or monitors the behaviour of persons in the EU.[301] Australian businesses may also be required to comply with the GDPR indirectly when entering into agreements with overseas entities that are subject to the GDPR. An overseas entity may seek a commitment from an Australian business to comply with the GDPR to help ensure the overseas entity's own compliance.[302]

The use of contracts for compliance with the GDPR

Article 46 of the GDPR recognises that contracts may be one method of ensuring personal data transferred outside the EU receives adequate protection.[303] As Australia's privacy laws are not recognised as adequate by the EU, Australian businesses that wish to trade with organisations in the EU bear the costs of additional contractual arrangements, including the costs of periodic audits of compliance with these arrangements.[304] Businesses bound by both the Act and the GDPR may be required to navigate inconsistent privacy protections that are applied to the same collection, use or

---

[296] Ibid art 45.
[297] Ibid art 46.
[298] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 14.
[299] 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).
[300] 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).
[301] General Data Protection Regulation (n 39) art 3. 'Monitor' includes activities such as behavioural advertising, profiling, surveillance and tracking through cookies and other technologies that involve personal data: Englezos (n 294); Michael Rustad and Thomas Koenig, 'Towards a global data privacy standard' (2019) 71(2) *Florida Law Review* 365.
[302] Englezos (n 294) 39.
[303] General Data Protection Regulation (n 39) art 46.
[304] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1329.

disclosure of personal information. For example, if an entity experiences a breach of a dataset containing personal information of both EU and non-EU residents, the entity will be required to comply with both the NDB Scheme as well as the GDPR notification requirements.[305]

Is EU adequacy necessary or desirable?

The DPI Report recommended that reforms to the Act have regard to whether revisions to the Act should be made such that it could be considered by the EC to offer 'an adequate level of data protection' to facilitate the flow of information to and from overseas jurisdictions such as the EU.[306]

Of Australia's top 15 two-way trading partners in goods and services (2016-17), 12 were from the APEC region and only two were from the EU (UK, Germany). During that period, APEC economies accounted for 72 per cent of total trade, while the EU accounted for 13.5 per cent.[307] As less trade is undertaken with the EU than within the APEC region, the Government's recent priority has been to ensure adequate privacy protections within and between APEC economies. Requiring businesses to comply with different information handling requirements under the Act, CBPR and GDPR could result in a regulatory landscape that is overly complex. On the other hand, compliance with the GDPR may give businesses a competitive advantage in engendering consumer trust.[308]

Questions

48. What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information?
    a. Are APP8 and section 16C still appropriately framed?
49. Is the exception to extraterritorial application of the Act in relation to acts or practices required by an applicable foreign law still appropriate?
50. What (if any) are the challenges of implementing the CBPR system in Australia?
51. What would be the benefits of developing a domestic privacy certification scheme, in addition to implementing the CBPR system?
52. What would be the benefits or disadvantages of Australia seeking adequacy under the GDPR?

[305] Under the NDB Scheme an APP entity must notify both the Commissioner and individuals affected if the threshold for notification is met. Under the GDPR, an entity must notify the relevant authority of all breaches and will be required to notify affected individuals when the requisite threshold is met. The degree of harm which triggers notification obligations under the NDB Scheme is higher than under the GDPR: Caitlin Surman, 'Juggling act: Extraterritorial application of the GDPR, and managing concurrent data breach notification obligations under the GDPR and Australian 'Privacy Act'' (2019) 16(5) *Privacy Law Bulletin* 91.
[306] ACCC, *Digital Platforms Inquiry* (n 1) 443.
[307] Australian Government Department of Foreign Affairs and Trade, *Trade in goods and services* (Web Page, accessed 1 October 2020).
[308] Rustad and Koenig (n 301) 365.

Regulation and enforcement

Enforcement powers under the Privacy Act and role of the OAIC

The Commissioner is responsible for enforcing compliance with the Act. The Commissioner can do this by investigating and resolving complaints about instances of non-compliance by entities, or by self-initiating an investigation into an act or practice of an entity.[309]

The current Australian law

Complaints and conciliation

The current framework of the Act places a strong emphasis on the Commissioner to attempt to resolve complaints by conciliation and, failing that, make binding determinations against entities including determinations for compensation and costs.[310] If the Commissioner considers it is reasonably possible that the complaint may be conciliated successfully, the Commissioner *must* make a reasonable attempt to conciliate the complaint.[311] The main remedies agreed in conciliated privacy complaints in 2018-19 were:

1. record amended
2. access provided
3. other or confidential
4. apology
5. compensation
6. changed procedures, and
7. staff training or counselling.[312]

Where compensation was awarded, the majority of awards were within the $1,000 - $5,000 range with only nine award amounts being over $10,001.[313]

The OAIC introduced an early resolution process in 2017-18 under which an Early Resolution team assess whether a resolution can be achieved between the parties soon after the complaint is lodged.[314] The Early Resolution team finalised 64.5 per cent of privacy complaints in 2018-19. It is only when the OAIC is unable to resolve a privacy complaint through the early resolution process that they make further inquiries and conciliate and/or investigate the matter.[315]

The OAIC received 3,306 privacy complaints in the 2018-19 financial year.[316] The average time it took for the OAIC to finalise each complaint (either through early resolution, conciliation or investigation and determination) was 4.4 months with 95 per cent of complaints being finalised within 12 months.

---

[309] Privacy Act (n 16) ss 36, 40(2).
[310] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1626.
[311] Privacy Act (n 16) s 40A(1).
[312] Office of the Australian Information Commissioner, *Annual Report 2018–19* (Report, 12 September 2019) 161.
[313] Ibid.
[314] Ibid 57.
[315] Ibid.
[316] Ibid 12.

Commissioner initiated investigations

The Commissioner has the power to investigate an act or practice that may be an interference with privacy on the Commissioner's own initiative. The Information Commissioner uses this power to respond to more systemic issues, where there has been an incident of significant community concern or discussion, or notification from a third party about a potentially serious privacy issue, rather than a direct response to an individual privacy complaint.[317]

In the 2018-19 financial year, the Commissioner initiated preliminary inquiries and/or investigations in relation to 15 matters. As at 30 June 2019, 10 of these matters and 12 matters from 2017-18 were ongoing.[318]

Investigations

When conducting investigations, the Commissioner has powers:

- to conciliate complaints;
- to make preliminary inquiries of any person;
- to require a person to give information or documents or to attend a compulsory conference; and
- to transfer matters to an alternative complaint body in certain circumstances.[319]

During the investigation, the Commissioner can compel the complainant, respondent and any other relevant person to attend a conference.[320] The Commissioner also has the power to obtain information and documents from persons and make inquiries of persons or examine witnesses on oath or affirmation.[321] It is an offence not to comply with the Commissioner's directions to attend or give information.[322]

During an investigation, the Commissioner is generally required to hold a hearing prior to making a determination unless the matter can be adequately determined in the absence of the parties, the circumstances do not warrant one, and neither party has requested a hearing.[323]

Following an investigation, a complaint will either be sent to conciliation or the Commissioner will make a determination either dismissing the complaint or finding the complaint substantiated.[324]

Determinations

The Commissioner has the power to make a determination after investigating a complaint or after a self-initiated investigation.[325] The determination can include a declaration that:

- the respondent (or person or entity) has engaged in conduct constituting (or an act or practice is) an interference with the privacy of an individual;
- the respondent (or person or entity) must take specified steps to ensure such conduct is not repeated or continued;

---

[317] Ibid 65.
[318] Ibid.
[319] Privacy Act (n 16) s 36A.
[320] Ibid s 46(1).
[321] Ibid ss 44-46.
[322] Ibid ss 46(2), 65-66.
[323] Ibid s 43(4).
[324] Ibid s 40A, 52.
[325] Ibid s 52.

- the respondent (or person or entity) should perform certain acts to redress any loss or damage suffered by the complainant;
- the complainant (or affected individual) is entitled to a specified amount of compensation; or
- that is would be inappropriate for any further action to be taken in the matter.[326]

Complainants or the Commissioner may apply to the Federal Court or the Federal Circuit Court for an order enforcing a determination made by the Commissioner.[327] There is currently no requirement for the Commissioner to make a determination where a complaint is not resolved by conciliation, nor is there a right of a party to require a determination in such circumstances. The Commissioner is also not obliged to make a determination after a Commissioner initiated investigation.[328]

In 2018-19, the Commissioner made three privacy determinations under s 52 of the Act.[329]

Civil penalty provisions – 'serious or repeated interferences with privacy

Section 80U of the Act empowers the Commissioner to apply to the Federal Court or Federal Circuit Court for an order that an entity, that is alleged to have contravened a civil penalty provision in that Act, pay the Commonwealth a penalty.

Importantly, under section 13G of the Act, an entity is liable for a civil penalty for either:

- engaging in an act or practice that is a serious interference with the privacy of an individual, or
- repeatedly engaging in an act or practice that is an interference with the privacy of one or more individuals.

Section 13G was inserted into the Act in 2012 to implement the Government's response to a recommendation from ALRC Report 108.

On 9 March 2020, the Commissioner lodged proceedings against Facebook in the Federal Court, alleging the social media platform has committed serious and/or repeated interferences with privacy in contravention of Australian privacy law.[330] These proceedings are the first time this provision has been tested in court.

Section 80U was based on a recommendation from ALRC Report 108. The ALRC considered the benefits of an 'enforcement pyramid' approach to regulation, where regulators use less interventionist measures first to encourage compliance, with more severe sanctions generally held in reserve as a threat.[331] The Act, to some extent, already adopted that approach, by initially relying upon encouraging compliance, and then reserving determinations (and enforcement in the courts) to situations where that was not successful. However, the ALRC considered that whilst there was some degree of escalation in the remedies available, and that the significance of determinations

[326] Ibid ss, 52(1), 52(1A).
[327] Ibid ss 55A, 62.
[328] Ibid s 52 (note this provision only states the Commissioner 'may' make a determination after investigating a complaint or after a CII rather than saying the Commissioner 'must').
[329] OAIC, *Annual Report 2018–19* (n 312) 60.
[330] Office of the Australian Information Commissioner, *Commissioner launches Federal Court action against Facebook* (Web Page, March 2020).
[331] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1659.

should not be underestimated, the available remedies should be strengthened. The ALRC concluded that a serious or repeated interference with the privacy of an individual warranted a civil penalty.[332]

The maximum penalty for a breach of s13G is 2000 penalty units. This amounts to $2.1 million for a body corporate. However, the Government has announced that it will increase that penalty to $10 million or three times the value of any benefit obtained through the misuse of information or 10 per cent of the company's annual domestic turnover – whichever is the greater.[333]

Increasing the spectrum of enforcement mechanisms

The Government also announced that it would implement reforms to provide the Commissioner with new infringement notice powers for failure to cooperate with efforts to resolve minor breaches.[334] An infringement notice gives the person to whom the notice is issued the option to pay a fine in full as an alternative to prosecution for an offence or litigation of a civil matter in court. For example, the Act currently provides that it is an offence for failing to give information to the Commissioner when this has been required under the Act.[335] The proposed reforms could enable the Commissioner to issue an infringement notice, which the entity could elect to pay, instead of the matter being heard by a court. This proposed reform will add to the spectrum of regulatory enforcement options that are available under the Act.

Questions

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

[332] Ibid 1663 at [50.51].
[333] Attorney-General's Department, *Tougher penalties to keep Australians safe online* (Web Page, 24 March 2019).
[334] Ibid.
[335] Privacy Act (n 16) s 66.

A Direct Right of Action

The ability of individuals to litigate a claim for breach of their privacy under the Act is limited. The DPI report recommended that individuals be given a direct right to bring actions and class actions against APP entities in court to seek compensatory damages as well as aggravated and exemplary damages (in exceptional circumstances) for the financial and non-financial harm suffered as a result of an interference with their privacy under the Act.[336]

The ACCC's rationale for this recommendation is that it would give individuals greater control over their personal information and provide an additional incentive for APP entities to comply with their obligations under the Act. It considers a direct right of action would increase the opportunity for the courts to interpret the APPs, providing greater clarity and certainty regarding the operation of the Act, and to set standards in relation to penalties and compensation for privacy breaches. It also considers that a direct right of action may reduce the enforcement burden on the OAIC.[337]

In the DPI response, the Government supported this recommendation in principle, subject to consultation "to identify the appropriate measures that can be taken to ensure individuals have adequate remedies for an interference with their privacy under the Privacy Act".[338]

This recommendation is supported by the findings of the 2020 ACAP survey which shows that 78% of respondents believe that they should have the right to seek compensation in the courts for a breach of privacy.[339]

The current Australian law

Currently the Act does not include a right of action enabling individuals to directly apply to a court to seek compensation for an act or practice that is an interference with their privacy.[340] Individuals may make a complaint about an alleged interference with their privacy to the Commissioner. If the Commissioner makes a determination in relation to the complaint, the Federal Court and the Federal Circuit Court have power to enforce the determination.[341] Individuals may also apply directly to the Federal Court and the Federal Circuit Court for an injunction against a person for contraventions of the Act.[342]

Complaints to the Commissioner

The Commissioner has power to investigate, conciliate and decline complaints.[343] The Commissioner may make a determination after investigating a complaint which includes dismissing the complaint or finding the complaint substantiated and making a determination that includes certain declarations, including that the complainant is entitled to a specified amount by way of compensation for loss or damage.[344]

---

[336] ACCC, *Digital Platforms Inquiry* (n 1) 473.
[337] Ibid.
[338] Department of the Treasury, *Regulating in the digital age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (n 3) 18.
[339] OAIC, *Australian Community Attitudes to Privacy Survey 2020* (n 11) 7.
[340] An interference with the privacy of an individual includes an act or practice that breaches an APP or registered APP code under the Privacy Act; Privacy Act (n 16) s 13(1).
[341] Privacy Act (n 16) s 36.
[342] Ibid s 80W; *Regulatory Powers (Standard Provisions) Act 2014* (Cth) s 121.
[343] Privacy Act (n 16) ss 40, 40A and 41.
[344] Ibid s 52.

Proceedings in the Federal Court and Federal Circuit Court to enforce a determination

Complainants or the Commissioner may apply to the Federal Court or the Federal Circuit Court for an order enforcing a determination made by the Commissioner.[345] There is no ability for an individual to apply to the court in relation to a determination by the Commissioner to dismiss a complaint.[346] If the Court is satisfied that the person or entity in relation to which the determination applies has engaged in conduct that constitutes an interference with the privacy of an individual, it may make such orders as it thinks fit.[347] It may also grant an interim injunction pending determination of the proceedings.[348] The Courts deal with the question of whether there has been an interference with privacy by way of hearing de novo.[349] This means that the Court hears the matter afresh and may overturn the Commissioner's determination regardless of legal or factual error.[350]

In considering the Court's jurisdiction and powers under the Act, it has been noted that:

> *The jurisdiction of this Court in relation to breaches of the Privacy Act is limited. The Scheme of the Privacy Act is for complaints about such breaches to be made to the Privacy Commissioner who will investigate the complaint and make a determination, ss 36 and 52. Determinations of the Privacy Commissioner are not binding or conclusive between any of the parties to the determination; s 52(1B) but there is provision in s 55A for certain persons to seek to enforce a determination in this Court or in the Federal Magistrates Court. There is however no provision in the Privacy Act for a breach of the Privacy Principles to be directly actionable in this Court.*[351]

Merits and judicial review of the Commissioner's decision

A decision of the Commissioner to make a determination following investigation of a complaint is reviewable by the AAT under the Act.[352] The AAT hears the matter de novo and may affirm, vary or set aside the decision and either remake the decision or remit the decision back to the Commissioner with directions.[353] Decisions of the Commissioner and the AAT under the Act may also be subject to judicial review, including under the *Administrative Decisions (Judicial Review) Act 1977* (Cth).[354] Significantly, the entity that is alleged to have breached the individual's privacy is not a party to proceedings in either merits or judicial review.

Right to seek an injunction

Individuals can seek injunctions including restraining and performance injunctions under the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) for contraventions of the Act.[355] For example, if a person is misusing the personal information of an individual in breach of APP 6, that

---

[345] Ibid ss 55A and 62.
[346] *Ajok v Minister for Immigration and Citizenship* [2010] FMCA 331 [29].
[347] Privacy Act (n 16) s 55A(2).
[348] Ibid s 55A(3).
[349] Ibid s 55A(5).
[350] Westlaw AU, *The Laws of Australia* (online at 30 September 2020) 2 Administrative Law, '2.7 Other Forms of Review and Appeal' [2.7.1050].
[351] *Day v Lynn* [2003] FCA 879 [50].
[352] Privacy Act (n 16) s 96.
[353] *Administrative Appeals Tribunal Act 1975* (Cth) s 43, unlike the Federal Court or the Federal Circuit Court under section 55A, the AAT cannot make orders enforcing a determination.
[354] *Administrative Decisions (Judicial Review) Act 1977* (Cth).
[355] Privacy Act (n 16) s 80W; *Regulatory Powers (Standard Provisions) Act 2014* (Cth) s 121.

individual may apply to the Federal Court or the Federal Circuit Court for an injunction to restrain the person from engaging in that conduct. Whilst the ability to seek an injunction is a form of a direct right of action that is currently available, it does not include an ability to seek compensation.

Framing a direct right of action

Compared with the current complaint and determination enforcement framework, and the right to seek injunctive relief, a direct right of action under the Act would provide individuals with an enforceable right to apply directly to a court for a determination of whether an entity regulated under the Act has breached the Act and for orders against the entity including orders for compensation. In determining the framing of a direct right of action, the policy objective of giving individuals greater control over their personal information and incentivising APP entities to comply with their obligations under the Act must be balanced with the need to ensure that court resources are being appropriately directed and are not taken up by trivial breaches of the Act or APPs.

There are various ways this could be approached. One way might be to limit the right of direct action to the courts to serious breaches of the Act or APPs. Consideration may also be given to ameliorating potential burden on the courts by allowing the Commissioner to be heard in proceedings and provide expert assistance as amicus curiae.

Alternatively, applying to the courts could be made subject to a complaint first undergoing conciliation by the OAIC or some other administrative body. This may reduce the burden on the court system and provide individuals with a potentially speedier dispute resolution mechanism while still providing more direct access to the courts than the current complaint mechanism. An example of such a model is in the *Australian Human Rights Commission Act 1986* (Cth) under which a person may apply to the Federal Court or the Federal Circuit Court alleging unlawful discrimination only if the President of the AHRC has issued a notice of termination in relation to the complaint.[356]

Alternatively, complainants could be permitted to apply directly to the courts or they could seek conciliation with the OAIC or another administrative body depending on their preference. This is similar to the application of the CDR in the banking sector. Under the CCA, a person who suffers loss or damage by an act or omission of another person in contravention of the privacy standards of the CDR or the Consumer Data Rules has a right to bring an action for damages against that person or may seek to resolve the dispute with the Australian Financial Complaints Authority.[357]

If individuals are permitted to seek compensation from entities regulated under the Act directly in the courts, it may be desirable to impose a cap on the damages that may be awarded. Capping compensation may be justified on the basis that it may reduce the incentive for parties to litigate, making the right of action potentially less costly. However capping the amount of damages which may be awarded could lead to a preponderance of lesser rather than more serious breaches of the Act coming before the courts and dissatisfaction and a lack of confidence in the direct right of action.

Questions

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

[356] *Australian Human Rights Commission Act 1986* (Cth) s 46PO.
[357] *Competition and Consumer Act 2010* (Cth) s 56EY; *Competition and Consumer (External Dispute Resolution Scheme – Banking Sector) Instrument 2019.*

A Statutory Tort of Privacy

There is currently no tortious right of action for invasion of privacy under the Act or any other Commonwealth, state or territory statute. The DPI report recommended that a statutory cause of action for serious invasions of privacy be introduced as previously recommended by the ALRC.[358]

The ACCC's stated rationale for this recommendation included providing protection for individuals against serious invasions of privacy that may not be captured within the scope of the Act. It also considered that it would increase the accountability of businesses for their data practices, give consumers greater control over their personal information, lessen the bargaining power imbalance between consumers and entities collecting their personal information and create a new deterrent discouraging entities from engaging in harmful data practices.[359]

In 2014, the ALRC recommended that if a statutory cause of action for serious invasion of privacy was to be enacted, it should be enacted by the Commonwealth, in a new Commonwealth Act (not the Act).[360] The ALRC considered that enacting the recommendations in its report would 'fill an increasingly conspicuous gap in Australian law, helping to protect the privacy of Australians, while respecting and reinforcing other fundamental rights and values, including freedom of expression'.[361]

In the DPI response, the Government noted the recommendation and stated that it would need to be considered through the review of the Act and related laws being undertaken to consider whether broader reform is necessary.

Is a statutory tort for invasion of privacy needed?

Adequacy of existing protections

In its Report 123, the ALRC noted that three previous law reform inquiries had considered and answered this question in the affirmative.[362] In 2016, reports of the New South Wales Standing Committee on Law and Justice and the South Australian Law Reform Institute (SALRI) recommended that statutory causes of action for serious invasions of privacy be introduced in those states.[363] Both reports based their recommendations on assessments that the existing privacy framework provided inadequate protection to people who suffer serious invasions of privacy.[364] The SALRI Report highlighted the role of technological advances in the impetus for reform.

> *This vulnerability* [to invasions of privacy] *arises largely as a result of technological development and the consequent ease with which individuals (and not just well equipped*

[358] ACCC, *Digital Platforms Inquiry* (n 1) 493.
[359] Ibid.
[360] ALRC, *Serious Invasions of Privacy in the Digital Era* (n 229) 59.
[361] Ibid 28.
[362] Ibid 20. These were the ALRC, *For Your Information: Australian Privacy Law and Practice* (n 66) Recommendation 74–1; NSW Law Reform Commission, *Invasion of Privacy* (Report 120, April 2009) 17; Victorian Law Reform Commission, *Surveillance in Public Places* (Final Report 18, May 2010).
[363] Standing Committee on Law and Justice, Parliament of New South Wales *Remedies for the Serious Invasion of Privacy in New South Wales* (Report, March 2016); South Australian Law Reform Institute, *A statutory tort for invasion of privacy* (Final Report, March 2016).
[364] Standing Committee on Law and Justice, *Remedies for the Serious Invasion of Privacy in New South Wales* (n 363) 57; South Australian Law Reform Institute, *A statutory tort for invasion of privacy* (n 363) 15.

Governments or organisations) can intrude into a person's private space and can collect, disclose and widely disseminate personal information.[365]

It is important to note that since the publishing of the ALRC Report 123, there have been significant developments in the criminal law with respect to some serious invasions of privacy. Notably the *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* (Cth) which amended the *Enhancing Online Safety Act 2015* (Cth) and the *Criminal Code Act 1995* (Cth) provides for an aggravated offence to the offence of using a carriage service to menace, harass or cause offence where the offence involves the transmission, making available, publication, distribution, advertisement or promotion of material and the material is private sexual material.[366] This Act also amended the *Enhancing Online Safety Act 2015* (Cth) to create civil penalty offences for the posting of intimate images on social media without a person's consent which can be imposed by a Federal Court or the Federal Circuit Court following application by the National e-Safety Commissioner.[367] The National e-Safety Commissioner also has powers including powers to investigate complaints and issue infringement notices with respect to intimate images and require social media providers to take reasonable steps to remove intimate images under these amendments.[368]

Some states also have specific voyeurism offences which operate concurrently with the Commonwealth laws. For example, in 2008, the *Crimes Amendment (Sexual Offences) Act 2008* (NSW) introduced specific offences concerning voyeurism and filming a person engaged in a private act.[369] Similar offences have also been introduced in Queensland, the ACT, Victoria, South Australia.[370] In 2017, Commonwealth, state and territory jurisdictions agreed to the National Statement of Principles Relating to the criminalisation of the Non-Consensual Sharing of Intimate Images.[371] This led to all states and territories with the current exception of Tasmania passing laws that introduced offences concerning the distribution of images without consent.[372] In New South Wales, these offences were introduced in the *Crimes Amendment (Intimate Images) Act* and in Queensland through the *Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Act*.[373]

The development of criminal laws that specifically concern serious invasions of privacy such as imaged based abuse may negate the need for a tort of privacy on a policy basis. Criminal laws have the advantage of being enacted for the public purpose and can have a specific deterrent and educative effect. In addition, the complaints and investigations process under the *Enhancing Online Safety Act 2015* (Cth) ensures that the victims of the serious breaches of privacy the Act covers do

---

[365] South Australian Law Reform Institute, *A statutory tort for invasion of privacy* (n 363) 15.
[366] *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* (Cth) ('Non-consensual Sharing of Intimate Images Act') Sch 2.
[367] Ibid sch 1; *Enhancing Online Safety Act 2015* (Cth) ('Enhancing Online Safety Act') ss 44B, 46.
[368] Non-consensual Sharing of Intimate Images Act (n 366) sch 1; Enhancing Online Safety Act (n 367) ss 19A, 19C, 44D, 46A.
[369] *Crimes Amendment (Sexual Offences) Act 2008* (NSW); *Crimes Act 1990* (NSW) ss 91I-91M.
[370] *Criminal Code Act 1899* (Qld) s 227A; *Crimes Act 1990* (ACT) s 61B; *Summary Offences Act 1953* (SA) ss 26A, 26B, 26D, 26E; *Summary Offences Act 1966* (Vic) ss 40, 41, 41A, 41B, 41D.
[371] Law Crime and Community Safety Council, *National Statement of Principles Relating to the criminalisation of the Non-Consensual Sharing of Intimate Images* (Statement of Principles, 19 May 2017).
[372] *Crimes Act 1900* (ACT) ss 72C-72D; *Crimes Act 1900* (NSW) 91P-91R; *Criminal Code Act 1983* (NT) ss 208AB, 280AC; *Criminal Code Act 1899* (Qld) ss 207A, 223, 227A, 227B, 229A, 229AA; *Summary Offences Act 1953* (SA). ss 26A-26E; *Summary Offences Act 1966* (Vic) ss 40, 41, 41C, 41DA, 41DB; *Criminal Code Act Compilation Act 1913* (WA) ss 221BA-221BF, 338, 338B and 338C.
[373] *Crimes Amendment (Intimate Images) Act 2017* (NSW); Crimes Act 1990 (NSW) ss 91N-91T; *Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Act 2019* (Qld) ss 207A, 223, 227B-229AA.

not need to take action against the complainant directly as such action may be expensive and traumatic. On the other hand, a tort of privacy does provide individuals with an option to take civil action against an individual or entity and seek damages such as compensation.

Breach of confidence

Individuals have a limited right of redress for invasions of privacy through an equitable action for breach of confidence.[374] Part VIII of the Act extends the remedies available in equity for breach of an obligation of confidence, however these provisions have not been extensively tested.[375] While the equitable action may provide redress in some circumstances, it has been noted that its traditional application to relationships of confidentiality constructed through contractual and commercial relationships makes it a 'poor fit' to breaches of privacy.[376] Stakeholders have also raised concerns that the action has not developed enough to be a reliable source of remedy.[377]

Development of a tort at common law

The abovementioned reports considered the need for a statutory tort against the backdrop of the common law not recognising a tort for invasion of privacy in Australia, despite the High Court leaving open the possibility of such a development.[378] While several lower courts have gone some way toward recognising a tort of invasion of privacy, these have not resulted in appellate decisions.[379] This means that if a tort for the serious invasion of privacy is not developed by the legislature, a tort to address this sort of harm could still develop at common law, as has occurred in New Zealand.[380]

The ALRC considered whether it would be better for a tort for invasion of privacy to be enacted by the Parliament or left to the courts to develop.[381] It noted that any significant development of the common law require well-resourced, determined litigants to take proceedings through the appeals process. It also noted that courts are limited to deciding the issues in dispute in the specific case before it, whereas the Parliament can proactively address emerging issues in the community. It considered that while statute law may become outdated by social and technological changes, it has greater capacity to address complex policy issues and legal concepts in more accessible way than case law for people without legal training. On balance, and given the uncertainty surrounding how a tort may develop at common law, the ALRC favoured the development of a tort through statute.[382]

---

[374] *Wilson v Ferguson* [2015] WASC 15.
[375] Privacy Act (n 16) Part VIII. The Federal Court in *Austen v Civil Aviation Authority* 50 FCR 272 stated at 277-278 that Part VIII didn't necessarily create a right of action like a tort but extended the remedies available in equity for a breach of an obligation of confidence.
[376] Standing Committee on Law and Justice, *Remedies for the Serious Invasion of Privacy in New South Wales* (n 363) 47; Mark Elliott, 'Privacy Confidentiality and Horizontality: The Case of the Celebrity Wedding Photographers', (2001) 60(2), *Cambridge Law Journal* 231, 232.
[377] Standing Committee on Law and Justice, *Remedies for the Serious Invasion of Privacy in New South Wales* (n 363) 46.
[378] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.
[379] ALRC, *Serious Invasions of Privacy in the Digital Era* (n 229) 23 noted that the cases of *Grosse v Purvis* [2003] QDC 151 (16 June 2003) and *Doe v Australian Broadcasting Corporation* [2007] VCC 281 were settled before appeals by the respective defendants were heard.
[380] *C v Holland* [2012] NZHC 2155 recognised a tort of intrusion.
[381] ALRC, *Serious Invasions of Privacy in the Digital Era* (n 229) 23.
[382] Ibid 24.

Framing a statutory tort for serious invasion of privacy

Types of privacy invasions

Compared with a direct right of action as recommended in the DPI, a statutory tort would allow individuals to seek redress for breaches of privacy not necessarily covered by the Privacy Act.

The ALRC recommended that a statutory tort cover two types of invasion of privacy, intrusion into seclusion and misuse of private information.[383] Intrusion upon seclusion would normally involve an intrusion into a person's physical space and would cover activities such as watching, listening to and recording another person's private activities.[384] Misuse of private information would most commonly involve the unauthorised public disclosure of personal information however the ALRC considered it would not be reasonable to confine the misuse to public disclosures as in some circumstances, the disclosure of personal information to one other person may be a serious invasion of privacy.[385] However, since the ALRC's recommendation, new criminal offences have been introduced that cover some intrusions upon seclusion and misuses of private information.

Reasonable expectation of privacy

In both cases, the ALRC recommended that a plaintiff be required to prove that a person in the position of the plaintiff would have a reasonable expectation of privacy in all the circumstances.[386] While the ALRC's recommended test is objective, when determining whether a plaintiff would have had a reasonable expectation of privacy in 'all of the circumstances' some of the circumstances may be the subjective expectations of the plaintiff.[387] Despite this, the subjective expectations of the plaintiff are not the focus of the ALRC's recommended test.[388] The noted strengths of an objective test include the ability of the test to adapt to changing community expectations and standards.[389]

Requirement for fault

A key issue for the design of a statutory tort of privacy is the types of liability it would cover. That is, liability based on intention, liability based on negligence or strict liability. The ALRC recommended that a statutory tort should be confined to intentional or reckless invasions of privacy and should not extend to negligent invasions of privacy or attract strict liability.[390] This was because the ALRC considered that the tort should apply to the most objectionable types of invasion of privacy and that the inclusion of negligence or strict liability would make the scope of the tort too broad.[391] However, it is questionable that an invasion of privacy due to gross negligence where a person may not have been reckless but failed to exercise even the slightest degree of care and diligence in relation to an obvious risk should be outside scope.

Competing public interests

The ALRC Report 123 considered that the court would need to weigh the complainant's right to privacy against countervailing public interests and be satisfied that the public interest in privacy

[383] Ibid 74.
[384] Ibid 76.
[385] Ibid 83.
[386] Ibid 92.
[387] Ibid.
[388] Ibid 92.
[389] Ibid 93-94.
[390] Ibid 110.
[391] Ibid 109.

outweighs any relevant public interest. A separate public interest defence would therefore be unnecessary.[392] Public interest factors may include freedom of expression, right to a fair trial, freedom of the media, the proper administration of government, open justice, public health and safety, national security, and the prevention and detection of crime and fraud.[393]

Characterisation as a tort?

Both the ALRC Report 123 and the New South Wales Standing Committee on Law and Justice report considered whether the right of action should be called a 'tort'. Whilst the New South Wales Standing Committee on Law and Justice did not reach a conclusion, the ALRC ultimately recommended that the cause of action should be called a tort.[394] This was on the basis that it would provide certainty and prevent disputes arising about a number of ancillary issues, including by making it clear that the common law principles concerning the vicarious liability of employers and legislative provisions that refer to liability in tort would apply to the new cause of action.[395]

Questions

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

[392] Ibid 143.
[393] Ibid 152.
[394] Ibid 67.
[395] Ibid 67-68.

Notifiable Data Breaches Scheme – impact and effectiveness

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 commenced with the enactment of the *Privacy Amendment (Notifiable Data Breaches) Act 2017*.[396] The purpose of the NDB scheme was expressed in the Minister's second reading speech which stated:

> *'the rationale for mandatory data breach notification is that, if an individual is at likely risk of serious harm because of a data breach involving their personal information, receiving notification of the breach can allow that person to take action to protect themselves from that harm. For example, an affected individual might change an online password or cancel a credit card after receiving notification that their personal information has been compromised in a data breach.'*[397]

The RIS which accompanied the Privacy Amendment (Notifiable Data Breaches) Bill 2016 provided that the objective of the mandatory data breach notification scheme is, consistent with the broad objectives of the Act, to promote the protection of privacy of individuals while recognising that this protection should be balanced with the interests of entities carrying out their legitimate functions and activities.[398] It also noted that a mandatory data breach notification scheme should result in an improvement in compliance with privacy obligations and encourage agencies and organisations to be transparent about their information handling practices.[399] A review of the impact and effectiveness of the NDB Scheme in this Review of the Act fulfils an obligation contained in the RIS.[400]

Scope of the NDB Scheme

The NDB Scheme is contained in Part IIIC of the Act.[401] The scope of the NDB Scheme is primarily defined in section 26WE(1) which states that the scheme applies if an APP entity holds personal information relating to one or more individuals and the APP entity is required under section 15 not to do any act, or engage in any practice, that breaches APP 11.1 in relation to the personal information.[402] The NDB Scheme also applies to credit reporting bodies or holders of tax file numbers.[403] Section 56ES of the CCA also extends the application of the NDB Scheme to certain data breaches under the CDR.[404]

---

[396] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth).
[397] Commonwealth, *Parliamentary Debates*, House of Representatives, 19 October 2016, 2430 (Michael Keenan).
[398] Attorney-General's Department, *Privacy Amendment (Notifiable Data Breaches) Bill 2016 Regulation Impact Statement* (Regulation Impact Statement, 11 January 2017) 15.
[399] Ibid.
[400] Ibid 43.
[401] Privacy Act (n 16) Part IIIC.
[402] Ibid s 26WE(1).
[403] Ibid.
[404] *Competition and Consumer Act 2010* (Cth) s 56ES. The object of this section is for Part IIIC of the Privacy Act to apply to an accredited data recipient, or a designated gateway, that holds a CDR consumer's CDR data in a corresponding way to the way that Part applies to an entity that holds an individual's personal information.

When notification obligations are triggered

The notification 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, or if the entity is aware that there are reasonable grounds to believe that there *has* been an eligible data breach of the entity. [405]

If the entity is only aware that there are reasonable grounds to suspect that the relevant circumstances amount to an eligible data breach of the entity, the entity is required to undertake a mandatory assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity.[406] The entity is required to take steps to ensure that this assessment is completed within 30 days after the entity becomes aware that there are reasonable grounds to suspect that an eligible data breach has occurred.[407]

The definition of 'eligible data breach' is contained in subsection 26WE(2) of the Act and has two limbs.[408] 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.[409] 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.[410]

When assessing the likelihood of harm, the entity must have regard to the non-exhaustive list of relevant matters in section 26WG of the Act. These include factors such as the kind or kinds and the sensitivity of the information that is the subject of the suspected data breach in addition to the persons, or the kinds of persons who have obtained or who could obtain, the information.[411]

Obligation to prepare a statement to OAIC

If an entity determines that an eligible data breach has occurred, it is required to provide a statement to the OAIC.[412] The statement is required to set out:

- the identity and contact details of the entity;
- a description of the eligible data breach that the entity has reasonable grounds to believe has happened;
- the kind or kinds of information concerned; and
- recommendations about steps that individuals should take in response to the eligible data breach that the entity has reasonable grounds to believe has happened.[413]

[405] Privacy Act (n 16) ss 26WH(1), 26WH(2), 26WK(1).
[406] Ibid s 26WH(2).
[407] Ibid.
[408] Ibid.
[409] Ibid.
[410] Ibid.
[411] Ibid s 26WG.
[412] Ibid ss 26WK, 26WL.
[413] Ibid s 26WK(3).

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.[414]

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. The persons the entity notifies depends on what is practicable in the circumstances.

The entity has two options. Under the first option, if it is practicable in the circumstances, the entity is required to notify the contents of the statement to each of the individuals to whom the information relates.[415] The entity is required to take steps that are reasonable in the circumstances to notify each of these individuals.[416] This means that the entity's notification obligations do not extend to notifying individuals where those steps are *not* reasonable in the circumstances.

Alternatively, under the second option, if it is practicable in the circumstances, the entity is required to notify the contents of the statement to each of the individuals who are 'at risk' from the eligible data breach by taking such steps that are reasonable in the circumstances.[417]

If it is not practicable for the entity to either notify the contents of the statement to each of the individuals to whom the information relates or each of the individuals who are at risk from the eligible data breach, the entity is required to publish a copy of the statement on the entity's website (if any) and take reasonable steps to publicise the contents of the statement.[418]

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.

Powers of the Commissioner

The Commissioner has a number of powers in relation to the NDB Scheme. The Commissioner can direct an entity to notify an eligible data breach if the Commissioner is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity.[419] The entity is required to prepare a statement and notify the contents of that statement to affected individuals or individuals at risk in a manner consistent with if the entity had conducted an assessment and determined that an eligible data breach occurred.[420]

The Commissioner also has powers to make declarations concerning compliance with the notification obligations.[421] The Commissioner can, on its own initiative or on application, declare that the statement and notification obligations do not apply to an entity or if the data breach is an eligible data breach of other entities, declare that the statement and notification obligations apply to those entities.[422] The Commissioner can also initiative or on application, specify a time frame within

[414] Ibid s 26WK(4).
[415] Ibid s 26WL(2)(a).
[416] Ibid.
[417] Ibid s 26WL(2)(b).
[418] Ibid s 26WL(2)(c).
[419] Ibid s 26WR.
[420] Ibid.
[421] Ibid s 26WQ.
[422] Ibid.

which the entity or entities must comply with their obligations to notify individuals affected by the data breach.[423]

The Commissioner may only make a declaration if it is satisfied it is reasonable in the circumstances to do so, having regard to the public interest, and any relevant advice received from an enforcement body or the Australian Signals Directorate, or any other relevant matter.[424] The broad purpose of these powers is to provide the Commissioner with a discretion to make certain exceptions from the scheme's requirements by declaration in exceptional circumstances such as where there is a law enforcement investigation being undertaken into a data breach and notification would impede that investigation, or where the information concerns matters of national security.[425]

Impact of the NDB Scheme

The NDB Scheme commenced on 22 February 2018. There are therefore some difficulties in determining at this stage whether the scheme has achieved its long term objectives.

Increase in notifications

The quantitative data available since the commencement of the NDB Scheme shows a significant increase in the number of data breaches that have been notified to the OAIC. From 1 April 2018 to 31 March 2019, the OAIC received a total of 964 notifications under the NDB Scheme and an additional 168 voluntary data breach notifications (which are notifications for breaches not deemed 'eligible data breaches' under the NDB Scheme usually because the threshold has not been reached or the entity is not bound by the Act).[426] This represents an increase of 712 per cent in data breach reporting compared to the previous 12 months under the voluntary scheme. More recently, the OAIC reported that they received a total of 1050 notifications for the 2019-20 financial year.[427]

Of the 964 notifications received by the OAIC from 1 April 2018 to 31 March 2019, 35 per cent were attributed to human error, 60 per cent were attributed to malicious or criminal attacks and five per cent were attributed to system faults.[428] The health sector was the leading reporter of data breaches followed by the finance sector.[429] The OAIC reported that this is consistent with international trends.[430]

Greater transparency and accountability

In its 12 month insights report, the OAIC stated that in the NDB Scheme's first year of operation, it has been evident that there has been greater transparency and accountability of entities concerning data breaches.[431] The OAIC states that it has observed entities activating data breach response plans to investigate and notify, to minimise immediate harms and prevent future breaches.[432] This

[423] Ibid.
[424] Ibid.
[425] Explanatory Memoranda, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) 95-96.
[426] Office of the Australian Information Commissioner, *Notifiable Data Breaches Scheme 12-month Insights Report* (Report 13 May 2019) 8.
[427] Ibid 5.
[428] Ibid 8.
[429] Ibid 13.
[430] Ibid.
[431] Ibid 19.
[432] Ibid.

suggests that the scheme has encouraged entities to be more proactive in managing their data security, which may assist with greater compliance with APP 11.

Overall effectiveness

The immediate impact of the NDB Scheme was a 712 per cent increase in notifications compared with the number of voluntary notifications made in the 12 months prior.

The OAIC reports that the increase in notifications reflects a significant increase in entities awareness of and compliance with their obligations to notify the OAIC and affected individuals where a breach of personal information is likely to result in serious harm.[433] As stated, the OAIC expressed that they have observed entities activating data breach response plans to investigate, assess and notify to minimise immediate harms and prevent future breaches.[434]

This indicates that in the short period since the commencement of the NDB scheme, it has been effective in increasing data breach notifications. OAIC also report that awareness of the NDB scheme appears to be high, aided by international developments and media attention.[435]

The OAIC has reported that in the January to June 2020 reporting period there have been multiple instances of incomplete notifications of data breaches where entities may not have fully met their obligations in regard to the content of the notification to individuals affected by the data breach.[436] The OAIC stated, as an example, that while entities notified affected individuals that their email addresses were involved in a data breach, on some occasions they did not advise that other personal information was also involved.[437]

The OAIC have also reported that during the January to June 2020 reporting period, 77 per cent of notifying entities were able to identify a breach within 30 days of it occurring and 74 per cent were able to complete their assessment of the breach and report it to OAIC within 30 days of becoming aware that the data breach potentially occurred.[438] Despite this, the OAIC also reported that in five per cent of notifications, assessment and notification took more than 121 days.[439]

Issues potentially impacting effectiveness

Multi Party Breaches

Multi-party breaches are data breaches where there is a breach of data held by multiple entities. Multi-party breaches have the potential to occur where there are supplier arrangements and through the use of cloud service products.

The management of multi-party breaches are a potential issue for some entities who are concerned about the effectiveness of the NDB Scheme.[440] The OAIC have stated that the effective navigation of multi-party breaches is an area of improvement for the NDB Scheme.[441]

---

[433] Ibid 9.
[434] Ibid 3.
[435] Ibid 9.
[436] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report – January-June 2020* (Report, 31 July 2020) 9.
[437] Ibid.
[438] Ibid 19.
[439] Ibid 19.
[440] OAIC, *Notifiable Data Breaches Scheme 12-month Insights Report* (n 426) 16.
[441] Ibid.

Under the NDB Scheme, an eligible data breach of one entity is also considered an eligible data breach of other entities that hold the affected information. Only one entity is required to carry out notification if a multi-party breach occurs. If that entity takes the steps required under the NDB Scheme, this constitutes compliance for all entities that hold the information but if no entity takes the necessary steps, all affected entities have breached their obligations.[442] It is up to the entities to determine who conducts the notification and the OAIC recommends that entities with the most direct relationships with individuals affected by the data breach carry out the notification.[443]

Compliance across multiple international frameworks

Entities are often required to manage personal information across multiple jurisdictions. Other jurisdictions have enacted data breach notification obligations that Australian entities may be required to comply with. An example is the data breach notification obligations under the GDPR.

If the GDPR applies and a personal data breach occurs, the controller of the data is required to, without undue delay and where feasible and not later than 72 hours after becoming aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 33, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.[444] Where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.[445] Also under Article 34, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is required to communicate the personal data breach to the data subject without delay.[446]

The requirement of the controller to notify the supervisory authority within 72 hours of becoming aware of the data breach differs from the notification timeframes under the NDB Scheme.[447] The requirement to comply with data breach notification obligations from across multiple international frameworks that differ significantly may increase the compliance burden on entities.

The emergence of other domestic notification frameworks

The effectiveness of the NDB Scheme may also be impacted by the emergence of other notification frameworks for managers of information.[448] The emergence of other information frameworks may increase the compliance burden on entities which may affect an entity's ability to carry out its legitimate functions and activities.[449]

An example of a data breach notification framework is clause 35 of the *Banking, Insurance, Life Insurance, Health Insurance, and Superannuation (prudential standard) determination No. 1 of 2018 Prudential Standard CPS 234 Information Security*.[450] This requires an APRA regulated entity to notify APRA as soon as possible, and in any case, no later than 72 hours, after becoming aware of an information security incident that:

---

[442] Ibid.
[443] Ibid.
[444] General Data Protection Regulation (n 39) art 33.
[445] Ibid.
[446] Ibid art 34.
[447] Surman (n 305) 93
[448] Lynton Brooks and Arvind Dixit, 'General data protection regulation: GDPR one year on' (2019) 93(10) *Law Institute Journal* 25.
[449] Ibid.
[450] Australian Prudential Regulation Authority, *Banking, Insurance, Life Insurance, Health Insurance, and Superannuation (prudential standard) determination No. 1 of 2018* (CPS 234, 30 November 2018) [35].

(a) Materially affected, or has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policy holders, beneficiaries or other customers or,
(b) Has been notified to other regulators, either in Australia or in other jurisdictions.[451]

This notification obligation is more in line with the notification obligations under Article 33 of the GDPR than the requirements of the NDB Scheme.[452]

The emergence of other notification schemes may increase entities' compliance burden because of differences in notification timeframes and the requirement to notify other regulatory bodies in addition to the Commissioner. While notification frameworks could be streamlined to avoid duplication, there may still be a need for multiple notifications where breaches include data that is not personal information.

Questions

63. Have entities' practices, including data security practices, changed due to the commencement of the NDB Scheme?
64. Has the NDB Scheme raised awareness about the importance of effective data security?
65. Have there been any challenges complying with the data breach notification requirements of other frameworks (including other domestic and international frameworks) in addition to the NDB Scheme?

[451] Ibid.
[452] Under clause 35(b), if a eligible data breach has been notified to OAIC, the breach must also be notified to APRA as it is an information security incident that has been notified to another regulator.

Interaction between the Act and other regulatory schemes

While the Act establishes the primary Commonwealth privacy framework, privacy protections also exist in other regulatory schemes. Regulators other than the OAIC also deal with privacy issues, including the ACCC, the Australian Communications and Media Authority (ACMA), the Office of the National Data Commissioner (ONDC), and the eSafety Commissioner.

Commonwealth regulation

Legislation regulating personal information handling

In addition to the Act, other Commonwealth legislation regulates the handling of personal information, including the *Freedom of Information Act 1982* and the *Archives Act 1983*, and federal taxation legislation. Other legislation that requires or authorises the disclosure of personal information include the *Australian Passports Act 2005* (Cth), *Corporations Act 2001* (Cth), *Telecommunications Act 1997* (Cth) (Tel Act), the *Telecommunications (Interception and Access) Act 1979* (Cth)(TIA Act), and the *Migration Act 1958* (Cth).[453] Federal legislation also contains a large number of secrecy provisions that impose duties on public servants not to disclose information obtained in the course of their duties.[454]

Specific privacy protections in other legislation

The original purpose of the Act was to provide a comprehensive set of general privacy protections for the Australian Government, which was subsequently extended to the private sector (excluding small businesses). As specific issues have arisen that have warranted stronger privacy protections, specific frameworks have been put in place to address those issues.

For example, the My Health Record system is a national public system for making health information about a healthcare recipient available for the purposes of providing healthcare to the recipient.[455] The purposes for establishing this system included to help overcome the fragmentation of health information and to improve the coordination and quality of healthcare provided to patients by different healthcare providers.[456] The Australian Digital Health Agency (ADHA) runs the My Health Record system and the OAIC oversees the privacy aspects of the system. The OAIC investigates complaints about how My Health Record information has been handled and also receives and assesses notifications about data breaches.[457]

Another recent example is the eSafety framework, established in 2015 to promote online safety.[458] The eSafety Commissioner administers a civil penalties scheme to address the non-consensual sharing of intimate images, known as image-based abuse. Victims of image-based abuse can report image-based abuse, and receive assistance to get intimate images quickly removed. There are also a range of civil remedies to hold the person responsible for the image-based abuse accountable.[459]

---

[453] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 66) 163.
[454] Ibid.
[455] *My Health Records Act 2012* (Cth) s 4.
[456] Ibid s 3.
[457] Office of the Australian Information Commissioner, *Sharing my health record — it's my choice* (Web Page, accessed 2 October 2020).
[458] Enhancing Online Safety Act (n 367) s 15.
[459] Australian Government eSafety Commissioner, *Civil penalties scheme* (Web Page, accessed 2 October 2020).

State and territory regulation

Most states and both territories have their own privacy legislation.[460] The ACT, Victoria, and recently Queensland, have also enacted human rights legislation that contain privacy rights.[461]

Personal information handling is also regulated under state and territory laws that do not specifically relate to privacy. For example, legislation containing secrecy provisions, listening and surveillance devices legislation, telecommunications legislation and FOI and public records legislation.[462]

Benefits and risks of dispersed privacy protections

The specific privacy protections contained in other frameworks were developed in response to specific issues where the information required additional protections and where those protections would not be appropriate to apply to all personal information. This approach has also allowed for regulators with expertise in certain industry sectors such as health services, health and medical research, and banking to handle privacy complaints within the broader industry context.[463]

However, it also has the potential to create uncertainty for consumers and industry. For example, consumers may experience confusion about which is the relevant regulatory framework they should bring a complaint under.

Overlapping Commonwealth and state and territory legislation regulating private health service providers illustrates this potential for confusion. 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. In NSW, Victoria and the ACT private sector health service providers must comply with both Australian and state or territory privacy laws when handling health information.[464] Queensland, the Northern Territory and Tasmania have privacy legislation that applies only to their public sector, including public sector health service providers. Western Australia and South Australia do not have specific privacy legislation.[465]

---

[460] *Privacy and Personal Information Protection Act 1998* (NSW); *Privacy and Data Protection Act 2014* (Vic); *Information Privacy Act 2009* (Qld); *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2014* (ACT); *Information Act 2002* (NT). The Western Australian government is currently consulting on privacy and responsible information sharing legislation for the WA public sector. South Australia has an administrative scheme under the Information Privacy Principles Instruction (SA). NSW, Victoria and the ACT also have specific legislation protecting the privacy of health records.

[461] *Human Rights Act 2004* (ACT) s 12; *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13; *Human Rights Act 2019* (Qld) s 25.

[462] For example privacy protections are found in the ACT, WA, SA and Vic Freedom of Information Acts, the SA, NT, NSW, Vic, WA, ACT and Tas Surveillance Devices Acts, and the Qld and Vic Public Records Acts.

[463] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 66) 506.

[464] Office of the Australian Information Commissioner, *Privacy for health service providers* (Web Page, accessed 2 October 2020); see e.g. *Health Records (Privacy and Access) Act 1997* (ACT)*, Health Records and Information Privacy Act 1998 (NSW), Health Records Act 2001 (Vic).* Note, the exception under the Act for the collection of health information where a permitted general situation or permitted health situation exists. Exceptions to use and disclosure provisions also exist under state and territory privacy legislation where there is an imminent threat to life or the health of a person, e.g. *Privacy and Personal Information Protection Act 1998* (NSW) ss 17(c), 18(1)(c).

[465] Office of the Australian Information Commissioner, *Privacy in your state* (Web Page, accessed 30 September 2020).

Interaction between the OAIC and other regulators

The OAIC is Australia's independent national regulator for privacy and freedom of information. It is charged with promoting and upholding privacy and information access rights. It is responsible for privacy functions that are conferred by the Act and other laws.

The Act allows for privacy complaints to be referred to certain other authorities such as the Commonwealth Ombudsman, the AHRC, and the Australian Public Service Commissioner.[466]

To assist and clarify its interaction with other regulatory bodies, the OAIC has entered into memorandums of understanding (MOUs) with other regulators, including the ACCC, ACMA, ADHA, IGIS, and the ACT in relation to the provision of privacy services. The OAIC has also entered into MOUs with international partners, including the UK Information Commissioner's Office, the Data Protection Commissioner of Ireland and the Personal Data Protection Commission of Singapore.[467]

ACCC and the consumer laws

The ACCC enforces the CCA and a range of additional legislation. It focuses on taking action that promotes the proper functioning of Australian markets, protects competition, improves consumer welfare and stops conduct that is anti-competitive or harmful to consumers.[468] The OAIC's MOU with the ACCC covers the exchange of information, acknowledges the need for effective consultation and cooperation with each other in order to carry out their roles.[469] The OAIC and ACCC have also entered into an MOU in respect of the Consumer Data Right.

As a result of recent advancements in the collection and use of consumers' personal data by businesses, the ACCC has increasingly taken action against companies for misleading and deceptive conduct in relation to their collection and use of consumers' personal information. In August 2020, the Federal Court found that online health booking platform HealthEngine Pty Ltd (HealthEngine) had engaged in misleading or deceptive conduct in contravention of s 18 of the Australian Consumer Law by not adequately disclosing to its customers that their personal information would be sent to third party private health insurance brokers. HealthEngine was ordered to pay a pecuniary penalty of $2,900,000.[470] In October 2019, the ACCC issued proceedings against Google for allegedly engaging in misleading conduct and making false or misleading representations to consumers about the personal location data Google collects, keeps and uses.[471]

ONDC and data availability and transparency

The ONDC is responsible for streamlining how public sector data is used and shared to promote greater use of public sector data as well as drive innovation and economic benefits from greater use of public sector data and build trust with the Australian community around government's use of

[466] Privacy Act (n 16) s 50(2).
[467] Office of the Australian Information Commissioner, *Memorandums of understanding* (Web Page, accessed 2 October 2020)
[468] Australian Competition and Consumer Commission, *About the ACCC* (Web Page, accessed 2 October 2020)
[469] Office of the Australian Information Commissioner, *MOU with ACCC – exchange of information* (Web Page, August 2020).
[470] *Australian Competition and Consumer Commission v HealthEngine Pty Ltd* [2020] FCA 1203.
[471] Australian Competition and Consumer Commission, *Google allegedly misled consumers on collection and use of location data* (Web Page, 29 October 2019).

data.[472] The ONDC aims to find the right balance between streamlining the sharing and use of public sector data while addressing privacy and security concerns.[473]

The ONDC is currently developing a data sharing framework for public sector data, working with the OAIC, to ensure that Australia's data sharing framework is underpinned by a strong foundation of transparency, privacy and security.[474] It has recently released a public exposure draft of the Data Availability and Transparency Bill 2020.[475] The legislation will ensure privacy is adequately protected by establishing clear regulations, including enforcement and accountability mechanisms.

ACMA and telecommunications legislation

ACMA is an independent Commonwealth statutory authority which regulates communications and media services in Australia and is responsible for enforcing the Tel Act.[476] Privacy protections under the Tel Act include prohibiting the use and disclosure of personal information, including any information relating to the contents or substance of a communication that has been carried by a carrier or carriage service provider.[477]

The Tel Act enables bodies and associations in the telecommunications industry to develop industry codes relating to telecommunications activities.[478] Industry codes may deal with matters including privacy and in particular: the protection of personal information, the intrusive use of telecommunications by carriers or service providers, the monitoring or recording of communications, calling number display, and the provision of directory products and services.[479] Before ACMA can register an industry code which deals directly or indirectly with a matter dealt with by the Privacy Act, it must consult the Information Commissioner to ensure he or she is satisfied.[480] The codes are voluntary, but the ACMA has the power to direct entities within its jurisdiction to comply with a code.[481] ACMA also investigates alleged breaches of privacy obligations under these codes such as the Television Code of Practice.[482]

TIA Act and oversight bodies

The TIA Act is another piece of Commonwealth legislation which protects privacy through regulating the interception of communications and access to stored communications and telecommunications data. The Commonwealth Ombudsman and the IGIS are the primary bodies who oversee use of the TIA Act. The Information Commissioner also has a range of powers and obligations in relation to the administration of the Tel Act and TIA Act.[483] These include the power to monitor compliance with Part 13, Division 5 of the Tel Act, requiring carriers and carriage service providers to make records of

---

[472][472] Office of the National Data Commissioner, *About Us* (Web Page, accessed 21 September 2020).
[473] Office of the National Data Commissioner, *Data Availability and Transparency Bill 2020 Exposure Draft* (Consultation Paper, September 2020) iii.
[474] ONDC, *About Us* (n 472).
[475] Office of the National Data Commissioner, *Consultation on the Data Availability and Transparency Bill 2020* (Web Page, accessed 25 September 2020).
[476] Australian Communications and Media Authority, *Who we are* (Web Page, accessed 2 October 2020).
[477] *Telecommunications Act 1997* (Cth) (Tel Act) s 276.
[478] Ibid s 112; ALRC, *For Your Information: Australian Privacy Law and Practice* (n 66) 185 at [2.89].
[479] Tel Act (n 477) s 113(3)(f).
[480] Ibid ss 116A, 117, 134.
[481] Office of the Australian Information Commissioner, *Telecommunications* (Web Page, accessed 21 September 2020).
[482] Australian Communications and Media Authority, *A Current Affair breaches privacy rules* (Web Page, 20 December 2019).
[483] OAIC, *Telecommunications* (n 481).

certain disclosures of personal information, including disclosures of telecommunications data collected and retained under the data retention scheme to law enforcement agencies.[484]

Questions

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

[484] Ibid.

Appendix A – Overview of the Australian Privacy Principles

Principle[485]	Title	Purpose
APP 1	Open and transparent management of personal information	Requires APP entities to manage personal information in an open and transparent way. Requires a clearly expressed and up to date privacy policy.
APP 2	Anonymity and pseudonymity	Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym.
APP 3	Collection of solicited personal information	Outlines when an APP entity can collect personal information or sensitive information that is solicited.
APP 4	Dealing with unsolicited personal information	Outlines how APP entities must deal with unsolicited personal information.
APP 5	Notification of the collection of personal information	Outlines when and in what circumstances an APP entity that collects personal information must notify an individual about certain matters.
APP 6	Use or disclosure of personal information	Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.
APP 7	Direct marketing	Outlines the circumstances in which an organisation may use or disclose personal information for direct marketing purposes.
APP 8	Cross-border disclosure of personal information	Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.
APP 9	Adoption, use or disclosure of government identifiers	Outlines the limited circumstances when an organisation may adopt a government related identifier as its own identifier, or use or disclose a government related identifier.
APP 10	Quality of personal information	Requires APP entities to take reasonable steps to ensure personal information that is collected is accurate, up to date and complete. Requires entities to take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant.
APP 11	Security of personal information	Requires an APP entity to take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.
APP 12	Access to personal information	Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them. Requires an APP entity to provide access unless a specific exception applies.
APP 13	Correction of personal information	Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

[485] See also Office of the Australian Information Commissioner, *Australian Privacy Principles quick reference* (Web Page, accessed 14 October 2020).

Appendix B - Privacy Act timeline

The following timeline highlights some of the key milestones in the development of the Privacy Act:

1972	Australia signs the International Covenant on Civil and Political Rights (ICCPR), which includes the right to privacy in Article 17.
1980	The Organisation for Economic Cooperation and Development (OECD) releases the first version of its Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data.
1983	The Australian Law Reform Commission releases its wide-ranging report on Privacy (ALRC Report 22), outlining the actual and prospective privacy risks in Australia and recommending new legislation to combat these risks.
1988	The Privacy Act passes both houses of parliament, giving effect to Australia's agreement to implement the OECD Guidelines, and to its obligations under Article 17 of the ICCPR. Much of this legislation is based on recommendations from ALRC Report 22.
1989	The Privacy Act commences, requiring agencies to comply with 11 Information Privacy Principles (the IPPs) when handling personal information and establishing the role of the Privacy Commissioner.
1991	The *Privacy Amendment Act 1990* (Cth) comes into effect, establishing a privacy framework around credit reporting.
2000	The *Privacy Amendment (Office of the Privacy Commissioner) Act 2000* establishes the Office of the Privacy Commissioner as a body independent from the Human Rights and Equal Opportunity Commission.
2001	The *Privacy Amendment (Private Sector) Act 2000* extends coverage of the Privacy Act to certain private sector organisations, including those with a turnover of greater than $3 million. These amendments introduce 10 National Privacy Principles (the NPPs) which apply to organisations which have been brought within the Privacy Act's scope.
2003	The Australian Law Reform Commission releases ALRC Report 96: Essentially Yours: The Protection of Human Genetic Information in Australia.
2005	The Office of the Privacy Commissioner conducts a review of the private sector provisions of the Privacy Act.
2005	The Senate Legal and Constitutional References Committee reports on the findings of its inquiry: *The Real Big Brother: Inquiry into the Privacy Act 1988.*
2008	The Australian Law Reform Commission releases ALRC Report 108: *For your information – Australian privacy law and practice*. This review responded to recommendations for broader review arising from both 2005 reports.
2010	The *Australian Information Commissioner Act 2010* (Cth) establishes the Office of the Australian information Commissioner. The role of Privacy Commissioner becomes a statutory office within the Office of the Australian Information Commissioner, under the Information Commissioner.
2014	The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* commences, implementing many significant reforms and significantly implementing ALRC Report 108. These reforms include: • replacing the IPPs and the NPPs with a single set of 13 Australian Privacy Principles (the APPs), • enhanced credit reporting requirements, • new powers for the Information Commissioner to create and register binding codes of practice, and • new enforcement powers for the Information Commissioner.

2014	The Australian Law Reform Commission releases ALRC Report 123: Serious Invasions of Privacy in the Digital Era, outlining a draft design for a statutory cause of action for serious invasions of privacy, and considering other innovative ways to reduce serious invasions of privacy in the digital era.
2015	The Parliamentary Joint Committee on Intelligence and Security considers privacy as part of its broader consideration of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, recommending that new mandatory data breach notification scheme be introduced.[486]
2018	The *Privacy Amendment (Notifiable Data Breaches) Act 2017* comes into effect, establishing a scheme under which agencies and organisations must report eligible data breaches to the Office of the Australian Information Commissioner.
2019	The ACCC's Digital Platforms Inquiry considers privacy law issues in the context of consumers' use of digital platforms, recommending that this review be conducted.

[486] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Report, 27 February 2015) Recommendation 38.