Russell Kennedy Government CPD

Privacy Update — An overview of key developments over the past year and what to expect in 2023

24 March 2023

Gina Tresidder, Principal

Webinar housekeeping

- All attendees will be on mute and their cameras turned off for the entire webinar
- We have BD tech support live to assist with any technical issues
- Use the chat function for any comments/technical issues
- Use the Q&A function for specific questions related to the webinar content – Questions will be addressed at the end of the webinar
- There will be a post webinar survey link sent at the end of the webinar. We value attendee feedback
- We will also have a QR code linking to our feedback survey towards the end of the presentation so you can provide instant feedback

Disclaimer

The information contained in this presentation is intended as **general commentary only** and should not be regarded as legal advice

Should you require specific advice on the topics or areas discussed, please contact the presenters directly

Introduction

Privacy Update

This session will cover:

1. Recent changes to the *Privacy Act 1988* (Cth)
2. Victorian Health Data Sharing Bill
3. Proposed future changes to the privacy landscape - Attorney-General's Privacy Act Review Report
4. Case studies – **Optus** and **Medibank**

Key Legislation

Key Legislation

Commonwealth

- The ***Privacy Act 1988*** (Cth) (the Act) imposes obligations on 'APP entities', namely:
  - Agencies: federal government entities and/or office holders; and
  - Organisations: includes individuals, body corporates, partnerships, unincorporated associations, trusts.
- The Act contains 13 **Australian Privacy Principles** (APPs) which address the collection, use and disclosure of personal information.

Victoria

- The ***Privacy and Data Protection Act 2014*** (Vic) (PDP) contains 10 **Information Privacy Principles** (IPPs) that outline how Victorian public sector organisations must handle personal information.
- The ***Victorian Protective Data Security Standards*** (VPDSS) establish 12 high level mandatory requirements to protect public sector information across all security areas including governance, information, personnel, Information Communications Technology (ICT) and physical security.
- The ***Health Records Act 2001*** (Vic), outlines how Victorian public sector agencies and health service providers manage health information.

Recent Changes

Recent Changes to the Privacy Act

The ***Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022*** (the **Amending Act**) came into force on 13 December 2022.

The Amending Act **increased the maximum civil penalty** for a serious and/or repeated interference with privacy for a body corporate to the greater of:

- **$50 million**;
- three times the value of the benefit obtained by the body corporate from the conduct constituting the serious and/or repeated interference with privacy; or
- if the value cannot be determined, 30% of the body corporate's 'adjusted turnover' during the 'breach turnover period'.

Recent Changes to the Privacy Act

The Amending Act strengthened the Commissioner's enforcement functions by:

- **expanding the declaration types** the Commissioner can make after investigating a complaint. The Commissioner can now make a range of declarations under section 52 of the Act, including requiring an entity to:
    - publish a statement about their conduct;
    - engage a 'suitably independent and qualified adviser' to review the process of compliance undertaken by the entity to improve their practice;
    - take specified steps to ensure their conduct constituting an interference with an individual's privacy is not repeated or continued.
- **allowing the imposition of infringement notices**, for failure to comply with notices requiring the production of documents or the answering of questions about an actual or suspected eligible data breach.
- **expanding the scope of the Privacy Act** where foreign entities are now required to comply with the Act's obligations so long as they carry on a business in Australia.

Recent Changes to the Privacy Act

The Amending Act has further strengthened the Commissioner's enforcement functions by:

- **requiring more specific information** from entities about eligible data breaches, by directing an entity to prepare a statement that includes the 'particular' kinds of information that may be breached to provide more specific knowledge to better assess the risk of harm to certain individuals who have had their data breached;
- **providing new powers to conduct assessments** where the Commissioner can require a person or entity to provide information or documents if they are suspected of possessing information in relation to an actual or suspected eligible data breach of an entity, or an entity's compliance with notification requirements under Division 3 of Part IIIC of the Act.

Recent Changes to the Privacy Act

The Amending Act has strengthened the Commissioner's information sharing functions by:

- **allowing the sharing of information with other bodies** for the purpose of exercising its own functions and duties under the Act or for the receiving body to exercise its own functions and duties. This includes an enforcement body, alternative complaint body, State or Territory authority, or an authority of the government of a foreign country that has functions to protect the privacy of individuals. Safeguards are in place to ensure information is only shared if the Commissioner is satisfied on reasonable grounds that the receiving body has satisfactory arrangements for protecting information or documents.
- **allowing the publication of determinations** on the OAIC website; and
- **allowing disclosure of information in the public interest**.

Victorian Health Data Sharing Bill

- The *Health Legislation Amendment (Information Sharing) Bill 2021* (Vic) has now passed both houses.
- This will establish a **centralised electronic system** to allow public hospitals and other health services to share patient health information.
- In Victoria, a patient's medical history can be held across various health services. Establishing a consolidated health information sharing platform is expected to **improve patient outcomes** by ensuring access to records in urgent situations where the patient is unable to provide this information.
- Only people engaged or employed by a participating health service will be authorised to access the system.
- The Bill introduces **two new criminal offences** to specifically deal with unauthorised access.
- This is important, because patients are **unable to opt-out** of the information sharing requirements set out in the Bill, and their **consent is not required** for their information to be included.
- There were last minute amendments to the legislation in the Upper House which did not result in a formal opt-out option for patients but instead a Privacy Management Framework must be established to "lock down" and prevent access to patient nominated sensitive information.

Attorney-General's Privacy Act Review Report

Attorney-General's Privacy Act Review Report

- Following the Australian Competition and Consumer Commission's (**ACCC**) 2019 Digital Platforms Inquiry final report, a review of the Privacy Act 1988 (**Act**) was instigated.
- After an extensive consultation period from October 2020 to January 2022, the **Attorney-General's Privacy Act Review Report** was released on 16 February 2023.
- A total of **116 proposals** have been made by the Attorney-General designed to better align Australia's laws with global standards of information privacy protection.
- The Government is seeking feedback by **31 March 2023**.

Attorney-General's Privacy Act Review Report

1. **Changes to 'small business' exemption** (Proposal 6)

- The removal of the 'small business' exemption under the Act to require compliance from more businesses.
- An impact analysis is suggested to be undertaken to better understand the impact of removing this exemption, and consulting small businesses to assist with compliance under the Act.

2. **Introduction of a 'fair and reasonable' test** (Proposal 12)

- Requirement for the collection, use, and disclosure of personal information to be 'fair and reasonable' in the circumstances.
- This will be determined objectively from the perspective of a reasonable person.
- This test will apply irrespective of whether consent has been obtained (exceptions for APPs 3.4 and 6.2).

Attorney-General's Privacy Act Review Report

3. **Additional rights for individuals** (Proposal 18)

- Provide individuals with a **right of access** and explanation about their personal information (including the source) if they request it.
- Introduction of a **right to object** to the collection, use or disclosure of personal information.
- Introduction of a **right to erasure** for any of their personal information.
- Introduction of a **right of de-indexing online search results** containing sensitive, inaccurate, or excessively detailed information.
- Relevant exceptions apply to these rights, including competing public interests, conflicts with legal documents, or technical infeasibilities.

4. **Requirement for a Privacy Impact Assessment for high privacy risk activities** (Proposal 13)

- APP entities will be required to conduct a Privacy Impact Assessment prior to the commencement of a high privacy risk activity.
- A high privacy risk activity will be one that is 'likely to have a significant impact on the privacy of individuals', with the OAIC setting factors that may indicate a high privacy risk to assist APP entities.

Privacy Act Review Report – Main Proposals (Further Protections under the Act)

5. Introduction of 'controllers' and 'processors' (Proposal 22)

- These concepts may cause a non-APP entity to be brought within the scope of the Act if they process information on behalf of an APP entity controller.

6. Enhancements to the Notifiable Data Breach (NDB) scheme (Proposal 28)

- If there are reasonable grounds to believe there is an eligible data breach, entities are required to provide a copy of the statement to the Commissioner within 72 hours after the entity becomes aware, and to notify individuals as soon as practicable.
- Any statement provided to the Commissioner must set out the steps the entity has taken or intends to take in response to the breach.

7. Additional obligations for 'de-identified' information (Proposals 4.5-4.8)

- Amending the definition of 'de-identified' to ensure that information is treated in a way that ensures no individual can be identified or reasonably identified.
- Introducing a criminal offence for malicious re-identification of de-identified information.

Attorney-General's Privacy Act Review Report

8. Change in operation of 'consent' (Proposal 11)

- Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.
- Expressly recognise the ability for persons to withdraw consent, and to do so as easily as the provision of consent.

9. Enforcement and Penalties (Proposals 25–27)

- Creation of **tiers of civil penalty** provisions allow for better targeted regulatory responses from the OAIC.
- Create a **direct right of action** to permit individuals to apply to the courts for relief in relation to an interference with privacy.
- Introduce a **statutory tort of privacy** for serious invasions of privacy.

Case Studies of Recent Major Data Breaches

Case study into Optus

- On 20 September 2022, Singtel Optus Pty Ltd (Optus) became aware of unusual activity on their systems.
- On 22 September 2022, Optus became aware of a data breach and released a media statement regarding the breach.
- On 24 September 2022, a ransom of $1 million USD was asked by the criminal threatening to release the data on the dark web if the ransom was not paid.
- Optus did not respond to the ransom requests, and on 26 September 2022, the criminal posted 10,000 individuals' records on the dark web.
- Shortly after releasing the data, on 27 September 2022, due to the publicity of the matter, the criminal deleted their earlier posts and issued an apology to the 10,000 individuals who have been affected by the data leak. The criminal further claimed that they deleted all records of customer data that it had acquired from Optus, however, this has not been confirmed by Optus.
- Since the data breach, Optus has been cooperating with Australian Federal Police (**AFP**), and State and Territory police to set up Operation Guardian to assist the 10,000 individuals at risk of identity fraud due to the data leak. Additionally, Optus has commissioned an independent external review of its cyberattack to better understand how the attack occurred and to learn how to prevent such an incident from occurring again.

Case study into Optus

The stolen data included:

- 9.8 million customers' names, dates of birth, phone numbers, email addresses.
- For a subset of customers, addresses, ID document numbers (including driver's licence, passport numbers, Proof of Age cards, and Medicare ID numbers).

Optus believes the following was not exposed:

- Payment details and account passwords.

OAIC investigation into Optus

OPTUS

- The Office of the Australian Information Commissioner (**OAIC**) recently commenced an investigation into the handling practices of Optus over its major data breach in 22 September last year.
- The OAIC will investigate whether Optus took reasonable steps to protect the personal information they held from misuse, interference, loss, unauthorised access, modification or disclosure. It will also consider whether the information collected and retained by Optus was necessary to carry out their business. Additionally, the OAIC will consider whether Optus took reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs.
- The investigation will be a co-ordinated with the Australian Communications and Media Authority (**ACMA**).
- If the Commissioner is satisfied that an interference with the privacy of individuals has occurred, the Commissioner may make a determination including requiring Optus to take steps to ensure the act or practice is not repeated or continued, and to redress any loss or damage. Civil penalties of up to $2.2 million for each contravention of serious and/or repeated interferences with privacy may be issued by the Federal Court as well (noting that these data breaches occurred before the introduction of higher civil penalties).
- The OAIC will not comment further until the conclusion of its investigation.

Class Actions against Optus

There are currently two potential class actions underway against Optus

- **Maurice Blackburn** has made a representative complaint to the OAIC against Optus and invites past or present Optus customers to register to receive updates about the class action investigation into any potential action and compensation which may be sought on their behalf.
- **Slater + Gordon Lawyers** are also investigating a potential class action against Optus and have invited interested affected parties to register with them.

Case study into Medibank

- On 13 October 2022, Medibank Private Ltd (Medibank) became aware of unusual activity on their systems.
- Throughout October, Medibank received messages and claims that their customer data had been stolen. On 20 October, Medibank became aware of stolen data after receiving a sample of 100 customer records from ahm and international student policy management systems. On 25 October, Medibank received a further 1000 customer records, relating to Medibank, international student, and ahm customers.
- On 26 October, Medibank became aware that significant amounts of data had been stolen.
- On 7 November, Medibank announced they would not be making any ransom payment, believing there was only a limited chance a ransom payment would prevent the personal data from being published.
- From 9 November onwards, the criminal began to release customer data on a dark web forum before releasing all stolen data on 1 December on the dark web.

Case study into Medibank

The stolen data included:

- Name, date of birth, address, phone number, and email addresses for around 9.7 million current and former customers and some of their authorised representatives (this includes 5.1 million Medibank customers, 2.8 million ahm customers, and 1.8 million international customers).
- Medicare Numbers (but not expiry dates) for ahm customers.
- Passport numbers (but not expiry dates) and visa details for international student customers.
- Health claims data for 160,000 Medibank customers, 300,000 ahm customers, and 20,000 international customers (this includes names of service providers and their location, as well as the codes associated with diagnosis and procedures administered where customers received certain medical procedures).
- Personal and health claims data for 5,200 My Home Hospital (**MHH**) patients.
- Contact details for 2,900 next of kin for these MHH patients.

Medibank believes the following was not exposed:

- Health claims data for extra services (such as dental, physio, optical and psychology).

OAIC Investigation into Medibank

- The Office of the Australian Information Commissioner (OAIC) recently commenced an investigation into the handling practices of Medibank over its major data breach in October last year.
- The decision follows the preliminary inquiries commenced by the OAIC in October 2022.
- The OAIC will investigate whether Medibank took reasonable steps to protect the personal information they held from misuse, interference, loss, unauthorised access, modification or disclosure. It will also consider whether Medibank took reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs.
- If the Commissioner is satisfied that an interference with the privacy of individuals has occurred, the Commissioner may make a determination including requiring Medibank to take steps to ensure the act or practice is not repeated or continued, and to redress any loss or damage. Civil penalties of up to $2.2 million for each contravention of serious and/or repeated interferences with privacy may be issued by the Federal Court as well (noting that these data breaches occurred before the introduction of higher civil penalties).
- The OAIC will not comment further until the conclusion of its investigation.

Class Actions against Medibank

There are currently two potential class actions against Medibank:

- **Bannister Law Class Actions**, **Centennial Lawyers**, and **Maurice Blackburn** have joined forces to investigate Medibank for its data breach, after Maurice Blackburn launched a representative complaint with the OAIC in November.
- **Omni Bridgeway** is funding a class action run by **Baker McKenzie**, which was filed with the Federal Court on 7 February 2023.

Q&A – Your Russell Kennedy Contacts

Gina Tresidder
Principal, Corporate and Commercial
P +61 3 8602 7243
E GTresidder@rk.com.au

Feedback

Scan this QR code to provide instant feedback on the session.

Russell Kennedy Lawyers

Russell Kennedy Pty Ltd
info@rk.com.au
russellkennedy.com.au

Melbourne
Level 12, 469 La Trobe Street
Melbourne VIC 3000
PO Box 5146
Melbourne VIC 3001 DX 494 Melbourne
T +61 3 9609 1555 **F** +61 3 9609 1600

Sydney
Level 6, 75 Elizabeth Street
Sydney NSW 2000
Postal GPO Box 1520
Sydney NSW 2001
T +61 2 8987 0000 **F** +61 2 8987 0077