IN-DEPTH

Privacy, Data Protection and Cybersecurity

EDITION 10

Contributing editor
Alan Charles Raul
Sidley Austin LLP

LEXOLOGY

Published in the United Kingdom
by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.thelawreviews.co.uk

ISBN 978-1-80449-214-7

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANDERSON LLOYD

ANJIE BROAD LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS LAW FIRM

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

JACKSON, ETTI & EDU

KALUS KENNY INTELEX

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

Chapter 6

AUSTRALIA

Sven Burchartz and Brighid Virtue[1]

I OVERVIEW

The concepts of 'privacy' and 'data protection' are largely treated as coextensive concepts in Australia and are primarily regulated by the Privacy Act 1988 (Cth) (Privacy Act) and, more specifically, the 'Australian Privacy Principles' (APPs) in Schedule 1 of the Privacy Act.

The Privacy Act applies to Australian federal government agencies and private sector 'organisations' with an annual turnover exceeding a specified threshold. It does not apply to individuals acting in their personal capacity and not carrying on a business.

In addition, each Australian state and territory has enacted their own legislation to regulate privacy and data protection by state-based public sector organisations, which are not otherwise subject to the provisions of the Privacy Act.

Specific industries also have their own privacy and data protection legislation and standards. For example:

a Victoria and New South Wales have enacted specific legislation to govern the use and collection of health information,[2] including establishing processes for handling complaints and creating mechanisms for individuals to obtain access to their information; and

b Australia's financial services regulator requires regulated financial services entities to comply with certain Prudential Standards[3] to ensure that regulated entities develop and maintain appropriate information security capabilities.

Australian courts have not yet recognised a specific cause of action based on a breach of privacy, despite the High Court of Australia having contemplated a legal development of this kind more than 20 years ago.[4]

However, the introduction of a statutory tort for serious invasions of privacy that are intentional or reckless is currently being considered as part of the Australian government's review of the Privacy Act and was proposed in Australia's Attorney General's Privacy Act Review Report (Privacy Act Review Report).[5] While it remains unclear whether this will come to fruition, the Office of the Australian Information Commissioner (OAIC) and the Law Council of Australia have openly stated their support for such an introduction.

---

1 Sven Burchartz is a partner and Brighid Virtue is a lawyer at Kalus Kenny Intelex.

2 See the Health Records and Information Privacy Act 2002 (NSW) and the Health Records Act 2001 (Vic).

3 See the Prudential Standard CPS 234 Information Security (CPS 234).

4 *Australian Broadcasting Commission v. Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

5 Attorney General's Department, Privacy Act Review – Report 2022.

Australia is also a party to the International Covenant on Civil and Political Rights (ICCPR) which prohibits unlawful or arbitrary interferences with a person's privacy.[6] However, the ICCPR can only be implemented and enforced in Australia at a domestic level to the extent the ICCPR is ratified under Australian law. While the Privacy Act and equivalent state legislation in Australia provide for some protection of the privacy of individuals, Australia has not yet ratified the ICCPR and has as such not recognised a fundamental right to privacy.

II THE YEAR IN REVIEW

There have been a number of significant changes to the Australian privacy law landscape over the past 12 months.

In late 2022, the Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022[7] passed both houses of the Australian Parliament and became law in Australia. The Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 increased the maximum penalty for serious or repeated privacy breaches to A$2.5 million for individuals and for companies, the greater of A$50 million, three times the value of any benefit obtained through the misuse of information (if the benefit can be determined) or, if the benefit cannot be determined, 30 per cent of a company's adjusted turnover in the relevant period. It also provides the Australian Information Commissioner with greater powers to resolve privacy breaches, among other things.[8]

Also in late 2022, the Australian Minister for Home Affairs and Cyber Security, the Hon. Clare O'Neil MP, announced that the Australian Federal Government will develop a cybersecurity strategy known as the 2023–2030 Australian Cyber Security Strategy (Strategy),[9] to help the Australian government achieve its declared vision of making Australia the most cybersecure nation in the world by 2030.

Since then, Australia's Attorney General released the Privacy Act Review Report, which sets out 116 proposals for reforming the Privacy Act. Some of the more significant reforms proposed in the Privacy Act Review Report include the introduction of:

a a direct right of action available for individuals whose privacy has been interfered with and who have suffered loss or damage as a result;[10]

b a statutory tort for serious and intentional or reckless invasions of privacy;[11]

c a 'right of erasure' which would allow individuals to require that APP entities delete the personal information that APP entity holds about them;[12] and

d in addition to the increased penalties and strengthened OAIC powers which came into effect in December 2022 and are mentioned above, a series of additional measures to strengthen enforcement of the Privacy Act.[13]

6 International Covenant on Civil and Political Rights, 19 December 1966, 999 UNTS 171, Can TS 1976 No 47 (entered into force 23 March 1976), Article 17.

7 Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022.

8 ibid.

9 Discussion Paper, 2023-–2030 Australian Cyber Security Strategy.

10 Australian government – Attorney General's Department, Privacy Act Review – Report 2022, Proposal 26.1.

11 ibid, Proposal 27.1.

12 ibid, Proposal 18.3.

13 ibid, Proposal 25.

Some additional, recent developments in Australia's cybersecurity laws include:

a the passing of the Online Safety Act,[14] which grants the eSafety Commissioner additional powers to regulate online content and impose stricter standards on online service providers;[15]

b amendments to the Surveillance Devices Act 2004 (Cth),[16] which grant enforcement agencies with additional powers to identify and disrupt online criminal activity; and

c amendments to the Autonomous Sanctions Act 2011 (Cth),[17] which allow the relevant Minister to impose targeted sanctions for, among other things, assisting or causing a 'significant cyber incident'.[18]

Finally, in a 2022 decision, the full Federal Court of Australia upheld the Federal Court's earlier finding that, by installing and managing cookies on physical devices of Australian users, there was a prima facie case that Facebook Inc 'carries on business' in Australia for the purposes of the Privacy Act.[19] This decision clarified that even with no physical presence in Australia, a foreign company may still be subject to the Privacy Act, and allowed the Australian Information Commissioner to proceed with its case against Facebook entities for alleged breaches of the Privacy Act.

Facebook was subsequently granted leave to appeal to the High Court of Australia. However, after a change to Australia's Federal Court Rules 2011,[20] the Australian Information Commissioner has successfully applied to revoke the grant of special leave. The OAIC's claims against Facebook, Inc for alleged breaches of the Privacy Act and its role in the Cambridge Analytica scandal can now proceed.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The Privacy Act 1988 (Cth) – Who does it protect and who does it apply to?

The Privacy Act applies to Australian federal government agencies[21] and certain private 'organisations'. 'Organisations' included any person or entity that carries on a business in Australia,[22] but does not include:

a small business operators – being organisations with an annual turnover of A$3 million or less;

b registered political parties; and

c state or territory authorities.

14 Online Safety Act 2021 (Cth).

15 Explanatory Memorandum, Online Safety Bill 2021 (Cth).

16 See the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth).

17 See the Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021 (Cth).

18 Explanatory Memorandum, Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Bill 2021.

19 *Facebook Inc v. Australian Information Commissioner* [2022] FCAFC 9.

20 Federal Court Legislation Amendment Rules 2022 (Cth) Rule 2(1), Schedule 1 Clause 13.

21 Privacy Act 1988 (Cth) Section 6(1).

22 ibid., Section 6(c).

Certain businesses are specifically excluded from the 'small business operator' exemption, including (but not limited to) organisations that provide health services, credit reporting bodies, businesses that sell or purchase personal information or otherwise handle sensitive information as defined within the Privacy Act.[23]

The removal of the small business exemption has been proposed by the Attorney General in the Privacy Act Review Report.[24]

Organisations that are subject to the Privacy Act and APPs are known as APP entities.

What types of information are regulated by the Privacy Act?

The Privacy Act governs the use, collection and disclosure of personal information.

The concept of personal information under the Privacy Act is very broad and is defined as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not'.[25]

Personal information includes (but is not necessarily limited to):

a an individual's name, signature, address, phone number or date of birth;
b sensitive information, including information about an individual's racial or ethnic origin, political opinions, professional or political or religious affiliations or memberships, sexual orientation or practices, criminal record, health, genetics or biometrics;
c credit information;
d employee record information;
e photographs; and
f IP addresses.

The Privacy Act also defines a number of subsets of personal information that are particularly significant and place specific obligations on the organisations that hold such information, including:

a sensitive information, as mentioned above;
b health information, which is also classified as sensitive information; and
c credit information, including the information provided to credit providers, and information provided by credit providers to a credit reporting body.

The distinction between personal information and sensitive information is particularly important. The collection of sensitive information is prohibited under the Privacy Act unless the individual consents to the collection, whereas personal information may be collected where it is reasonably necessary to conduct an organisation's business.[26]

23 ibid., Section 6D(4).

24 Australian Government – Attorney General's Department, Privacy Act Review – Report 2022, Proposal 6.1.

25 Privacy Act 1988 (Cth) Section 6(1).

26 ibid., Section 3.3.

Australian privacy legislation does not currently differentiate between a data controller and a data processor. Instead, any APP entity which handles personal information is subject to the obligations of the APPs. The introduction of the concepts of data 'controllers' and 'processors' in the Privacy Act is proposed in the Privacy Act Review Report.[27]

Penalties for breach of the Privacy Act

The OAIC may impose penalties for serious and repeated breaches of the Privacy Act. As mentioned above, the maximum penalty has recently increased to A$2.5 million for individuals, and for companies, the greater of the following:

a A$50,000,000;

b if the court can determine the value of the benefit that the body corporate, and any related body corporate, have obtained directly or indirectly and that is reasonably attributable to the conduct constituting the contravention – three times the value of that benefit; or

c if the court cannot determine the value of that benefit – 30 per cent of the adjusted turnover of the body corporate during the breach turnover period for the contravention.

ii General obligations for data handlers

An APP entity may only collect personal information (other than sensitive information) by lawful and fair means, and directly from the individual (subject to some exemptions).[28] APP entities must not collect and hold personal information unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.[29]

While an APP entity does not require express consent to collect personal information (other than sensitive information), the AAP entity must, either at the time of collection or soon as practical after collection occurs, take all reasonable steps to ensure the relevant individuals are aware that their personal information has been collected.[30] Any such notification must include certain information, as set out in the Privacy Act.[31]

Once the personal information has been collected, it must not be disclosed by the APP entity to any third party or used for any purpose other than the purpose for which it was collected, unless:

a the individual consents to such disclosure;

b the information is not sensitive in nature, the individual would reasonably expect the information to be used for such purpose, and such purpose is related to the purpose of the original collection; or

c required by law.[32]

27 Australian Government – Attorney General's Department, Privacy Act Review – Report 2022, Proposal 22.1.

28 Privacy Act 1988 (Cth), APP 3.5.

29 ibid., APP 3.2.

30 ibid., APP 5.

31 ibid., APP 5.2.

32 ibid., APP 6.

APP entities must ensure the security of all personal information they hold, and must destroy or deidentify any personal information that is no longer required for the purpose it was collected.[33] This includes ensuring that personal information is not misused, lost, accessed without authority, modified or disclosed.[34]

iii Data subject rights

Access

APP entities must allow individuals to access their personal information upon request.[35] There are limited circumstances where an APP entity may refuse to allow an individual to access their personal information, including (but not limited to) circumstances where such access may pose a threat to public safety or where the access would impact the privacy of others.[36] Where access is refused, formal written notice outlining the reasons for refusal must be provided to the individual.[37]

APP entities must respond to a request for access within a reasonable time frame.[38]

Where a request to access relates to information held by a government organisation, the APPs operate in conjunction with the federal Freedom of Information Act[39] (FOI Act), which provides the opportunity for individuals to access information held by an Australian government organisation.[40]

Correction

Where an individual requests an APP entity to correct their personal information, or where the APP entity reasonably believes that any personal information it holds is inaccurate, out of date, incomplete or misleading for the purpose of which it is being held, the APP entity must:

a correct the information;

b take reasonable steps to notify other APP entities of the correction; and

c provide the individual with notices or copies of any complaints in relation to the correction.[41]

Portability

While an APP entity must respond to any request from an individual to access their personal information, the Privacy Act does not currently provide for a general right to data portability in Australia.

33 ibid., APP 11.2.

34 ibid., APP 11.

35 ibid., APP 12.

36 ibid., 12.3.

37 ibid., APP 12.9.

38 ibid., APP 12.

39 Freedom of Information Act 1982 (Cth).

40 ibid., Section 3A.

41 Privacy Act 1988 (Cth), APP 13.

However, the Competition and Consumer Act[42] provides a 'Consumer Data Right' for individuals who provide personal information to eligible providers within the Banking Sector in Australia. The Consumer Data Right is designed to give customers more control over their information.[43]

Erasure

The Privacy Act does not provide individuals with the right to require an APP entity to erase their data upon request.

However, APP entities have data correction obligations[44] and obligations to erase or de-identify personal information that is no longer required by law to be held.[45]

The introduction of a right for individuals to require APP entities to erase their personal information upon request is considered in the Privacy Act Review Report.[46]

iv Specific regulatory areas

Workplace records

The Fair Work Act[47] requires employers to hold information in their employee records, which may be personal information under the Privacy Act. Where personal information has been collected in relation to a private sector current or former employee's employment, it is not subject to the APPs. This includes their contact details, salary details, terms of employment, taxation information and banking information. Importantly, the APPs do apply to unsuccessful candidates, and any personal information collected by an employer when being used for a purpose that is not directly related to an individual's employment.[48]

Although some stakeholders had expected the Privacy Act Report to propose removing the employee records exemption, such a proposal was not made. The Attorney General has instead proposed more specific measures to enhance privacy protections for private sector employees.[49]

Health records

While Australian private healthcare providers fall within the definition of 'organisations' and therefore must comply with the Privacy Act, state-funded public healthcare providers are subject only to the requirements of privacy legislations at a state level.

In addition to the Privacy Act, private healthcare providers in New South Wales, Victoria and Australian Capital Territory are also required to comply with the requirements of their respective state's or territory's privacy laws. In Western Australia and South Australia, private healthcare providers are subject only to the Privacy Act and do not have specific state legislation governing how they handle personal information.[50]

42 Competition and Consumer Act 2010 (Cth).

43 Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth).

44 Privacy Act 1988 (Cth), APP 13.

45 ibid., APP 11.2.

46 Australian Government – Attorney General's Department, Privacy Act Review – Report 2022.

47 Fair Work Act 2009 (Cth), Section 535(1).

48 Privacy Act 1988 (Cth), Section 7B(3).

49 Australian Government – Attorney General's Department, Privacy Act Review – Report 2022, Proposal 7.1.

50 OAIC Article, 'Privacy in your state', accessed at: https://www.oaic.gov.au/privacy/privacy-in-your-state.

The My Health Records Act requires organisations that have access to the MyHealth records database to take all reasonable steps to protect healthcare information from misuse, unauthorised access or unauthorised disclosure.[51]

v Technological innovation

Online tracking and use of cookies

Federal and state-based privacy laws in Australia do not explicitly regulate the collection and use of data cookies. However, where cookies collect information which falls within the broad definition of 'personal information' as set out in the Privacy Act, the obligations contained within the APPs may apply.

The introduction of a definition of 'geolocation tracking data' concerning the collection and holding of an individual's precise location by reference to particular places and times is proposed in the Privacy Act Review Report.[52]

Behavioural advertisement

Given that behavioural advertising is a form of direct marketing,[53] APP entities must not use the personal information they hold for the purposes of behavioural advertising (or direct marketing generally), unless:

a the personal information was collected from the individual by the organisation itself, and that individual would reasonably expect that their information may be used for such purpose; and

b the organisation provides a simple means for the individual to opt out of any such behavioural advertising or direct marketing.[54]

In addition, the Competition and Consumer Act prohibits the use of a consumer's information to unfairly target users where it is making a false and misleading claim or where the conduct is considered misleading and deceptive.[55]

The introduction of an unqualified right for individuals to opt out of direct marketing is proposed in the Privacy Act Review Report.[56]

The Australian government is currently considering whether to impose additional obligations on APP entities that conduct online targeted advertising, including whether individuals should have greater rights to self-manage their personal information when collected for the purposes of behavioural advertising.[57]

51 My Health Records Act 2012 (Cth), Section 59.

52 Australian Government – Attorney General's Department, Privacy Act Review – Report 2022, Proposal 4.10.

53 Office of the Australian Information Commissioner (OAIC), 'Australian Privacy Principles guidelines', Chapter 7: Australian Privacy Principle 7 – Direct marketing (Privacy Guidelines, 22 July 2019), accessed at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing/.

54 Privacy Act 1988 (Cth) APP 7.

55 Competition and Consumer Act 2010 (Cth), Schedule 2 (Australian Consumer Law).

56 Australian Government – Attorney General's Department, Privacy Act Review – Report 2022, Proposal 20.2.

57 Australian Government – Attorney General's Department, Discussion Paper – Privacy Act Review 2021.

Facial recognition

Facial recognition information is considered 'sensitive information' under the Privacy Act.[58] This means that information obtained through the use of facial recognition technology must only be collected with prior consent.

Profiling and automated decision making

While the Privacy Act does not regulate artificial intelligence and automated decision-making technologies specifically, the APPs provide that personal information may only be used for the primary purpose for which it was collected. Personal information can only be used for a secondary purpose if an individual would reasonably expect that the APP entity would use their personal information for such secondary purpose, and the secondary purpose is related to the purpose of collecting the information in the first instance.[59]

On this basis, unless an APP entity has notified the individual of their personal information being collected for the purposes of profiling and automated decision-making technologies, this privacy principal cannot be satisfied.

Anonymisation and de-identification

While there are no specific obligations under the Privacy Act for organisations to anonymise or de-identify personal information, individuals have some rights to not identify themselves or to use a pseudonym when dealing with an APP entity.[60]

When personal information has been appropriately anonymised or de-identified it will no longer be 'personal information' as defined in the Privacy Act.[61] In order to anonymise or de-identify personal information correctly, any information that may identify an individual must either be amended or removed, together with any other information that could be used to re-identify an individual.

A prohibition on APP entities re identifying de identified information obtained other than directly from the individual to whom the information relates is proposed in the Privacy Act Review Report.[62]

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

i Restrictions on international data transfers

Personal information must not be disclosed to an organisation outside Australia unless the disclosing organisation has taken steps to reasonably ensure that the recipient of the information does not breach the APPs.[63]

58 Privacy Act 1988 (Cth), Section 6(1).

59 ibid., APP 6.1.

60 ibid., APP 2.1.

61 OAIC, 'De-identification and the Privacy Act', accessed at https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act.

62 Australian Government – Attorney General's Department, Privacy Act Review – Report 2022, Proposal 4.6.

63 Privacy Act 1988 (Cth), APP 8.1.

However, this obligation does not apply where:

a the disclosing organisation reasonably believes that the recipient is subject to laws with similar protections to the provisions of the APPs;

b the individual has provided their express consent to the disclosure, knowing that by providing consent, the recipient is not required to comply with the Privacy Act; and

c the disclosure is required by law or court order.[64]

ii Data localisation requirements

While the Privacy Act does not specifically restrict data localisation outside of Australia, an APP entity must ensure that the personal information it holds is not disclosed to overseas entities without complying with the restrictions on international data transfers described above.[65]

However, there are data localisation rules for specific industries where the nature of the personal information held is particularly sensitive. For example, information relating to an individual's medical records[66] and financial and taxation information[67] must be stored in Australia.

V COMPANY POLICIES AND PRACTICES

All APP entities must have a current privacy policy and take all reasonable steps to ensure the privacy policy is easily accessible.[68] Most organisations choose to include their privacy policy on their website to satisfy this requirement.

The privacy policy of an APP entity must include details of how the organisation collects and handles personal information,[69] including, for example:

a what and how personal information will be collected;

b where the personal information will be stored;

c the reasons for collection of personal information; and

d how personal information will be used or disclosed.

APP entities must also take reasonable steps to implement internal policies and practices to ensure that the APPs are complied with.[70] This should include standard practices for impact assessments, data breach response plans, conducting internal privacy training and implementing policies for managing privacy complaints and enquires.[71]

64 ibid., APP 8.1.

65 ibid., APP 8.

66 My Health Records Act 2012 (Cth), Section 77.

67 Privacy Act 1988 (Cth), Section 20Q(3).

68 ibid., APP 1.5.

69 ibid., APP 1.4.

70 ibid., APP 1.2.

71 OAIC, 'Privacy management framework: enabling compliance and encouraging good practice', accessed at https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-framework-enabling-compliance-and-encouraging-good-practice.

VI DISCOVERY AND DISCLOSURE

i Disclosure in relation to Australian laws

Generally, personal information can only be used or disclosed by an APP entity for the primary purpose for which it was collected.[72]

However, the Privacy Act provides some exceptions to this requirement which relate to matters of Australian law, law enforcement or court procedures, including where:

a disclosure is required by or under Australian law or a court/tribunal order;[73]

b disclosure is reasonably necessary for the exercise or defence of a legal or equitable claim;[74] and

c disclosure of personal information will assist authorities with locating a missing person[75] or where the APP entity reasonably believes that an individual has engaged in unlawful activity or misconduct of a serious nature.[76]

ii Response to foreign government requests

An APP entity holding personal information must ensure that any overseas disclosure, including where required by foreign law or in accordance with a court order from a foreign jurisdiction, complies with the disclosure requirements set out in the Privacy Act.[77]

However, the disclosure subject to foreign laws or a foreign court order will not constitute a breach of the Privacy Act by the relevant APP entity where an overseas recipient (which has received personal information in accordance with the provisions of the Privacy Act) discloses personal information in accordance with the law or a court order in its jurisdiction.[78]

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The OAIC is the independent Australian government agency primarily responsible for enforcing the Privacy Act. Its functions include (but are not limited to) guidance, monitoring and advice related functions.[79]

The powers of the OAIC include:

a monitoring the security and accuracy of information held by an entity, where that information is information to which Part IIIA of the Privacy Act applies; and

b examining the records of entities to ensure that they are not using information for unauthorised purposes and are taking steps to adequately prevent the unlawful disclosure of such information.[80]

72 Privacy Act 1988 (Cth) APP 6.1.

73 ibid., APP 8.2(c).

74 Privacy Act 1988 (Cth) Section 16A(1), Item 4.

75 ibid., Item 3.

76 ibid., Item 2.

77 OAIC, 'Chapter 8: APP 8 – Cross-border disclosure of personal information', accessed at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information.

78 Privacy Act 1988 (Cth) Section 13D.

79 ibid., Section 27(1).

80 ibid., Section 28A.

The OAIC has broad investigative powers where an individual has lodged a formal complaint regarding interference with their privacy, but also has discretionary investigative powers to (at the OAIC's initiative):

a investigate an act or practice that may be an interference with the privacy of an individual or a breach of the APPs; and

b conduct an assessment of whether personal information held by an APP entity is being maintained and handled in accordance with the APPs.[81]

Where the OAIC has commenced an investigation at its own initiative, the OAIC may:

a correspond with the respondent and other sources as required to gather information. Importantly, the OAIC may compel a person to provide information, produce documents or give evidence to the OAIC as part of any such investigation; and

b form a preliminary view in relation to the matter and choose whether to discontinue the investigation or take appropriate regulatory action.[82]

The process followed by the OAIC when investigating a formal privacy complaint is generally more involved and often includes the OAIC attempting to conciliate the complaint. Where the complaint cannot be resolved by conciliation, the OAIC may determine to take regulatory action.[83]

Examples of the regulatory and enforcement actions that the OAIC may take include:

a issuing an infringement notice to a person who fails to give information, answer a question or produce a document to the OAIC when that person is required to do so under the Privacy Act;[84]

b seeking an injunction against a person to enforce the Privacy Act; or

c where a civil penalty provision of the Privacy Act has been breached (for example, serious and repeated interferences with privacy),[85] the Commissioner applying to the courts for a civil penalty order.[86]

The OAIC also has the power to apply to the court for an order that an entity pay the Commonwealth of Australia a penalty, because of their alleged contravention of the Privacy Act.[87]

81 ibid., Section 33C(1)(a)(i).

82 OAIC, 'Guide to Privacy Regulatory Action Chapter 2: Commissioner Initiated Investigations and Referrals, accessed at https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-2-commissioner-initiated-investigations-and-referrals.

83 OAIC, 'Guide to Privacy Regulatory Action Chapter 1: Privacy Complaint Hangling Process', accessed at https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-1-privacy-complaint-handling-process.

84 Privacy Act 1988 (Cth), Section 80UB.

85 Privacy Act 1988 (Cth), Section 13G.

86 OAIC, 'Guide to privacy regulatory action Chapter 2: Commissioner initiated investigations and referrals', accessed at https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-2-commissioner-initiated-investigations-and-referrals.

87 OAIC, 'Guide to Privacy Regulatory Action Chapter 7: Civil Penalties', accessed at https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-civil-penalties.

As mentioned above, the maximum penalty for serious and repeated breaches of privacy has recently increased to A$2.5 million for individuals and for companies, the greater of A$50 million, three times the value of any benefit obtained through the misuse of information (if the benefit can be determined) or, if the benefit cannot be determined, 30 per cent of a company's adjusted turnover in the relevant period.

Beyond the OAIC, there are a number of Australian regulators responsible for certain aspects of privacy and data protection in Australia. This includes Australia's primary competition regulator and consumer law watchdog, the Australian Competition and Consumer Commission (ACCC).[88] The ACCC, together with the OAIC, is responsible for monitoring compliance with the 'Consumer Data Right', which is a regulatory framework designed to provide consumers with greater choice and control over the personal data Australian businesses hold about them.[89]

ii Recent enforcement cases

Joint investigation into the Latitude Financial Corporate Group

In May 2023, the OAIC, along with the New Zealand Office of the Privacy Commissioner, commenced a joint investigation into how the 'Latitude Financial' corporate group (Latitude) handles the personal information of its customers.[90] The joint investigation was announced after Latitude experienced a data breach which resulted in 7.9 million Australian and New Zealand customers' drivers' licence details being stolen.

The investigation will focus on whether reasonable steps were taken by Latitude to destroy or de-identify its former customers' personal information. It is alleged that of the affected individuals, only 3.2 million individuals details were provided to Latitude (or associated entities) within the past 10 years.

This investigation is ongoing, and is the first joint investigation by Australia and New Zealand.

Investigations into Medibank and Optus

In December 2022, the OAIC commenced separate investigations into Medibank (one of Australia's largest private health insurance providers) and Optus (one of the largest telecommunications companies in Australia), pursuant to the powers set out in Section 40(2) of the Privacy Act. These investigations came after both Optus and Medibank experienced significant data breaches.

Optus reported that as a result of its data breach, approximately 10 million current and former customers had their personal data stolen.

88 ACCC, 'About us', accessed at https://www.accc.gov.au/about-us.

89 ACCC, 'Focus Areas: Consumer data right (CDR)', accessed at https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0.

90 'Joint Australia–New Zealand investigation into Latitude group', accessed at: https://www.oaic.gov.au/newsroom/joint-australianew-zealand-investigation-into-latitude-group.

Medibank reported that as a result of its data breach, approximately 9.7 million current and former customers had their personal data stolen.

The main focus of the OAIC's investigations is whether Optus and Medibank took reasonable steps to protect the personal information that they hold from misuse, interference, loss, unauthorised access, modification or disclosure in accordance with their obligations under the Privacy Act.[91]

It is expected that the investigations will take some time to complete, and an outcome will not be seen until 2024.

OAIC proceedings against Facebook

In March 2020 the OAIC commenced proceedings against Facebook Inc and Facebook Ireland Pty Ltd (together, Facebook),[92] alleging that the personal information of its users had been disclosed for a purpose other than the purpose for which it was collected, and was at risk of being disclosed to Cambridge Analytica and used for political profiling.

The OAIC alleges that, as a result of this conduct, Facebook committed serious or repeated interferences with privacy in breach of the Privacy Act. The OAIC is seeking civil pecuniary penalties against Facebook for the alleged breaches. This is the first time that the OAIC has sought civil pecuniary penalties of this kind.

The Federal Court granted the OAIC leave to serve originating process documents on Facebook in respect of the alleged breaches. Although this was merely a procedural step and provides little insight into the likely outcome of the case, it does demonstrate the Court's view that the OAIC had at least a prima facie case against Facebook.

Facebook appealed the Court's decision to grant the OAIC leave to serve the originating process. However, the full bench of Australia's Federal Court rejected that appeal in February 2022. The full bench's decision provided some important commentary in relation to when businesses based outside of Australia will be considered to have an 'Australian link' and therefore be subject to the extra-territorial application of the Privacy Act.

The Federal Court's decision upheld the primary judge's view that installing cookies on devices located in Australia could be considered 'carrying on a business', in which case an Australian link is established and Facebook is subject to the Privacy Act.

This case is ongoing and it remains to be seen whether the findings of the full Federal Court will be contested in subsequent proceedings.

Following Facebook's unsuccessful appeal in the Federal Court, Facebook was granted leave to appeal to the High Court of Australia. However, after a change to Australia's Federal Court Rules 2011,[93] the Australian Information Commissioner was successful in an application to revoke the grant of special leave for Facebook to appeal to the High Court of Australia. The High Court unanimously decided that because of those changes to the Federal Court Rules, Facebook's grounds for appeal were no longer of public importance.[94] This means that the OAIC can serve proceedings on Facebook and the matter will progress through the courts. This case is ongoing.

91 Privacy Act 1988 (Cth), APP 11.

92 *Facebook Inc v. Australian Information Commissioner* [2022] FCAFC 9.

93 Federal Court Legislation Amendment Rules 2022 (Cth) Rule 2(1), Schedule 1 Clause 13.

94 *Facebook Inc v. Australian Information Commissioner* [2023] HCATrans 22 (7 March 2023).

iii Private litigation

Currently, there is no specific statutory right or cause of action which private plaintiffs can commence legal proceedings for a data breach, or otherwise a breach of their privacy, in Australia. In light of this, it is difficult for private plaintiffs to bring privacy claims, including privacy class actions, in our jurisdiction. Generally, where an individual's privacy has been breached, that individual must decide whether to make an individual or representative complaint to the OAIC.

However, there have been instances in Australia where individual or groups of claimants have commenced legal proceedings for other causes of action under Australian law (for example, breach of contract or misleading and deceptive conduct), depending on the circumstances of the breach and the relationship between the private plaintiff and the entity that allegedly breached their privacy or caused a data breach.

In December 2019, the NSW Supreme Court accepted a A$275,000 settlement as fair and reasonable in a data breach class action. This was the first class action of its kind in Australia.[95]

Recently, a number of class actions have been commenced against Optus and Medibank over the data breaches outlined in Section VII.ii. These are the first data class actions to be bought after the first one was settled in 2019.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Before disclosing personal information about an individual to a person who is not in Australia or an external territory (i.e., an overseas recipient), APP entities must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.[96] In practice this generally means the entity disclosing the information must ensure that it enters into a confidentiality or privacy agreement with the overseas recipient, which imposes an obligation on the overseas recipient to:

a handle the disclosed information as if its handling of that information were subject to the APPs; and

b not handle the information in a way that would amount to a breach of the APPs.

It is expected that further clarification of the specific obligations of APP entities to ensure overseas recipients do not breach the APPs will form part of the Privacy Act reforms currently underway.

The Privacy Act provides that APP entities that disclose personal information to overseas recipients are accountable for any act or practice of the overseas recipient, as they relate to the personal information that is disclosed, including any acts or practice that fail to comply with the APPs.[97]

Although the Privacy Act contains obligations on APP entitles in relation to sharing personal information with overseas entities, there are no general data localisation

95 *Evans v. Health Administration Corporation* [2019] NSWSC 1781.

96 ibid., APP 8.

97 ibid., Section 16C.

requirements. There are, however, some industry-specific prohibitions on certain types of personal information being shared or held outside of Australia; for example, under the My Health Records Act 2012 (Cth) discussed in Section III.iv.[98]

Finally, the Privacy Act also contains extraterritoriality provisions setting out when the Privacy Act will apply to act or practices taken part in outside of Australia and the external territories.[99] In particular, these extraterritorial provisions provide that the Privacy Act will apply to acts and practices of organisations that have an Australian link, even if the relevant act or practice is engaged in outside of Australia and the external territories.

An Australian link will be established if the organisation carries on business in Australia and collected or held the personal information in Australia at the time of the breach.[100] However, an act or practice will not be an interference with the privacy of an individual if the act or practice is required by an applicable law of a foreign country.[101]

IX CYBERSECURITY AND DATA BREACHES

i Safeguarding requirements

The Privacy Act requires APP entities to take all reasonable steps to protect the personal information that they hold from:

a misuse;
b interference and loss; and
c unauthorised access, modification or disclosure.[102]

While these obligations do not relate only to information stored on computer systems, networks and databases, the nature of these obligations can be seen to place general cybersecurity obligations on APP entities for the personal information that they hold.

Examples of reasonable steps that should be taken by APP entities to comply with these obligations include:

a conducting internal training and regularly reviewing the internal governance practices, procedures and systems of the relevant APP entity;
b taking positive steps to access the security practices of the relevant APP entity, as well as the security of third-party providers; and
c de-identifying and destroying personal information held by the relevant APP entity as soon as that information is no longer required for the collection purpose.[103]

The OAIC has noted that there is no definitive list of reasonable steps to be taken, and that the steps that are reasonable for one APP entity will likely depend on their circumstances.[104]

98 My Health Records Act 2021 (Cth), Section 77.
99 Privacy Act 1988 (Cth), Section 5B.
100 ibid., Section 5B(3).
101 ibid., Section 13D.
102 Privacy Act 1988 (Cth), APP 11.
103 OAIC, 'Australian Privacy Principles guidelines Chapter 11: APP 11 – Security of personal information', accessible at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information.
104 ibid.

In addition, entities that are regulated by Australia's financial regulator are required to (among other things) maintain an information security capability that is proportionate to the size and extent of threats to its information assets.[105]

ii Notifiable Date Breach Scheme

The OAIC's Notifiable Data Breach Scheme requires APP entities to notify affected individuals and the OAIC of a data breach if that data breach is an 'eligible data breach' because it occurred after 22 February 2022 and the following criteria are met:

a unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur);

b this unauthorised access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates; and

c the APP entity has not been able to prevent the likely risk of harm with remedial action.[106]

Currently, the Australian Information Commissioner expects APP entities to assess and notify the OAIC and affected individuals of an eligible data breach within 30 days of becoming aware of the breach. However, a reduction in that time frame to 72 hours is proposed in the Privacy Act Review Report.[107]

X SOFTWARE DEVELOPMENT AND VULNERABILITIES

While Australia does not have any specific legal requirements for secure software development, the Australian Signals Directorate (the Australian government agency responsible for foreign signals intelligence, support to military operations, cyberwarfare, and information security) through its 'Australian Cyber Security Centre' has developed an Information Security Manual and Guidelines for Software Development (Guidelines).[108]

The Australian Signals Directorate also encourages businesses to develop processes and procedures to assist in identifying, verifying, resolving and reporting on vulnerabilities disclosed by people who may be internal or external to the business (known as a vulnerability disclosure programme).[109] However, this is not yet a legal requirement.

105 APRA, 2019, Prudential Standard CPS 234, accessible at https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf.

106 OAIC, 'When to report a data breach', accessible at https://www.oaic.gov.au/privacy/notifiable-data-breaches/when-to-report-a-data-breach.

107 Australian Government – Attorney General's Department, Privacy Act Review – Report 2022. Proposal 28.2.

108 Australian Signals Directorate, 'Information Security Manual', Guidelines for Software Development, accessed at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-software-development.

109 Australian Signals Directorate, 'Vulnerability Disclosure Programs Explained', accessed at https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/vulnerability-disclosure-programs-explained.

XI DIGITAL GOVERNANCE AND CONVERGENCE WITH COMPETITION POLICY

In 2020, the Australian government directed the ACCC to commence a formal price inquiry into markets for the supply of digital platform services (the Inquiry). The Inquiry is ongoing. Pursuant to the Inquiry, the ACCC is considering (among other things) practices of suppliers in digital platform services markets that may result in consumer harm, market trends that may affect the nature and characteristics of digital platform services and developments in markets for the supply of digital platform services outside Australia.

The services covered by the Inquiry include:

a digital platform service, including but not limited to internet search engines, social media services and online private messaging services;

b digital advertising supplied by digital platform service providers; and

c data collection, storage, supply, processing and analysis services supplied by:

- digital platform service providers; and
- data brokers.[110]

The Final report is due on 31 March 2025.

XII OUTLOOK

The regulation of privacy and cybersecurity in Australia is anticipated to undergo significant changes in the next year as a result of the Attorney General's Privacy Act Review Report and the Australian government's ongoing review of the Privacy Act.

As discussed above, the Privacy Act Review Report proposes a number of changes to Australia's regulatory framework in respect of privacy and cybersecurity including the scope of the Privacy Act and how it is applied and enforced, whether individuals should have access to a cause of action or other rights to enforce privacy obligations under the Privacy Act and whether a statutory tort for serious invasions of privacy should be introduced into Australian law.[111]

The Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Online Privacy Bill) proposes to introduce significant changes to the privacy law landscape in Australia, including:

a the introduction of the Online Privacy Code which is intended to provide for stronger regulation of social media and online platforms that collect or trade in personal information;

b the introduction of wider investigative powers of the OAIC; and

c harsher penalties under for certain kinds of breach under the Privacy Act.[112]

110 Josh Frydenberg, Treasurer, 'Competition and Consumer (Price Inquiry – Digital Platforms) Direction 2020', accessed at https://www.accc.gov.au/system/files/Ministerial%20direction%20-%20Digital%20platform%20services%20inquiry.pdf.

111 ibid.

112 ibid.

ISBN 978-1-80449-214-7