Australasia's largest insurance & dispute resolution firm

wotton kearney

A founding member of LEGALIGN GLOBAL

Cyber, Tech & Data Risk Report

APR23

W+K INSIGHTS

INTERACTIVE PDF

Chambers TOP RANKED Asia-Pacific 2023 Wotton + Kearney

Australasian Lawyer 2021 5-STAR CYBER LAWYERS

Welcome to W+K's Cyber, Tech and Data Risk Report

Issue 5, April 2023

We are delighted to publish Issue 5 of our *Cyber, Tech and Data Risk Report*, which is our first wrap-up of relevant news for 2023 for insurers, brokers and their customers doing business in Australia and New Zealand in the cyber, tech and data fields.

In this month's report, we look at a range of cyber issues and developments, including the implications of the Commonwealth's Privacy Act Review Report, the release of the Australian Cyber Security Strategy Discussion Paper on Regulatory Change, APRA's supervision priorities, and the OECD's adoption of the Declaration on Government Access to Personal Data Held by Private Sector Entities. We provide updates on significant litigation, including the Medicare 'class actions' and the OAIC proceedings against Facebook. In the IT liability space, we also look at a recent NSWCA decision that highlights the cost of IT liability risk.

In New Zealand news, we cover the OPC's guidance on breaches in the healthcare sector, CERTNZ's cyber incident communications advice, and the High Court's permanent injunction restricting access to information published on the dark web.

We also share highlights from recent reports by OAIC and Coveware, highlights from media coverage of disclosure obligations, insights from our Legalign Global partner DACB, and other international news.

For more information about any of these stories, please contact a member of our Cyber, Privacy + Data Security team or Technology Liability team.

Kieran Doyle
Partner, Sydney
Head of Cyber + Technology
T: +61 2 8273 9828
kieran.doyle@wottonkearney.com.au

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

wotton kearney
A founding member of LEGALIGN GLOBAL

Contents

CYBER INCIDENT HELPLINES
Australia: 1800 316 706
New Zealand: 0800 9525 2467
auscyberclaims@wottonkearney.com.au
nzclaims@wottonkearney.com

Cyber – Australia

Class actions against Medibank

In the aftermath of the large-scale ransomware attack that compromised the data of up to 9.7 million customers last year, Medibank is now facing two concurrent 'class actions' that come from two very different angles. One is being heard in the Federal Court in line with the standard class action regime, and the other is being heard before the OAIC as part of a representative complaint under the *Privacy Act 1988* (Cth).

The Federal Court class action hones in on allegations of breach of contract, misleading and deceptive conduct, and breach of confidence from the perspective of the health insurer-customer relationship. The OAIC representative action focuses on interferences with individuals' privacy under the *Privacy Act 1988* (Cth).

The only previous data breach class action run in Australia in the Federal Court was regarding the NSW Ambulance Service, which settled in 2019. No data breach class actions have gone to final hearing in Australia as yet.

In addition to the privacy class actions, Medibank now also finds itself facing a securities class action arising from the incident, which is the first time securities class actions have been filed in Australia arising from a cyber incident.

The two privacy actions against Medibank, taken together, represent an important shift in privacy law and a timely opportunity to test the bounds of the existing regime under the *Privacy Act 1988* (Cth) and under the general law. We will shortly be publishing an article about the interaction between the two sets of proceedings and what they might mean for the future of privacy litigation and enforcement in Australia.

Privacy Act Review Report

On 16 February 2023, the Commonwealth Attorney-General's Department released the much-anticipated Privacy Act Review Report, following two years of extensive review of the *Privacy Act 1988* (Cth) and consultation with various stakeholders.

The Review Report includes 116 proposed reforms that aim to strengthen the protection of individual's personal information. If these reforms are implemented following consultation, they will inherently increase the complexity of privacy law in Australia, significantly increase compliance costs for entities holding information, and, ultimately, claims costs for those entities and their insurers.

The recommendations include proposals to:

- require notification of a data breach to the OAIC within 72 hours if an entity believes that there has been an eligible data breach (with further notification to be given subsequently). This is a 'hard' timeframe, stated in the Review Report to be aligned with SOCI and in line with community expectations. While at first blush, this is a significant sharpening of the current 30-day timeline, we understand the triggers for each are different – 30 days to investigate a 'suspected' breach vs. 72 hours to notify if they discover one has occurred.

Either way, ultimately, we would expect it to increase the costs of responding to data breaches due to increased regulatory complexity (for example, iterative rounds of correspondence with the OAIC)

- introduce a statutory tort for serious invasions of privacy and amend the Privacy Act to allow for a direct right of action to allow individuals to apply for relief regarding an interference with privacy, which will have a significant impact for insurers regarding claim risk – as a result, there will be more avenues for individuals to submit claims against insureds, on which class actions could be founded, and
- introduce an obligation on businesses to periodically review the time for which they retain personal information and 'erase' personal information that no longer needs to be retained, which ultimately creates more grounds to breach privacy obligations for entities holding personal information.

It's not yet clear how the Australian cyber insurance market will react to the proposed reforms, and we don't expect to see the full scope of that impact until months or years after the finalised suite of reforms takes effect.

Ultimately, increased complexity of privacy law in Australia will mean increased costs in managing data breaches, and an increased risk of regulatory penalties.

We will unpack the full details of the proposed reforms and the implications for the insurance market in our upcoming Privacy Act Review Report article.

Ultimately, increased complexity of privacy law in Australia will mean increased costs in managing data breaches, and an increased risk of regulatory penalties.

OAIC proceedings against Facebook over the Cambridge Analytica scandal

The OAIC's substantive proceedings against Facebook Inc and Facebook Ireland (collectively, Facebook) will now return to the Federal Court. On 7 March 2023, the High Court of Australia granted the OAIC's application to revoke Facebook's special leave to appeal to the High Court due to a change in the Federal Court Rules regarding overseas service. The effect of this is to clear the way for proceedings to return to the Federal Court, meaning that the OAIC's substantive proceedings seeking civil penalties against Facebook over the Cambridge Analytica matter will now progress.

To recap the history of the OAIC's proceedings against Facebook:

- On 9 March 2020, the OAIC lodged proceedings against Facebook in the Federal Court, alleging that the social media platform had committed serious and/or repeated interferences with privacy in contravention of Australian privacy law. The allegations are that from 12 March 2014 – 1 May 2015
  - Facebook disclosed the personal information of Australian Facebook users to the This Is Your Digital Life app, in breach of Australia Privacy Principle (APP) 6
  - Facebook did not take reasonable steps during this time to protect its users' personal information from unauthorised disclosure, in breach of APP 11, and
  - as a result, Australians' information was exposed to the risk of being disclosed to Cambridge Analytica and used for political purposes.
- On 25 September 2020, Facebook Inc applied for leave to appeal the Court's interlocutory decision dated 14 September 2020 (regarding service of legal documents on the US-based entity) to the full Federal Court. In the 14 September 2020 decision, Justice Thawley was satisfied that the Commissioner had established a *prima facie* case that Facebook Inc was carrying on business in Australia, and was collecting and holding personal information in Australia at the relevant time, under s 5B(3) of the *Privacy Act 1988* (Cth).
- Facebook Inc appealed the 14 September 2020 decision, and on 7 February 2022, the Full Federal Court dismissed its appeal.

- Facebook Inc sought, and on 16 September 2022 was granted, special leave to appeal to the High Court of Australia regarding the Full Federal Court's decision.
- After a change to the Federal Court Rules 2011, which came into effect in January 2023, the Commissioner applied to revoke the grant of special leave to Facebook Inc.

On 7 March 2023, the High Court granted the Commissioner's application to revoke the grant of special leave. This was on the basis that the matter no longer raised an issue of public importance.

Release of Australian Cyber Security Strategy Discussion Paper Regulatory Change

The Australian Government took a further step towards its target to make Australia the most cyber-secure country in the world by 2030, releasing its Discussion Paper on the 2023 – 2030 Australian Cyber Security Strategy on 27 February 2023. The Strategy will shape Australian cyber policy and regulation into the medium-term and beyond. Its development is being assisted by an Expert Advisory Board.

The Discussion Paper invites submissions on key questions that will shape the Strategy, as well as flagging a range of government responses, including better coordination, international cooperation and automatic threat blocking at scale. Of particular interest to companies, insurers and their clients are the questions the Discussion Paper asks that have the potential to re-shape the regulatory sphere or affect the response to, or cost of, cyber incidents. For the legal and insurance industries, the most noteworthy issues relate to the potential regulatory reforms, including the introduction of a new Cyber Security Act and regulating and/or clarifying the position on ransom payments.

Under express consideration as part of the Strategy are:

- more explicit specification of best practice cyber security standards, a welcome development for Australian directors and executives who have been faced with rising penalties and regulatory vigilance without a yardstick against to measure prioritisation of investment (the proverbial cart before the horse that we've been discussing for some time)
- simplification of regulatory frameworks, including reporting obligations (this has been a creeping problem over the last few years, with a multiplicity of overlapping obligations applying across regulated sectors – you can read our earlier commentary here)
- the previously flagged prohibition of ransom payments and/or clarification of the legal obligations applying to payment of ransom, and
- what government support should be available to victims following a cyber incident, including mechanisms for national response and sharing the root cause findings from investigations of major cyber incidents.

The release of the Discussion Paper closely preceded the Biden-Harris Administration's release of the US National Cybersecurity Strategy. There are some visible themes emerging globally. Among them, there is a shift to clearly communicating an expectation of companies (critical infrastructure and beyond) to take more action to help protect the personal information of citizens and to invest in the long-term resilience and security of enterprises and products.

Submissions to the Discussion Paper, which closed on 15 April 2023, can be made online here.

OAIC Notifiable Data Breaches Report, Jul – Dec 2022

The Office of the Australian Information Commissioner (OAIC) published its semi-annual report summarising the notifiable data breach key statistics and trends across July to December 2022.

As a refresher, not all cyber incidents resulting in data breaches are required to be reported. A data breach is required to be reported to the OAIC when three criteria are established:

1) personal information has been lost, or has suffered unauthorised access or disclosure
2) the loss, access, or disclosure is likely to result in serious harm to one or more individuals, and
3) the organisation that suffered the breach is unable to prevent the risk of serious harm through remedial action.

The key findings, when compared to the first half of 2022, were:

- a 26% increase in reported data breaches (497 breaches, up from 393)
- a 26% increase in reported data breaches (497 breaches, up from 393)
- health service providers continue to top the list, reporting 14% of notifiable data breaches (71), followed by the finance industry (68)
- human error was the cause of 25% of all notifications (123 notifications, a 5% decrease from 129)[1]
- contact information remains the most common type of personal information involved in breaches
- the majority (88%) of notifiable data breaches affected 5,000 individuals or fewer, and
- 71% of entities notified the OAIC within 30 days of becoming aware of an incident, continuing to demonstrate both overall compliance with the 30-day timeframe and the difficulty of detecting incidents and completing investigations within a few weeks.

[1] While human error is a factor in many data breaches in various forms, it should be noted that this category of notifiable data breach relates specifically to cases where a person discloses or loses personal information directly (e.g. by sending it to the wrong recipient, or losing a data storage device).

The latter half of 2022 also saw several large-scale and high-profile data breaches, which fast-tracked the enactment of the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022*. As previously reported, the *Privacy Act 1988* (Cth) was amended last year to give the OAIC expanded investigative powers and to implement a significantly increased penalty regime for serious or repeated interference with privacy.

In light of the above, OAIC Commissioner Angelene Falk commented in the report that:

- "Organisations should take appropriate and proactive steps to protect against and respond to a range of cyber threats."
- "This starts with collecting the minimum amount of personal information required and deleting it when it is no longer needed."
- "Organisations need to be on the front foot and have robust controls, such as fraud detection processes, in place to minimise the risk of further harm to individuals."

In short, the ever-increasing incidence of notifiable data breaches, as well as the increase in penalties and regulatory activity, continue to suggest that insured organisations should ensure they are robustly protecting personal information they collect and hold, and are equipped to act quickly and comprehensively to contain a data breach. This will include having an up-to-date data breach response plan and communications in place, and making sure all personnel are familiar with their roles and obligations.

> Insured organisations should ensure they are robustly protecting personal information they collect and hold, and are equipped to act quickly and comprehensively to contain a data breach.

14%

of notifiable data breaches were reported by ***health service providers***

26%

increase in reported data breaches

FBI shuts down Hive ransomware network

After a month-long campaign working with law enforcement agencies in Germany and the Netherlands, the US Department of Justice has announced that the FBI has taken control of the servers used by the Hive ransomware group, cutting off its ability to communicate with its members and extort its victims.

Hive is one of the most active and prominent ransomware groups, known for extorting hospitals, school districts and critical infrastructure. It employs the ransomware-as-a-service model (where they develop a ransomware strain and create an interface with which to operate it and then recruit affiliates to deploy the ransomware against victims). Hive is particularly known for double extortion tactics in which the attackers encrypt the victims' data to prevent victims from accessing it and also threaten to publicly leak the information unless the ransom is paid. The data used is most frequently the most sensitive data in a victim's system to increase the pressure to pay. Once the ransom is received from the victim, Hive affiliates and administrators split the money 80/20, according to the FBI. Since June 2021, the group has targeted more than 1,500 victims globally and captured more than $100 million in ransom payments.

The takedown of Hive follows an earlier win by the FBI in July 2022 when it penetrated the Hive gang's computer networks, captured its decryption keys, and provided more than 300 decryption keys to victims of Hive attacks around the world, saving victims from collectively paying a ransom amount of $130 million.

The group's dark web site (where it typically leaks stolen data) now displays a message in both English and Russian stating: "This hidden site has been seized. The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Hive Ransomware."

However, despite this win, ransomware attacks are far from over. Ransomware groups are difficult to wipe out because the members tend to resurface in other groups and capacities. For this reason, Caroline Seymour, Vice President of Product Marketing for disaster recovery firm Zerto, emphasises that to combat a ransomware attack, an organisation's primary focus must be getting their system back up and running.

"*When a service provider is disabled and access to data is held in exchange for ransom, the best way to fight back and get up and running again is to have a recovery solution in place that protects systems from disruption and provides a path to instant recovery.*"

However, many organisations turn to backups that are a day or even a week old to restore their data, Seymour adds. That leads to gaps and data loss that can impact the business and add to the overall cost of recovery.

UK sanctions ransomware actors

The recent sanctioning of various ransomware actors in the UK may have implications for businesses in Australia considering paying ransoms, as well as for insurers that span multi-jurisdictions.

Each case of ransomware will require closer scrutiny on a case-by-case basis as the sanctions regime continues to develop.

Recent Coveware report (Q4)

Coveware is a cyber extortion incident response firm. It recently released its Q4 report, which featured some interesting insights:

Fewer ransomware victims are paying – only 37% of victims paid ransom in Q4 of 2022. On an annual basis, 41% of victims paid in 2022 compared to 76% in 2019.

Although fewer companies are paying ransoms, the average ransom payments have increased by 58% in Q4 2022 from Q3 2022. Due to the decline in profitability, Coveware has seen that threat actors are changing their tactics. They are slowly moving to targeting victims higher up in the market, hoping it will result in larger ransom payments.

The most observed ransomware variant in Q4 2022 was Hive. However, as discussed above, the FBI has recently taken control of the servers used by the Hive ransomware group.

In Q4, the public, professional services, healthcare and software services sectors were the industries most impacted by ransomware. Coveware saw a noticeable difference in industries impacted by ransomware as there was a move away from ransomware attacks on the professional services sector, which has historically been one of the biggest targets. This aligns with threat actors' new tactics in targeting larger mid-market companies.

Coveware has identified three key factors that have contributed to this low number of ransomware payments:

1) Organisations are investing more in security and incident response planning. As organisations have heightened their appreciation for existential risk of a ransomware attack, this has helped increase funding to security and incident response teams.
2) Law enforcement agencies have changed strategies slightly. They are focusing on arrests, as well as on helping victims, and imposing costs on economic levers which make cybercrime profitable.
3) Fewer ransomware victims are paying, causing the dollar amount of ransom proceeds in the cyber extortion economy to shrink. This means the costs of carrying out a cyberattack increase. A smaller number of threat actors will be able to make a living from ransomware attacks, in turn leading to fewer attacks.

OECD moves to facilitate cross-border transfers of personal information

On 14 December 2022, the member countries of the OECD, including Australia, adopted the *Declaration on Government Access to Personal Data Held by Private Sector Entities*. While not having the force of law, the declaration is significant for international privacy law and cross-border data transfers as it represents a first step to enabling smoother cross-border data flows. As the OECD notes, this is a critical enabler of the global economy.

To recap:

- In the *Schrems II* decision, the Court of Justice of the European Union (CJEU) struck down the so-called "EU-US Privacy Shield", an intergovernmental agreement on which thousands of US companies relied for processing data sourced from EU trading partners and consumers. The *Schrems II* decision ushered in a fairly undesirable legal status quo; the personal information of EU (and now UK) citizens couldn't be sent offshore to countries whose data protection regimes were not 'adequate' for the purposes of the EU General Data Protection Regulation (GDPR) unless additional safeguards were put in place.

While the reasons for lack of adequacy vary, the *Schrems II* decision was focused on US laws that gave government agencies and law enforcement bodies broad powers to access personal data held by corporations with limited controls and protections.

- Australia is among the countries considered not to have adequate data protection laws in place. Apart from the fact that there are several exemptions to the application of the Privacy Act, we also have laws that are analogous to those discussed in *Schrems II* (e.g. problematic for GDPR purposes because they allow law enforcement agencies to obtain personal information without a warrant).
- As a result, companies cannot share the personal data of EU and UK citizens with vendors, partners or corporate group members in Australia (and other countries whose data protection laws are not 'adequate') unless appropriate safeguard measures are put in place. Those safeguards generally need to consist of the implementation of standard contractual clauses or binding corporate rules within corporate groups, and other supplementary measures to augment the level of protection available to EU citizens whose data is being transferred.
- The end result is that companies seeking to transfer EU (and UK) citizens' data to countries like Australia have to jump through a complicated set of regulatory hoops or risk non-compliance with the GDPR and the associated hefty penalties. This creates legal and operational inefficiency, with each company needing to perform its own analysis and implement its own supplementary measures before basic business functions can be performed. This is particularly troublesome for intra-corporate group data transfers and for corporations operating across jurisdictions.

The declaration addresses this issue head-on by setting out the safeguards that countries should implement when their government agencies and law enforcement bodies access personal data held by companies. The declaration recognises seven shared principles, which the OECD Members have agreed reflect commonalities drawn from their existing laws and practices, including transparency, legal basis, and redress.

Over time, the implementation of the safeguards referred to in the declaration by member countries should:

- lessen the need for individual corporate assessments of appropriate safeguards, and
- make it less likely that companies moving EU (and UK) citizens' data overseas will run afoul of GDPR restrictions on data-offshoring.

The declaration is a step in the process of solving a privacy compliance headache that has been plaguing companies who do business in (and so need to transfer EU data to) Australia. If implemented by member countries, it will ultimately reduce the compliance burden on insureds and their exposure to penalties under the EU GDPR regime (and UK equivalent).

APRA's supervision priorities

APRA has released its policy and supervision priorities for the next 12 to 18 months. One of its most significant priorities is to improve the 'cyber resilience' of regulated entities. This priority has emerged in the wake of significant data breaches in 2022 (e.g. the Optus and Medibank incidents) that resulted in the exposure of the personal information of millions of Australians.

As improving cyber resilience becomes a top priority for APRA, the regulator has indicated that it will undertake comprehensive assessments of an entity's compliance with Prudential Standard CPS 234 Information Security (CPS 234) – a rule that ensures that an entity has the appropriate security measures in place to withstand cyberattacks and other information security threats. In addition, the priorities statement from APRA indicates that, in 2023, it will 'rigorously pursue' entities that breach the CPS 234 standard and conduct "targeted deep-dive reviews on areas of weakness that fail to meet expectations".[2]

One of APRA's other priorities is ensuring "sound operational risk management", meaning that a key goal for APRA is to ensure financial institutions are able to identify and respond to business disruptions caused by events such as the pandemic, natural disasters and cyberattacks. As a result, APRA proposes to introduce a new cross-industry Prudential Standard CPS 230 Operational Risk Management (CPS 230) by 1 January 2024, which will set out the minimum standards for managing operational risk, including updated requirements for business continuity.[3]

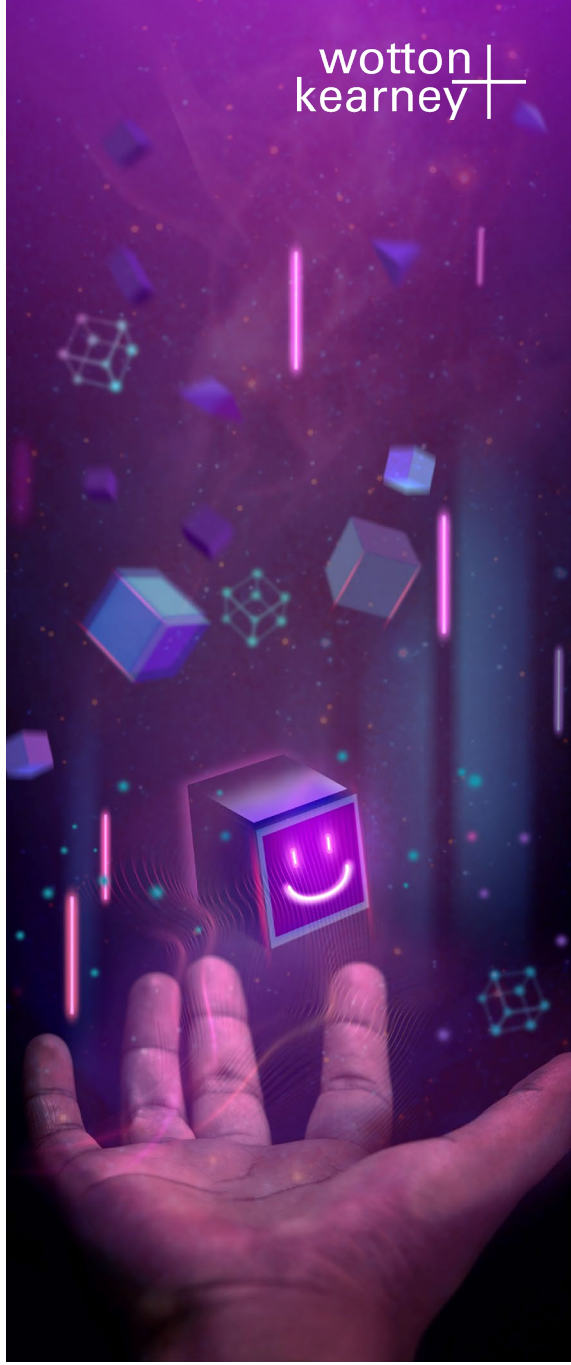
Given APRA's announcement that it intends to scrutinise organisations for compliance with CPS 234, it is imperative that, in the next 12 to 18 months, APRA-regulated entities remain aware of the notification requirements under CPS 234. Specifically, they need to[4] notify APRA of:

- a security incident within 72 hours of becoming aware, and
- any "information security control weaknesses" within 10 days of becoming aware.

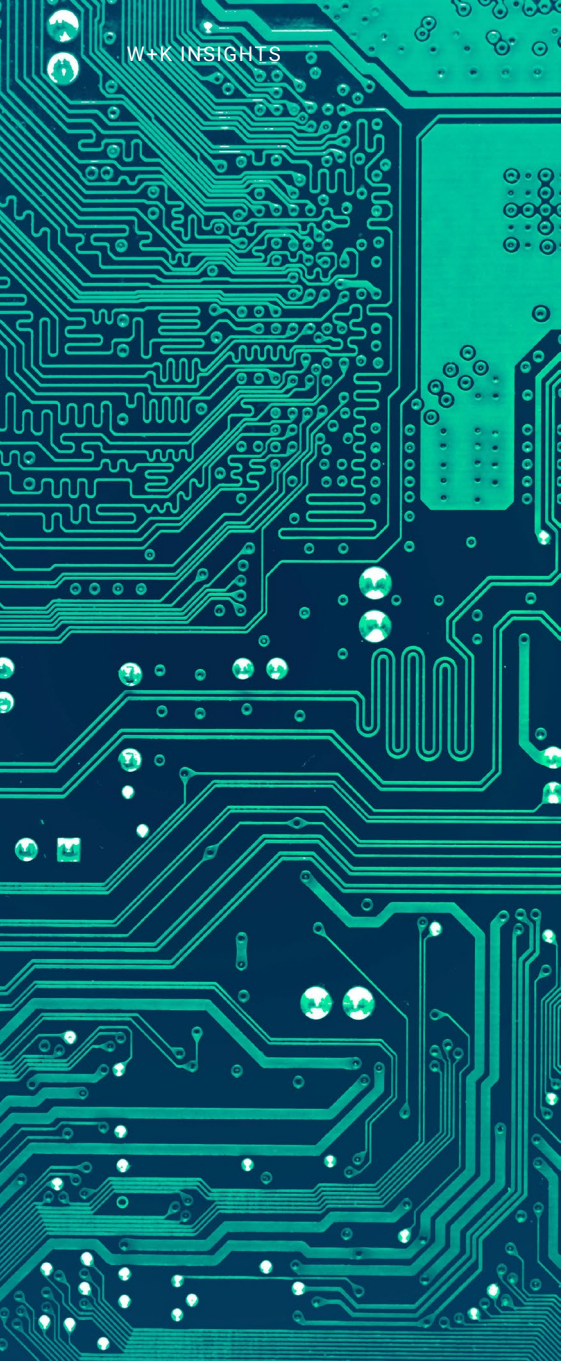
Covering crypto

W+K senior associate Jessica Chapman, who won the Australian Insurance Law Association's inaugural Gill Award for her paper on insuring the cryptocurrency industry, recently contributed to a feature on cryptocurrency and Web3 in the *ANZIIF Journal*. The feature explored the risks associated with the assets and what aspects are still holding insurers back from offering insurance products to the sector.

The key issue is regulatory certainty, with most regulators around the world acting very slowly and with caution. While shifting the tide will require a lot of time and work by regulators, this is an important and unavoidable process, not least from a consumer protection perspective. Regardless of what regulators do or do not do, the industry is not slowing down, and new applications of this technology are being developed month by month. The outcome of the Australian Federal Government's ongoing review of the sector, and the regulatory position, will be one to watch.



[2] Information Paper, APRA's Supervision Priorities (1 February 2022), p. 6
[3] https://www.apra.gov.au/operational-risk-management
[4] APRA, Prudential Standard CPS 234 Information Security



wotton kearney

Technology Liability

Recent NSWCA decision highlights cost of IT liability risk

A recent NSW Court of Appeal (NSWCA) decision, *Renown*, highlights the potential for IT providers that breach supply and installation contracts – and their insurers – to end up paying out higher damages awards. Notably, the NSWCA found that the proper measure of damages involved assessing the reasonable costs when they were actually incurred or, if not incurred already, the reasonable costs as proved as at the trial.

In litigated cases with similar circumstances, insurers and insured IT providers should be aware that:

- damages for loss incurred due to defective IT systems/products may be assessed as at the date of hearing
- replacement costs of a defective IT system/product may be paid out in circumstances where this is more economical than remediating the defective system
- even if "the guilty party is entitled to an allowance for the benefit to the innocent party from that action (the avoided loss principle)", this saving by way of 'betterment' will only be accounted for in damages awarded if the saving is substantiated by the 'guilty' party via expert evidence, and
- casual and temporary employees' remuneration may be included in the award of damages where the nature of the employees' employment solely relates to working on solutions to resolve issues with defective IT systems/products. However, this case demonstrates that damages for diversion of time for ordinary employees are unlikely to be recoverable.

For more information about this appeal decision and how it provides useful guidance for IT providers (particularly software developers and suppliers) and their insurers regarding the assessment of damages where a breach of a supply and installation contract is established, read our article here.

> Notably, the NSWCA found that the proper measure of damages involved assessing the reasonable costs when they were actually incurred or, if not incurred already, the reasonable costs as proved as at the trial.

New Zealand

OPC provides guidance for breaches in the healthcare sector

The OPC has provided some commentary on reporting and avoiding privacy breaches in the health sector.[5]

The health sector is by far the most highly represented sector in the OPC's privacy breach notification statistics. The OPC's latest blog post shines a light on the types of issues seen in the health sector and its expectations around breach notification, highlighting that:

- repeat offenders are an issue – many breaches reaching the serious harm threshold were caused by previously identified issues that had not been resolved, or where remediation had not been actioned
- it was important organisations documented and addressed 'near misses' to prevent re-occurrences
- breaches did not just occur through external disclosures, and could extend to inappropriate internal access, or breaches other disclosure (for example, destruction of information) – staff were a common victim of internal privacy breaches
- human error remained a major cause of privacy breaches (although the OPC's more recent statistics point to malicious activity overtaking accidental disclosure as the number one cause of privacy breaches[6]), and
- email hygiene and confirming contact details are critical to avoiding email-based breaches – major breaches had been reported as a result of individuals simply completing an address incorrectly or failing to use the BCC field.

The OPC's post re-enforces that good privacy practices are critical to avoiding privacy breaches, or at the very least minimising the risk and ensuring you respond in the right way. While accidents do happen, it is important organisations have engrained processes to ensure that these are logged, and lessons learned and implemented. Critical to this is ensuring staff can recognise a privacy incident, and that privacy officers are empowered to implement change. Organisations should also have a clear incident response plan in place.

The OPC's post emphasises that while all breaches need a response, that response does not always need to include notification. Entities holding and using personal information should have a clear framework for distinguishing a "notifiable privacy breach" from a non-notifiable incident.

[5] https://www.privacy.org.nz/blog/reporting-and-avoiding-privacy-breaches-in-the-health-sector
[6] https://www.consumer.org.nz/articles/malicious-activity-now-the-main-cause-of-serious-privacy-breaches-in-nz

Injunctions endorsed as a tool in the incident response toolkit

Following the well-publicised Mercury IT ransomware late last year, the High Court has now made permanent an injunction sought by Te Whatu Ora restricting access to information published on the dark web.[7] The original injunction, sought without notice, restrained all use, access or distribution of information exfiltrated from Mercury IT's network during the attack. Information was subsequently posted on a dark web data leak website. The injunction mirrors that obtained following the Waikato DHB ransomware attack in 2021.

The OPC has released a blog post on the injunction, noting that injunctions are an important tool in responding to a cyber incident: "You have to act fast. It might sound drastic but reaching out to the courts can help prevent further harm by making it clear to everyone, that no one should breach the confidences that apply to that compromised data."[8] While this is a useful endorsement of injunctions, this latest commentary from the OPC suggests that injunctions will be seen as a necessary element of any response to a well-publicised cyber incident going forward. This resets expectations in a similar way to the OPC's comments around dark web monitoring in the wake of the Waikato DHB attack.

Beyond restricting dissemination, injunctive relief can prove useful for a range of purposes in the wake of a cyber incident, including compelling cloud service providers to reveal details of information exfiltrated to their platforms (see, for example, *C v Mega Limited* [2020] NZHC 2636, in which the applicant obtained orders against Mega Upload for disclosure of documents and information). As the OPC points out in its blog post, the key is to identify risks early and act to obtain any necessary injunctive relief quickly. Engaging with experienced breach counsel early in the process is of critical importance.

CERTNZ publish cyber incident communications advice

CERTNZ has issued a framework for public communications following cyber incidents.[9] The framework provides some useful guidance for organisations either preparing incident response plans or dealing with communications in the heat of a live incident. We encourage agencies to consider the framework alongside their insurance obligations and any legal notification requirements and guidance.

The CERTNZ framework encourages entities to work through a robust process of ascribing responsibilities for various communications and working through a notification framework. Key takeaways include:

- identifying and empowering a communications lead
- ensuring the communications lead has access to the incident response team
- balancing the message to ensure it communicates what you need while also not tipping off attackers in a way that might be unhelpful, or making statements you cannot support and may need to walk back from later, and
- ensuring messages accept responsibility, avoid downplaying, address feelings of vulnerability, are easy to understand, and avoid damaging credibility.

The framework is a useful tool for organisations considering proper communications in a cyber incident. We advise entities to contact their insurers and professional advisors before making any substantive communications. Engaging with communications experts and breach counsel will ensure that any communications are suitable for the given situation.

[7] *Te Whatu Ora Health New Zealand v Unknown Defendants* [2022] NZHC 3568
[8] https://www.privacy.org.nz/publications/statements-media-releases/injunctions-a-valuable-tool-in-data-breach-toolkit-2
[9] https://www.cert.govt.nz/business/guides/communicating-a-cyber-security-incident/public-communications-for-cyber-security-incidents-a-framework-for-organisations

Global insights from Legalign Global

Our Legalign Alliance colleagues, DAC Beachcroft, provide an Asia-Pacific update.

Indonesia passes new legislation on personal data protection

Our Legalign Global colleague DAC Beachcroft review new legislation introduced in Indonesia responding to periods of concern in respect of repetitive data breaches.

Ushering in a new era for data protection practices in Indonesia, it is hoped that the Personal Data Protection Law will act as a handbrake against the levels of criminal activity recently seen in local data breach occurrences.

You can access the full article by DACB's Andrew Robinson, Summer Montague and Hermanto Moeljo here.

Singapore: Court of Appeal rules on 'emotional distress' as loss or damage

We consider a recent decision in the Court of Appeal in Singapore holding that "Emotional Distress" should constitute a form of loss or damage under Section 32(1) of the Personal Data Protection Act.

The decision provides useful clarification – in that emotional distress is an actionable head, whereas a simple loss of control is not – and serves as a cautionary warning to all organisations engaged in the collecting or processing of personal data.

You can access the full article by DACB's Andrew Robinson, Summer Montague and Hermanto Moeljo here.

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

- Alexander Holburn (Canada)
- BLD Bach Langheid Dallmayr (Germany)
- DAC Beachcroft (UK)
- Wilson Elser (US)

Australian Cyber, Privacy + Data Security contacts

Kieran Doyle
Head of Cyber + Technology (Sydney)
T: +61 2 8273 9828
kieran.doyle@wottonkearney.com.au

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

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

Jessica Chapman
Senior Associate (Sydney)
T: +61 2 8273 9876
jessica.chapman@wottonkearney.com.au

Ellie Brooks
Senior Associate (Melbourne)
T: +61 3 9604 7987
ellie.brooks@wottonkearney.com.au

Ryan Loney
Senior Associate (Melbourne)
T: +61 3 9116 7817
ryan.loney@wottonkearney.com.au

Matt O'Donnell
Senior Associate (Brisbane)
T: +61 7 3236 8736
matt.odonnell@wottonkearney.com.au

Carmen Yong
Solicitor (Sydney)
T: +61 2 8273 9824
carmen.yong@wottonkearney.com.au

Jordan Chen
Solicitor (Sydney)
T: +61 2 9064 1875
jordan.chen@wottonkearney.com.au

Jorge Nicholas
Solicitor (Melbourne)
T: +61 3 9604 7995
jorge.nicholas@wottonkearney.com.au

Tara Connelly
Paralegal (Sydney)
T: +61 2 9064 1864
tara.connelly@wottonkearney.com.au

Cecilia Askvik
Business Development Manager (Sydney)
T: +61 2 9064 1839
cecilia.askvik@wottonkearney.com.au

Avram Lum
eDiscovery + Cyber Forensic Manager (Sydney)
T: +61 2 8273 9875
avram.lum@wottonkearney.com.au

Kat Norton
eDiscovery + Cyber Consultant (Sydney)
T: +61 2 8273 9988
kat.norton@wottonkearney.com.au

New Zealand Cyber, Privacy + Data Security contacts

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

Laura Glasson
Senior Associate (Christchurch)
T: +64 4 974 0464
laura.glasson@wottonkearney.com

Mathew Harty
Solicitor (Auckland)
T: +64 9 940 3882
mathew.harty@wottonkearney.com

Casey Williams
Solicitor (Wellington)
T: +64 4 909 9714
casey.williams@wottonkearney.com

Giulia Wiesmann
Solicitor (Wellington)
T: +64 4 974 4020
giulia.wiesmann@wottonkearney.com

To learn more about our cyber, privacy and data security expertise, click here.

Technology Liability contacts

Kieran Doyle
Head of Cyber + Technology (Sydney)
T: +61 2 8273 9828
kieran.doyle@wottonkearney.com.au

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

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

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

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

Karren Mo
Special Counsel (Melbourne)
T: +61 3 9116 7869
karren.mo@wottonkearney.com.au

To learn more about our technology liability expertise, click here.

Australian offices

Adelaide
Level 1, 25 Grenfell Street
Adelaide, SA 5000
T: +61 8 8473 8000

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

Canberra
Suite 4.01, 17 Moore Street
Canberra, ACT 2601
T: +61 2 5114 2300

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

Melbourne – Health
Level 36, Central Tower
360 Elizabeth 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

www.wottonkearney.com.au

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

wotton kearney

A founding member of LEGALIGN GLOBAL

Chambers TOP RANKED Asia-Pacific 2023 Wotton + Kearney

Australasian Lawyer 2021 5-STAR CYBER LAWYERS