Shaping the future of insurance law

wotton kearney

A founding member of LEGALIGN GLOBAL

Cyber, Tech & Data Risk Report

W+K's wrap-up of the month's cyber, technology and data risk news for insurers, brokers and their customers doing business in Australia and New Zealand.

JUL22

W+K INSIGHTS

INTERACTIVE PDF

TOP RANKED Chambers Asia-Pacific 2022 Wotton + Kearney

Australasian Lawyer 2021 5-STAR CYBER LAWYERS

Australia

OAIC makes submission on Australian Data Strategy

On 14 July 2022, the Office of the Australian Information Commissioner (OAIC) made its submission to the Department of the Prime Minister & Cabinet's consultation on the Australian Data Strategy.

The Strategy's focus is to align a range of existing legislation, strategies, policies and reviews that regulate the use of data and the protection of personal information. According to the OAIC: "The Strategy broadly intersects with the OAIC's existing regulatory role and responsibilities under several laws and whole-of-government initiatives, including the Privacy Act (and its ongoing review), the FOI Act, the Consumer Data Right, the *Data Availability and Transparency Act 2022*, the Australian Cyber Security Strategy, the National Data Security Action Plan, and the Digital Identity scheme."

The OAIC's submission placed a strong emphasis on reforming Australia's Privacy Act and included some key recommendations around:

- **increased accountability for regulated entities** – in particular, "establishing a positive duty on organisations to handle personal information fairly and reasonably and to require regulated entities to take a proactive approach to meeting their obligations as the parties best equipped to understand their complex information handling flows and practices", and
- **harmonisation and global interoperability** – the OAIC emphasised the need for consistent regulation across Australia's states and territories on laws that "purport to address privacy issues", as well as to put in place a framework to facilitate the flow of data internationally, which allows for referencing other legal frameworks "including the General Data Protection Regulation, which are appropriate to be adopted or adapted to the Australian context."

OAIC launches investigation into facial recognition technology and biometric data

On 12 July 2022, the OAIC announced that it had opened investigations into the "personal information handling practices of Bunnings Group Limited and Kmart Australia Limited, focusing on the companies' use of facial recognition technology."

The use of facial recognition technology and sensitive biometric data like facial images remains controversial. Globally and locally, multiple regulatory investigations and controversies suggest this technology and data are likely to trigger consumer and customer complaints, regulatory inquiries and penalties, brand and reputational damage, and associated costs for the organisations that deploy it.

Organisations considering using facial recognition technology and biometric data should weigh the business benefits against the likely consequences. They should also review their privacy and data retention policies to ensure they will stand up to scrutiny, and implement privacy impact assessments and robust customer notification regimes.

Digital platform regulators announce priorities

The head four members of the digital platform regulators, ACCC, ACMA, OAIC and eSafety, released a report at the end of June 2022 stating their priorities for 2022/2023. These are:

- **digital transparency** – focusing on improving the transparency of what digital platforms are doing to protect Australians from harm and what consumer data is used for, and
- **examining algorithms** – looking into the impacts of algorithms on profiling, promotions, spread of disinformation, harmful content, product ranking and sponsored displays on online marketplaces.

The report also noted that all four regulators will improve collaboration to collate and share information with each another to promote efficiently implemented digital platforms regulation.

The regulators are also currently looking at whether there is a need for competition and consumer reform for digital platforms.

Claims against MSPs and CSPs on the rise

As ransomware and related cybercrime has established itself as one of Australia's fastest growing security threats,[1] there has been a corresponding increase in exposure risks for IT professionals. In particular, liability risks for managed service providers[2] (MSPs) and cloud service providers[3] (CSPs) have become significantly heightened, as the nature of the businesses makes them, and subsequently their customers, prime targets for cybercriminals.

Two ongoing international examples illustrate the litigation risks faced by Australian MSPs and CSPs in this fast-developing area of law, both in terms of the likely allegations to be raised and the heads of damages sought.

In Singapore, gaming hardware manufacturer Razer is currently suing multinational info-technology company Capgemini regarding a 2020 data breach that exposed Razer's customer and sales data.[4] A trial commenced in Singapore's High Court on 13 July 2022.

Razer contends that Capgemini breached its contractual obligations, including to ensure that its IT systems were secure and making sure that its personnel had the appropriate and adequate skills, qualifications and experience. Razer also alleges that Capgemini was negligent, having owed Razer a duty of care as the subject-matter experts in the IT field.

Razer is seeking damages of at least US$7 million (S$9.85 million), including loss of profits, forensic investigation costs, and costs of engaging a law firm to advise on breach response.

In the United States, the ongoing class action litigation in *Allen v Blackbaud Inc* is an example of potential liability of a CSP, to both its own clients and to the customers of its clients. Blackbaud (a cloud computing provider that manages servers for non-profits, education institutions and healthcare organisations) was the subject of a ransomware attack during February to May 2020, in which sensitive and personal data from students, patients, donors and other individual users was accessed by the threat actors.

In its 2021 interlocutory decision, the Supreme Court of South Carolina found that Blackbaud owed the plaintiffs a duty to protect their PII and PHI under South Carolina law due to the contractual relationship between Blackbaud and its customers. The court found that this duty extended to the prevention of cyberattacks because, regardless of whether those attacks were criminal acts of third parties, Blackbaud knew of the risk of cyberattacks but failed to take adequate measures to guard against them.

Whilst there are significant differences between US and Australian law, it is easy to see how an Australian court could come to a similar conclusion about the scope of a CSPs duty to its client and, potentially, the customers of its clients.

Cyber incident reporting obligations for infrastructure add to regulatory complexity

July 2022 saw the end of the three month grace period for reporting cyber incidents under the *Security of Critical Infrastructure Act* 2018 (Cth) (SOCI Act). From 8 July 2022, owners and operators of critical infrastructure assets must report cyber security incidents to the Australian Cyber Security Centre (ACSC). A parallel obligation applying to telecommunications carriers and carriage services providers has also commenced.

The concept of a potentially reportable 'cyber security incident' under the SOCI Act is broad. To meet the threshold for reporting, the incident will need to be unauthorised, involve some element of access, modification or impairment of computers or systems, and impact the availability of a critical infrastructure asset.

Likewise, critical infrastructure assets are defined under the SOCI Act to include critical infrastructure assets in diverse sectors, including communications, financial services, water/sewerage, energy, health, higher education/research, food/grocery, transport, space, aviation and defence.

This reporting obligation joins other legislative measures geared towards improving the cyber security resilience and readiness of Australian business and industries.

While it's a sound objective, the reporting obligations put organisations, which are already under pressure during an unfolding cyber incident, in the undesirable position of having to navigate regulatory complexity, including the plethora of overlapping notification obligations.

[1] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020-annual-report-2021.pdf

[2] Who deliver services such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers' premises, in their own data centres (hosting) or in a third-party data centre.

[3] Who offer cloud-based platform, infrastructure, application or storage services.

[4] Approximately 100,000 Razer customers were impacted in the incident, however the company has stated that no sensitive data, such as credit card numbers or passwords, were exposed (only order details, customer and shipping information).

To make the picture a bit clearer, we've shown the various notification regimes that may apply to a cyber incident in the table below.

Who? Person required to notify	**Who?** Agency to be notified	**What?** Trigger for notification obligation	**When?** Max timeframe for notice to be given	**How?** Method of notification	**Why?** Act or regulation
Owners/operators of 'critical infrastructure assets'	*Australian Cyber Security Centre (ACSC)*	Cyber security incident	12 hours or 72 hours depending on incident impact *(+ different timeframe for follow-up written reports)*	Urgent oral – 1300Cyber1 Written – cyber.gov.au	*Security of Critical Infrastructure Act* 2018 (Cth)
Organisations with annual revenue >$3M and others covered by the *Privacy Act* 1988 (Cth)	OAIC, individuals	Eligible data breach	As soon as practicable after investigation into incident and preparation of statement describing impact (entities must take 'all reasonable steps' to complete investigations within 30 days)	Statement to the OAIC and affected individuals	*Privacy Act* 1988 (Cth)
Carriers	ACSC	Broad threshold. At the lower end it's enough that you have an 'imminent' cyber security incident which is likely to have an impact on asset availability, integrity, reliability, confidentiality.	12 hours or 72 hours depending on incident impact *(+ different timeframe for follow-up written reports)*	As above for SOCI Act reporting	*Telecommunications (Carrier Licence Conditions – Security Information) Declaration* 2022
Eligible carriage service providers	ACSC	As above.	12 hours or 72 hours depending on incident impact *(+ different timeframe for follow-up written reports)*	As above for SOCI Act reporting	*Telecommunications (Carriage Service Provider – Security Information) Determination* 2022
An accredited data recipient in a designated sector (currently Banking, Energy)	ACSC	Security incident	As soon as practicable or within <30 days	As above for SOCI Act reporting	*Competition and Consumer (Consumer Data Right) Rules* 2020
APRA-regulated entities (banks, authorised deposit taking institutions, superannuation funds, insurance companies)	APRA	Information security incident (with material effect on the entity or the interests of depositors, policyholders, beneficiaries or other customers, or which has been notified to other regulators)	72 hours (but as soon as possible)	To a regulated entity's usual APRA contacts	*CPS 234 Information Security*
Australian Financial Services and credit licensees	ASIC	'Reportable situation' – Note that this could include a significant breach or likely significant breach of 'core obligations' including investigations into significant breaches	Within 30 calendar days	Via the approved form on the ASIC Regulatory Portal	*RG 78 Breach reporting by AFS Licensees and Credit Licensees* *Corporations Act 2001 (Cth)*
Listed entities	ASX	Listed entity comes into possession of information concerning it that a reasonable person would expect to have a material effect on the price or value of its securities	Immediately (and a trading halt needs to be considered if a full disclosure cannot be made immediately)	Via ASX Online	*ASX Listing Rule 3.1* *Corporations Act 2001 (Cth)*

New Zealand

New Zealand welcomes new Privacy Commissioner

The New Zealand Office of the Privacy Commissioner has welcomed its new Commissioner, Michael Webster. After the previous commissioner, John Edwards, took on the role of Information Commissioner at the ICO (UK), Mr Webster formally began his role on 5 July 2022. Mr Webster was previously the Secretary of the Cabinet Office for 13 years.

In his new role as Privacy Commissioner, Mr Webster will be responsible for promoting and overseeing the principles set out by the Privacy Act 2020. The principles set out how personal information can be collected, used, stored and disclosed. At a practical level, this involves reviewing legislation and policies that affects privacy, issuing statements on good privacy practice, making decisions on complaints made against businesses and agencies, and advising agencies on the operation of the Privacy Act.

It remains to be seen how the approach of the OPC may change under Mr Webster's stewardship. Mr Webster is scheduled to discuss his perspectives and priorities in the new role at an upcoming webinar hosted by the OPC on 28 July 2022.

FMA releases cyber security guidance for market services licensees

The Financial Markets Authority (FMA) has continued its focus on cyber risk in the financial sector, issuing a new information sheet for market services licensees under the Financial Markets Conduct Act 2013.

The information sheet follows the cyber resilience information sheet, issued in July 2021, which was targeted at financial advice providers. Both the June 2022 and the July 2021 information sheets follow the FMA's thematic review of cyber resilience in FMA-regulated entities in 2019. The thematic review itself used the NIST cyber security framework for self-assessment of cyber resilience.

The June 2022 information sheet emphasises the expectations of those holding market services licensees and the standard conditions inherent within that licence. This includes:

- ensuring that licence holders maintain "secure and reliable" IT systems using "adequate technology architecture, cyber security systems, processes and controls in place to ensure their technology risks are being managed",
- ensuring that systems, processes and controls are tested and assessed on a regular basis,
- requiring licence holders stay up-to-date on cyber security threats and closely consider supply chain risk,
- establishing incident response plans, which are reviewed and tested on a regular basis,
- notifying the FMA "as soon as practicable" of "any technological or cyber security event that materially disrupts or affects the provision of their regulated services, or has a material adverse impact on one of more customers", and
- conducting a comprehensive post-incident root cause analysis to understand the cause of an incident and provide the FMA with a post-incident report.

The information sheet makes it clear that entities captured under part 6 of the FMCA 2013 are subject to robust cyber security requirements, requiring regular consideration and reassessment. The FMA also expects to be notified of a broader range of incidents than may be captured by the Privacy Act 2020. While there is a focus on impact on customers, the notification threshold bites on any "technological or cyber security event".

Insureds in the financial sector, and those insuring them, should closely consider how the latest position adopted by the FMA may impact their cyber security and information governance risk posture, and whether their incident response plans need reviewing considering the latest guidance.

wotton kearney
A founding member of LEGALIGN GLOBAL

CERT NZ issues Q1 2022 report

CERT NZ has released its Cyber Security Insights report for Q1 of 2022, providing an overview of cyber security incidents impacting New Zealanders from 1 January - 31 March.

The CERT NZ reports are limited to the information provided in voluntary notifications to CERT NZ. That said, the reports provide a helpful insight into New Zealand's cybercrime environment.

The key takeaways from the most recent report are:

- Incident reports responded to by CERT NZ in this quarter were down by 41% compared to Q4 of 2021, although this represented a reversion to the mean after a very active Q4 2021 and 63% more notifications than the same quarter in 2021. This is broadly in line with a downturn in claims observed in W+K's NZ cyber, privacy and data security team.
- While attackers continue to predominantly use phishing as an attack method (59% of reports), there is a clear increase in popularity in the targeting of non-fungible tokens (NFTs) to carry out various scams. NFTs remain largely unregulated and difficult to trace, making them fertile ground for cyber criminals.

To protect against these scams, organisations should consider using two-factor authentication, having strong passwords and applying patches promptly.

Global updates

For recent international developments, please see our Legalign Global colleagues' recent updates below:

- Alexander Holburn (Canada) – Privacy publications
- BLD Bach Langheid Dallmayr (Germany) – Publications
- DAC Beachcroft (UK) – Cyber and Data Risk publications
- Wilson Elser (US) – Cybersecurity and Data Privacy publications

Reporting obligations put organisations already under pressure during an unfolding cyber incident in the undesirable position of having to navigate regulatory complexity, including the plethora of overlapping notification obligations.

Key contacts

For more information on the content in this report, please contact our senior team members.

wotton kearney

A founding member of LEGALIGN GLOBAL

Australia

Kieran Doyle
Partner, Australian Cyber Lead (Sydney)
T: +61 2 8273 9828
kieran.doyle@wottonkearney.com.au

Cyber, Privacy & Data Security
Technology Liability

Nick Lux
Partner (Melbourne)
T: +61 3 9604 7902
nick.lux@wottonkearney.com.au

Technology Liability

Nicole Gabryk
Special Counsel (Sydney)
T: +61 2 9064 1811
nicole.gabryk@wottonkearney.com.au

Cyber, Privacy & Data Security

Stephen Morrissey
Special Counsel (Sydney)
T: +61 2 8273 9817
stephen.morrissey@wottonkearney.com.au

Technology Liability

Magdalena Blanch-de Wilt
Special Counsel (Melbourne)
T: +61 3 9116 7843
magdalena.blanch-dewilt@wottonkearney.com.au

Cyber, Privacy & Data Security
Technology Liability

View W+K's full team

New Zealand

Joseph Fitzgerald
Partner, New Zealand Cyber Lead (Wellington)
T: +64 4 260 4796
joseph.fitzgerald@wottonkearney.com

Cyber, Privacy & Data Security
Technology Liability

Laura Bain
Senior Associate (Wellington)
T: +64 4 974 0464
laura.bain@wottonkearney.com

Cyber, Privacy & Data Security

Australian offices

Adelaide
Hub Adelaide, 89 Pirie Street
Adelaide, SA 5000
T: +61 8 8473 8000

Brisbane
Level 23, 111 Eagle Street
Brisbane, QLD 4000
T: +61 7 3236 8700

Canberra
Canberra, ACT 2601
T: +61 2 5114 2300

Melbourne
Level 15, 600 Bourke Street
Melbourne, VIC 3000
T: +61 3 9604 7900

Perth
Level 49, 108 St Georges Terrace
Perth, WA 6000
T: +61 8 9222 6900

Sydney
Level 26, 85 Castlereagh Street
Sydney, NSW 2000
T: +61 2 8273 9900

New Zealand offices

Auckland
Level 18, Crombie Lockwood Tower
191 Queen Street, Auckland 1010
T: +64 9 377 1854

Wellington
Level 13, Harbour Tower
2 Hunter Street, Wellington 6011
T: +64 4 499 5589

www.wottonkearney.com.au

wotton kearney

A founding member of LEGALIGN GLOBAL

TOP RANKED Chambers Asia-Pacific 2022 Wotton + Kearney

Australasian Lawyer 2021 5-STAR CYBER LAWYERS