PRIVACY

Mid-year review: 2023

LANDER & ROGERS

Guide

INTRODUCTION

Lander & Rogers' Digital Economy practice has been closely following key privacy developments in Australia amid growing regulatory activity and clampdowns on the privacy practices of companies. Our Privacy Mid-Year Review summarises these key privacy developments.

During the first six months of 2023, a number of significant privacy events shaped the regulatory landscape in Australia. Australian regulators and lawmakers were active in response to high-profile data breaches and privacy incidents.

Privacy and data protection continue to be a hot topic for businesses, industries and sectors across Australia and internationally. The fallout from major data breaches and anticipated privacy law reform has refocused organisations' efforts to uplift privacy compliance and data governance.

We will continue to monitor privacy developments with interest, and anticipate more privacy regulatory and reform activity in the second half of 2023.

Timeline of key events

16 February 2023: Privacy Act Review

Attorney-General's Department releases final report.

1 March 2023: OAIC report

Notifiable Data Breaches Report: July to December 2022 published.

7 March 2023: OAIC v Facebook

Full Court of the High Court of Australia revokes Facebook Inc's special leave to appeal to the High Court seeking to appeal the Full Federal Court's decision that held the Information Commissioner had established *prima facie* that Facebook Inc was carrying on a business in Australia.

3 May 2023: Privacy Commissioner

Standalone Privacy Commissioner role announced by the Attorney-General.

8 May 2023: Clearview Inc v Australian Information Commissioner

Administrative Appeals Tribunal hands down decision.

10 May 2023: Latitude Finance data breach

Office of the Australian Information Commissioner and New Zealand Office of the Privacy Commissioner commence joint investigation into Latitude Group.

27 June 2023: Medibank Private cyber incident

APRA imposes $250 million capital adequacy requirement on Medibank Private following its examination of Medibank's information security environment.

26 July 2023: ACCC v Facebook

Federal Court orders $20 million fine against Facebook subsidiaries in ACCC misleading and deceptive conduct case.

PRIVACY ACT REVIEW

On 16 February 2023, the Attorney-General's Department published the Privacy Act Review: Report 2022 (**Report**). Refer to our previous legal insight for more information about the Report.

The Attorney-General's Department sought public feedback on the Report following its publication, with a deadline of 31 March 2023. We are now waiting with keen anticipation for the Australian government's response to the Report and the likely introduction of legislation to significantly amend the Privacy Act.

A number of the proposals in the Report raised significant and complex policy changes that would strengthen and broaden the reach of Commonwealth privacy laws in Australia. Three significant areas for reform canvassed by the Report are outlined below.

Removal of small business and employee records exemptions (Proposals 6.1 and 7.1)

The Report proposed the removal of the "employee records" and "small business" exemptions, which have been a feature of the Privacy Act since the introduction of the National Privacy Principles in 2001.

If adopted, removal of the small business exemption would be a significant change and require businesses with an annual turnover of less than $3 million to introduce or uplift their current privacy compliance program to comply with the Privacy Act. Removal of the employee records exemption would require employers to handle employee records relating to the employment of employees in accordance with the Privacy Act.

Mandatory privacy impact assessments (Proposal 13.1)

The Report also proposed that all APP entities be required to complete a privacy impact assessment (**PIA**) prior to undertaking a "high privacy risk activity". The Report noted a "high privacy risk activity" could be defined as any function or activity that is likely to have a significant impact on the privacy of individuals. This test would align with the circumstances when a PIA must be completed under the Australian Government Agencies Code.

Protection of de-identified information (Proposals 4.5, 4.6, 4.7 and 4.8)

Significantly, the Report contained a number of proposals aimed at protecting de-identified information and criminalising the malicious re-identification of de-identified information.

The protection of de-identified information is outside the scope of the Privacy Act. Bringing de-identified information within the scope of the Privacy Act, as proposed, would require APP entities to comply with APP 8 and 11.1 when handling de-identified information by:

- taking reasonable steps to protect de-identified information (APP 11.1); and
- ensuring overseas entities do not re-identify disclosed de-identified information or further disclose information in such a way as to undermine the effectiveness of the de-identification (APP 8).

The future of privacy law in Australia

The privacy reform pendulum is swinging towards more privacy regulation in Australia to better align with global privacy and data protection standards. While this may impose a greater regulatory burden on organisations, it may also help organisations to streamline compliance activities if Australian privacy laws move towards harmonisation with global standards, in particular the General Data Protection Regulation (**GDPR**).

The matrix of domestic and international privacy and data protection laws is complex, and we predict any attempt to align the Privacy Act with other global standards would be a welcome development.

CASE STUDY

Clearview AI Inc v Australian Information Commissioner

The recent findings of a review by the Administrative Appeals Tribunal into the practices of facial recognition software service Clearview provide valuable insights into the extra-territorial application of the Privacy Act.

What is Clearview AI Inc?

Clearview AI Inc (**Clearview**) is an entity incorporated in Delaware, USA that offers a facial recognition software service to law enforcement agencies.

The Clearview technology

Clearview developed a computer program known as a "web crawler" that visits public websites to identify and collect facial images, including image metadata.

The facial images are stored in a database hosted on Clearview servers outside of Australia. Clearview uses these images to draw a "vector" from the facial features contained in the images and stores those vectors in a separate database.

A customer can search the Clearview image database by uploading an image to the Clearview system to compare that image against the Clearview image database. Sufficiently similar images identified by the Clearview software are provided to the customer.

Clearview offered its services to law enforcement agencies in Australia on a trial basis.

OAIC privacy investigation

In July 2020, the Office of the Australian Information Commissioner (**OAIC**), with the United Kingdom Information Commissioner's Office opened a joint investigation into Clearview's activities. Clearview ceased offering free trials to Australian law enforcement agencies after the investigation was announced. However, Clearview continued to collect images from servers located in Australia.

The Australian Information Commissioner and Privacy Commissioner determined Clearview breached the *Privacy Act 1988* (Cth) (**Privacy Act**). Refer to our previous insight on the OAIC's investigation into Clearview's privacy practices for more information about the determination.

Clearview sought to review the OAIC's decision in the Administrative Appeals Tribunal (**AAT**).

AAT review

The AAT considered the following issues:

1. Whether Clearview has the necessary "Australian link" and is bound by the Privacy Act.
2. If yes to Question 1, whether Clearview is an "APP entity".
3. If yes to Question 2, whether Clearview's activities breached APP 1.2, APP 3.3, APP 3.5 and APP 5.1 of the Privacy Act.

AAT findings

Extra-territorial application of the Privacy Act

The AAT determined Clearview has the necessary "Australian link" and its acts and practices outside Australia are subject to the Privacy Act. Consequently, Clearview was found to be an "APP entity".

Despite having no offices or servers in Australia, Clearview was still "carrying on a business in Australia" and subject to the Privacy Act. The AAT found the acquisition of images from servers located in Australia (and worldwide) was a key element of Clearview's business and therefore it was carrying on a business in Australia.

In 2022, the Privacy Act was amended to broaden the scope of the extra-territorial application of the Privacy Act. The AAT found Clearview was bound by the Privacy Act under both the pre- and post-2022 wording of the extra-territorial provisions of the Privacy Act.

Breach of APPs

The AAT determined Clearview breached APP 1.2 and APP 3.3 of the Privacy Act. The AAT was satisfied that it had not breached any other APP.

Clearview was collecting images of individuals' faces to be used for biometric identification. The AAT considered that when biometric information is acquired and used for biometric identification it becomes sensitive information. Consequently, Clearview was collecting the sensitive information of individuals without consent in breach of APP 3.3.

The AAT also determined, as a consequence of breaching APP 3.3, Clearview also breached APP 1.2 by failing to take reasonable steps to implement practices, procedures and systems to comply with the APPs.

Next steps

The AAT's findings are significant given there is limited judicial consideration of the extra-territorial application of the Privacy Act. It is evident from this case that consideration of a business' activities and online data collection practices are crucial in determining whether a business has an "Australian link". This approach reflects modern e-commerce, the use of new technology, and the digital economy in which we operate.

The AAT will consider in a separate hearing whether a declaration under section 52 of the Privacy Act should be made and issue a formal review decision in relation to the Privacy Commissioner's determination.

The AAT decision *Clearview AI Inc and Australian Information Commissioner* [2023] AATA 1069 (8 May 2023) is published on the AustLII website.

REGULATOR ACTIVITY

In the first half of 2023 we witnessed:

- the launch of a joint investigation into Latitude Finance by the OAIC and New Zealand's Office of the Privacy Commissioner
- the announcement of a standalone Privacy Commissioner
- the publication of the OAIC's bi-annual Notifiable Data Breaches Report.

Investigation into Latitude Financial Services

In March 2023, Latitude Financial Services (**Latitude**) experienced a data breach that affected 7.9 million individuals across Australia and New Zealand.

The following types of personal information about Latitude's customers were compromised (in approximate numbers):

- 7.9 million driver licence numbers and some personal information (name, address, telephone number and date of birth)
- 103,000 copies of driver licences or passports
- 53,000 passport numbers
- 100 monthly account statements
- Income and expense information for 900,000 loan applications (including bank account and credit card numbers).

A large amount of the data was compromised in part. For example, only some but not all of the names, addresses and dates of birth of individuals were compromised together with driver licence numbers. Additionally, a number of the credit card numbers had expired.[1]

On 10 May 2023, the OAIC announced an investigation into the Latitude Group, together with the New Zealand Office of the Privacy Commissioner. This is the first joint privacy investigation by the Australian and New Zealand privacy regulators.

Standalone Privacy Commissioner

On 3 May 2023 the Attorney General, the Hon Mark Dreyfus KC MP announced that a standalone Privacy Commissioner will be appointed to perform the privacy functions under the *Australian Information Commissioner Act 2010* (Cth) (**AIC Act**).

This will result in a return to a three-Commissioner model of the OAIC, with three standalone statutory office holders:

- Australian Information Commissioner
- Privacy Commissioner
- Freedom of Information Commissioner.

Currently, the Australian Information Commissioner, Ms Angelene Falk, holds a dual appointment as the Privacy Commissioner under the AIC Act.

The new standalone Privacy Commissioner appointment ties in with the Federal Government's budget allocation of $45.2m over four years from 2023–24 (and $8.4m per year ongoing) for stronger privacy protection and enforcement. This funding is primarily allocated to the OAIC to support the standalone Privacy Commissioner appointment, progress investigations and enforcement, and enhance its data and analytics capability. This initiative will drive a stronger focus on board oversight of data governance.

The Federal government's commitment to privacy is notable given the 46% increase in malicious attacks cited in the OAIC's latest Notifiable Data Breaches Report.

Notifiable Data Breaches Report July to December 2022

The OAIC released the Notifiable Data Breaches Report for the period of July to December 2022, published on 1 March 2023 (the **NDB Report**).

The key findings in the Report include:

- a 26% increase in notified breaches
- a 41% increase in malicious or criminal attacks resulting in data breaches
- a 5% decrease in breaches caused by human error
- the health sector experienced the most breaches, closely followed by the finance sector
- the most common type of compromised personal information was contact information
- 88% of breaches affected 5,000 individuals or fewer
- 71% of entities notified the OAIC within 30 days of being aware of a data breach.

The NDB Report provides a useful snapshot of the types and scale of data breaches affecting APP entities. It also provides useful scenarios, guidance and insights into the OAIC's regulatory approach. Again, the OAIC reinforces the importance of:

- implementing the Australian Cyber Security Centre Essential Eight mitigation strategies for protection against online threats
- having a data breach response plan in place that incorporates the Notifiable Data Breaches Scheme requirements, and
- timely notification.

Given the OAIC's increased powers to enforce compliance with the Notifiable Data Breaches Scheme, implementing systems and processes to ensure timely notification to the OAIC and affected individuals of a data breach will be vital to reduce the risk of regulatory intervention in the midst of a data breach.

1. Latitude Financial, Latitude Cyber Response: Information, updates and support for those affected accessed <https://www.latitudefinancial.com.au/latitude-cyber-incident/>.

CASE STUDY

OAIC v Facebook

Proceedings against social media giant Facebook demonstrate that the jurisdiction of the OAIC extends even to companies located predominantly outside of Australia.

Current state of play

On 9 March 2020, the OAIC commenced proceedings against Facebook Inc and Facebook Ireland (together, **Facebook**) in the Australian Federal Court, alleging "serious or repeated interferences with the privacy of an individual" in contravention of section 13G of the *Privacy Act 1988* (Cth).

The OAIC's proceedings relate to the Cambridge Analytica data breach scandal and Facebook's disclosure of the personal information of over 300,000 Australian Facebook users to British firm Cambridge Analytica.

Since 2020, Facebook has challenged the OAIC's jurisdiction and the service of documents on Facebook Inc. In 2022, Facebook was granted special leave to appeal to the High Court of Australia to determine whether the OAIC has jurisdiction to serve Facebook Inc legal documents in the United States of America.

On 7 March 2023 the High Court's decision granting Facebook special leave to appeal was revoked by the Full Court of the High Court of Australia following legislative changes to the Federal Court Rules 2011 (**FCR**) regarding overseas service requirements (Division 10.4) on the basis grounds of appeal were "no longer of public importance".[2]

Key takeaways

- As Facebook has been unable to set aside the service of the OAIC's application on Facebook Inc, the proceedings will return to the Federal Court to determine the substantive issues against Facebook Inc and Facebook Ireland.
- Following the FCR amendments, the requirements for serving documents in Federal Court proceedings on companies outside the Australian jurisdiction have become less onerous. For example, leave is no longer required for service where direct jurisdiction can be established (rule 10.42). This basis for jurisdiction over subject matter can be provided for by rule 10.42(j). Leave can also be requested from the Court (rule 10.43).
- Ultimately, companies should be aware that even where they are predominantly located outside of Australia, the OAIC may nevertheless be able to commence proceedings in the Federal Court by relying on the amended rules regarding overseas service.

2. *Facebook Inc v Australian Information Commissioner & Anor* [2023] HCATrans 22 (7 March 2023) accessed <http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/HCATrans/2023/22.html>.

CASE STUDY

Facebook subsidiaries fined $20 million for misleading customers

On 26 July 2023, the Federal Court ordered two Facebook subsidiaries, Facebook Israel Ltd and Onavo Inc to each pay a pecuniary penalty of $10 million for engaging in misleading conduct in breach of the Australian Consumer Law. The enforcement action demonstrates the importance of considering consumer law in data collection and handling.

Background

In December 2020, the Australian Competition and Consumer Commission (**ACCC**) commenced proceedings in the Federal Court against Facebook Inc (now Meta Platforms Inc) and two Facebook Inc subsidiaries, Onavo Inc and Facebook Israel Ltd.

Onavo Inc and Facebook Israel Ltd were responsible for developing and marketing the mobile app "Onavo Protect" to Australian consumers. The Onavo Protect app was a free virtual private network (**VPN**) service available to Australian customers from December 2016 to May 2019.

The ACCC alleged Facebook and Onavo engaged in false, misleading or deceptive conduct when promoting the Onavo Protect app to Australian customers between 1 February 2016 and 31 October 2017. During this time over 270,000 Australian customers downloaded the app.

Onavo Protect was withdrawn from the Apple app store in August 2018 and the Google Play store in February 2019.

Misleading or deceptive conduct

Facebook Ireland and Onavo Inc advertised and promoted the Onavo Protect app as protecting users' personal information and keeping its data safe. The content of the listings for Onavo Protect on the Google Play store or Apple app store did not sufficiently disclose to Australian consumers that users' data would be used for purposes other than providing the Onavo Protect service.

However, Facebook Israel Inc and Onavo Inc collected personal mobile activity data such as users' internet and app activity and disclosed anonymised and aggregated data to Facebook Inc for commercial benefit. This included supporting market analytics and identifying future acquisitions.

Disclosures about how the data of Australian consumers would be used for other purposes were set out in the Onavo Protect Terms of Service and Privacy Policy. These disclosures were not sufficiently proximate to the Onavo Protect app store listings.

Facebook Israel Inc and Onavo Inc admitted that contents of the listings that promoted the protection of user data and safety were likely to mislead or deceive, and liable to mislead the public, in the absence of sufficient disclosures to Australian consumers of the fact that users' data would be used for purposes other than providing Onavo Protect.

Facebook Israel Inc and Onavo Inc admitted to contravening the Australian Consumer Law and that their conduct was likely to mislead or deceive (section 18), or liable to mislead the public as to the nature and characteristics of Onavo Protect (section 33).

The case against Meta was dismissed by the Federal Court after settlement negotiations between the ACCC, Facebook Israel Inc and Onavo Inc.

Key takeaways

The ACCC's enforcement action highlights the intersection between privacy and consumer law and data protection as a consumer right. Consumer law must be a key consideration for all organisations when establishing and promoting their data collection and handling practices, regardless of whether the organisation is bound by the Privacy Act.

Organisations can no longer simply rely on their terms of service and privacy policy discretely hyperlinked on a website to set out how personal data will be used and disclosed.

The disclosure of such information must be sufficiently prominent to consumers, especially if easily accessible marketing or advertising content does not accurately represent the true picture of how personal data will be used and disclosed by an organisation.

The Federal Court decision *Australian Competition & Consumer Commission v Meta Platforms Inc* [2023] FCA 842 can be found on the Federal Court of Australia website.

CASE STUDY

APRA regulatory action against Medibank

On 27 June 2023, the Australian Prudential and Regulation Authority (**APRA**) announced it would impose on Medibank Private (**Medibank**) a capital adequacy requirement of $250 million.

This follows APRA's review of the cyber security incident that Medibank faced in October 2022, with the increased capital adequacy requirement reflecting weaknesses identified in Medibank's information security environment by APRA.

Background

In October 2022, 9.7 million past and present Medibank customer records were stolen from Medibank systems and subsequently leaked on the dark web by cybercriminals after Medibank refused to pay the criminals' ransom demands. The records contained sensitive customer information, including customers' medical conditions and treatment.

Capital adjustment

The increased capital adequacy requirement became effective from 1 July 2023 and will remain in place until APRA is satisfied with an agreed remediation program of work completed by Medibank. The capital adjustment is applied to Medibank's operational risk charge under the Private Health Insurance (**PHI**) Capital Framework.

Key takeaways

The action taken by APRA against Medibank is a reminder to all APRA regulated companies of the strict stance the authority has towards cyber security data breaches.

Where companies have inadequate controls and risk management systems, specifically regarding preventing unauthorised access to private consumer data, it is crucial that businesses take action to strengthen their security environment and data management prior to any potential cyber exposures.

APRA Member Suzanne Smith stated: "This action demonstrates how seriously APRA takes entities' obligations in relation to cyber risk and that APRA will respond strongly to identified weaknesses in cyber security controls."[3]

3. Australian Prudential and Regulation Authority, Media Release: APRA takes action against Medibank Private in relation to cyber incident, 27 June 2023, accessed 28 July 2023 <https://www.apra.gov.au/news-and-publications/apra-takes-action-against-medibank-private-relation-to-cyber-incident>

PRIVACY

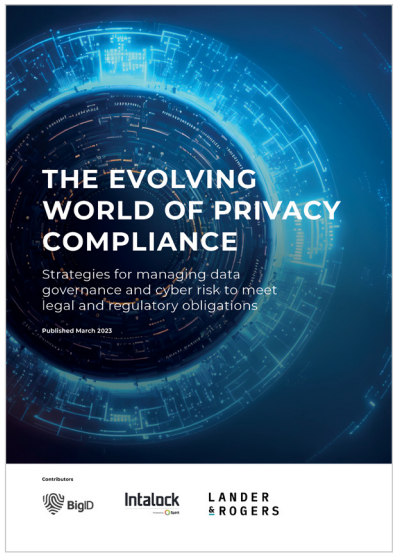
LANDER & ROGERS PRIVACYCOMPLY

Privacy impact assessments (**PIA**) are a useful risk management tool to assess and manage the privacy impacts of a project. The Privacy Act Review has recommended a PIA must be conducted for all activities with high privacy risks.

In the wake of sustained cyber attacks and failures in data management across Australian businesses, Lander & Rogers has developed a privacy-by-design / privacy impact assessment software product to help businesses embed privacy-awareness and risk mitigation practices in their businesses, without delay.

Our goal is to ease the compliance burden and improve privacy protection across SMEs and large corporations with our tool, PrivacyComply.

Visit the Lander & Rogers website for more information about PrivacyComply.



EVOLVING WORLD OF PRIVACY COMPLIANCE WHITE PAPER

The privacy and data protection landscape is a tapestry of complex and competing laws. Lander & Rogers recently co-authored a white paper to provide businesses with a pathway to navigate this landscape.

The white paper accompanied a "Privacy Roadshow" that our clients were invited to attend to learn more about an enterprise-wide, cross-disciplinary approach to data and privacy management.

Access a copy of the white paper here, or reach out to a member of our team for more information.

Our team

Rob Neely
Partner
Corporate

D +61 2 8020 7704
E rneely@landers.com.au

Lisa Fitzgerald
Partner
Corporate

D +61 3 9269 9103
E lfitzgerald@landers.com.au

Keely O'Dowd
Senior Associate
Corporate

D +61 3 9269 9526
E kodowd@landers.com.au

Edward Lyons
Senior Associate
Corporate

D +61 2 8020 7613
E elyons@landers.com.au

ABOUT US

Founded in 1946, Lander & Rogers is one of the few remaining truly independent Australian law firms and a leader in legal tech innovation.

With offices across the eastern seaboard of Australia, Lander & Rogers has grown organically resulting in a unified firm with a strong focus on client and staff care.

We believe legal services involve more than just the law – practical, commercial advice and exceptional client experience are equally important to our clients and to us.

Lander & Rogers advises corporate, government, not-for-profit and private clients in insurance law and litigation, family law, workplace relations & safety, real estate, corporate transactions, digital & technology and commercial disputes.

The firm is global in approach, working closely with a network of leading firms to provide advice to clients, both domestically and abroad. Lander & Rogers is also the exclusive Australian member of the largest worldwide network of independent law firms, TerraLex.

Brisbane

Level 11 Waterfront Place
1 Eagle Street
Brisbane QLD 4000

T +61 7 3456 5000
F +61 7 3456 5001

Melbourne

Level 15 Olderfleet
477 Collins Street
Melbourne VIC 3000

T +61 3 9269 9000
F +61 3 9269 9001

Sydney

Level 19 Angel Place
123 Pitt Street
Sydney NSW 2000

T +61 2 8020 7700
F +61 2 8020 7701

landers.com.au