Australasia's largest insurance law firm

wotton kearney

A founding member of LEGALIGN GLOBAL

Cyber, Tech & Data Risk Report

DEC22

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 4, December 2022

We are delighted to publish Issue 4 of our *Cyber, Tech and Data Risk Report*, which is our final wrap-up of relevant news for the calendar year for insurers, brokers and their customers doing business in Australia and New Zealand in cyber, tech and data.

In this month's report, we look at a range of cyber issues and developments, including the Australian Government responses to the proliferation of cyber incidents involving major Australian corporates and the increased consequences of data breaches. We discuss AFCA's recent decision regarding a 'misleading advice' cyber dispute, and how international security pacts have heightened Australia's risk of cyberattacks. We also share highlights from recent ACSC and OAIC reports, as well as some insights from our Legalign Global partners, including into emerging threats and supply chain breaches.

In the IT liability space, we look at Snapchat's alleged liability for drug deaths and a range of emerging risks associated with the metaverse. We also explore the first decision in a common law jurisdiction that considers the duties of blockchain software developers.

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

It's worth keeping in mind that hackers increase the frequency of their attacks over the holiday season. W+K's Cyber, Privacy + Data Security team will be on-call, monitoring cyberxmas@wottonkearney.com.au and our Cyber Incident Hotline over the break. We are available to take instructions, triage calls and help with urgent incidents. Find out more here.

CYBER INCIDENT HOTLINE
1800 316 706

Cyber – Australia

Legislative developments – privacy

Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

Parliament passed the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 on 28 November 2022. The OAIC has welcomed[1] this development as it "enhances the OAIC's ability to regulate in line with community expectations and protect Australians' privacy in the digital environment" and "introduces significantly increased penalties for serious and or repeated privacy breaches and greater powers for the OAIC to resolve breaches."

The Bill increases the maximum penalties for serious or repeated privacy breaches from the current $2.22 million penalty to whichever is the greater of:

- $50 million
- three times the value of any benefit obtained through the misuse of information, or
- 30 per cent of a company's adjusted turnover in the relevant period.

The Bill also provides the OAIC with greater powers to resolve privacy breaches and quickly share information about data breaches to help protect customers by:

- providing the OAIC with greater powers to publicly share information that is in the public interest, as well as gather information (particularly regarding data breaches), and
- widening its extra-territorial application to include organisations that carry on business in Australia (even if they do not necessarily collect or hold information in Australia).

NSW – Privacy and Personal Information Protection Act 1998 (PPIP Act)

The Privacy and Personal Information Protection Amendment Bill 2022 passed in the NSW Parliament on 16 November 2022. The amendments to the PPIP Act will come into effect 12 months following assent, from 28 November 2023.

They aim to strengthen privacy legislation in NSW by:

- creating a Mandatory Notification of Data Breaches (MNDB) Scheme that will require public sector agencies bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm
- applying the PPIP Act to all NSW state-owned corporations that are not regulated by the Commonwealth *Privacy Act 1988*, and
- repealing s117C of the *Fines Act 1996* to ensure that all NSW public sector agencies are regulated by the same mandatory notification scheme.

The MNDB Scheme will require agencies to satisfy other data management requirements, including maintaining an internal data breach incident register and having a publicly accessible data breach policy.

[1] https://www.oaic.gov.au/updates/news-and-media/oaic-welcomes-passing-of-privacy-bill

Ahead of the Scheme's implementation, the Information and Privacy Commission NSW has announced[2] it will work with agencies covered under the PPIP Act and release guidance and resources to ensure they have the required systems, processes and capability in place.

Government considers new laws to make ransom payments illegal

Australia's Home Affairs Minister, Clare O'Neil, recently announced that the government is considering making payment of ransoms to threat actors illegal, following recent high-profile attacks in Australia. The Minister emphasised that, in the short-term, cyber security reform needs to be successful. She also made it clear the government is considering longer-term outcomes, such as banning ransom payments. The Minister also mentioned that Medibank, which recently suffered a data breach that resulted in the medical histories and private information of millions of customers being stolen, did the right thing in not paying the ransom payment demanded by the threat actor.

Navigating the post-Optus cyber legal landscape

We recently published an article that focuses on the fallout from recent data breaches, including the various actions the Australian Government has taken in response to the proliferation of cyber incidents involving major Australian corporates and the increased consequences of data breaches.

The measures the Government is taking or proposing include:

- the passing of the *Privacy Legislation Amendment (Enforcement and Other Measures) Act* 2022, which significantly increases the maximum penalties for 'serious' or 'repeated' privacy breaches
- temporary amendments to the *Telecommunications Regulations 2022* (Cth) to enable telecommunications carriers to disclose documents and information to financial services providers and state and federal agencies and authorities (to facilitate the management of fraud risk arising from the Optus data breach)
- more powers and a higher budget for the Australian privacy regulator, OAIC, to boost its investigative and enforcement capacity, and
- an expanded extra-territorial application of the Privacy Act to foreign organisations carrying on a business in Australia, even if they do not obtain personal information directly from a source in Australia.

Mooted additional laws in the cyber, data and privacy space include:

- laws to regulate how companies manage the data they collect (there is no indication yet of what those data reform laws might be, or how they might fit with existing regimes)
- reform of the *Security of Critical Infrastructure Act* (which the Australian Government considers did not assist it when the Optus breach occurred), and
- regulation of ransomware payments.

Other privacy reforms being considered (expected in 2023 and beyond) include eliminating existing exemptions from the application of the Act, stronger requirements for consent (to collection and use of data), and the introduction of a right of individual enforcement (e.g. a statutory tort of privacy).

Put together, the reforms and proposed reforms could be expected to materially increase the risk, complexity and cost of responding to cyber security incidents and data breaches, and, almost inevitably, the average cost of cyber insurance claims. In the current Australian landscape, well-developed privacy and data policies and processes, as well as cyber incident and data breach response capability, are an essential addition to cyber security resilience and a sound investment in protection from heightened regulatory consequences.

[2] https://www.ipc.nsw.gov.au/media-releases/media-release-nsw-privacy-commissioner-welcomes-assent-privacy-and-personal-information-protection-amendment-bill-2022

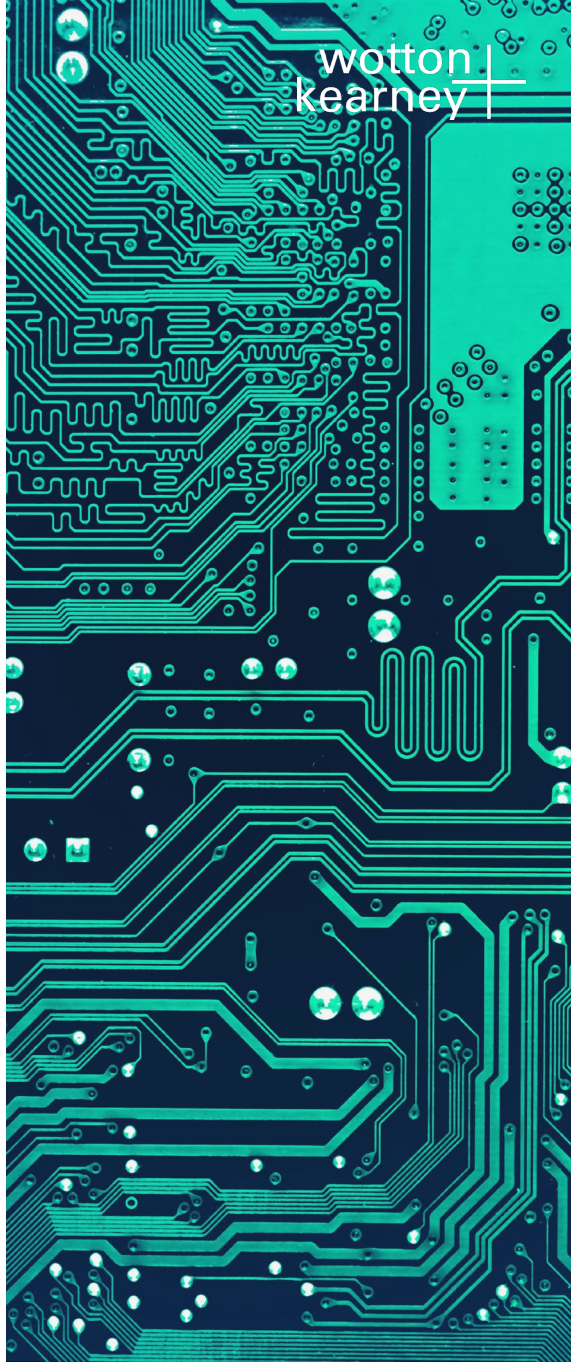
AFCA finds in favour of insurer in ‘misleading advice’ cyber dispute

A recent decision by the Australian Financial Complaints Authority (AFCA) regarding a ‘misleading advice’ cyber dispute has now been published. It concerns the distinct roles of insurers and their representatives during the claims process and emphasises the need for policyholders to be familiar with the terms and conditions of their insurance policies.

On 10 July 2021, the complainant made a claim under its cyber event protection insurance policy after a cyber breach event resulted in its hardware becoming encrypted by a threat actor. The insurer declined the claim in part, saying that tangible property (hardware) was not covered under the complainant’s policy as the complainant had not selected that optional cover at inception. The complainant stated that it was misled by the insurer into believing that the cost to replace the hardware would be covered, claiming that, during the claims process, it was advised by the insurer and its representatives not to pay the threat actor to regain its hardware and to purchase new hardware. The value of the new hardware purchased by the complainant on the advice of the insurer’s cyber breach coach was $52,366.

On 18 August 2022, the dispute was heard before the AFCA, which held that the insurer did not mislead the complainant about the scope of cover under the policy. Rather, there was evidence that the complainant was reminded by the insurer before it purchased the new hardware that tangible property was not covered under the policy. The insurer had clearly referred to the policy exclusion and reminded the complainant that it had not taken out the extra optional cover under its policy. The complainant also had access to the full terms and conditions of the policy and was told by its insurer that the cyber breach coach was not an insurance claims handler and was not going to be involved in making a decision on cover under the policy. The AFCA went on to state that the recommendations of the insurer and its representatives to replace the hardware were based on risk management and operational imperatives – replacing the hardware would be something the complainant would have to have done in any case.

Overall, the AFCA noted that it would not have been fair to require the insurer to pay a claim for which it is not liable under the policy, or otherwise. Interestingly, the AFCA also noted that, even if the insurer had misled the complainant, it does not consider that the complainant suffered loss as a result, as it is more likely than not that the purchase of hardware would have happened in any case. The complainant has an obligation to mitigate its losses where possible, and so it appears it took the appropriate steps in this case. The fact that, by the complainant taking that action, the insurer’s potential liability under another limb of cover was reduced/eliminated does not in itself mean the insurer should cover the cost of replacement hardware.



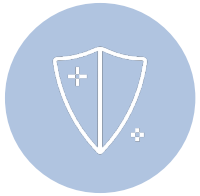
International security pacts heighten Australia's risk of cyberattacks

Australia's involvement in international security pacts (such as AUKUS and the Quadrilateral Security Dialogue) over the past two years has inadvertently put the nation at more risk of cyberattacks than ever. Australia is increasingly coming on to the radar of cyber hackers, leading to their increased scrutiny of Australian organisations. The ACSC has acknowledged[3] Australia's prosperity is attractive to cybercriminals. Brian Grant, the ANZ director of French technology group Thales Cloud Security, also suggests that many organisations have already been attacked but are not aware of it, as cyber hackers often "stay under the radar ready for an economic, geopolitical or financial event"[4] before they attack.

Consequently, current security approaches are no longer fit for the evolving threat landscape. The amendments to the *Security of Critical Infrastructure (SOCI) Act 2018* in July have resulted in many more organisations being subject to the strict 12-hour cyber incident reporting requirements. However, it is becoming clear that addressing these threats is not a matter of increasing compliance. Rather, organisations across the entire spectrum of critical infrastructure need to ensure that cyber security is part of their safety practices.

A global survey of 2,700 organisations has shown that while three quarters of respondents were very, or somewhat, concerned about security risks and threats from employees working remotely, only 45% had a formal ransomware plan in place, and only half of critical infrastructure organisations surveyed used multi-factor authentication.

In parallel, the Minister for Cyber Security flagged in a keynote address opening AustCyber's Cyber Week last month that the SOCI Act needed reform, noting it was not up to the challenges arising from recent high-profile cyber security incidents[5]. The Minister indicated a revamped national cyber security strategy will be published next year.



It is becoming clear that addressing these threats is not a matter of increasing compliance. Rather, organisations across the entire spectrum of critical infrastructure need to ensure that cyber security is part of their safety practices.

[3] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022#:~:text=Australia's%20prosperity%20is%20attractive%20to%20cybercriminals.&text=In%202021%E2%80%9322%2C%20cybercrimes%20directed,value%20transactions%20like%20property%20settlements.

[4] https://www.ragtrader.com.au/news/we-have-become-a-target-optus-hack-a-warning-for-retailers

[5] https://www.youtube.com/watch?v=0YCVS8DWKsM

Cyber basics – when do I have to report a data breach?

This article is the second in a series of 'cyber basics' articles, which aim to assist with cutting through the complexity of the law around cyber incidents and data breaches.

A data breach under Australian law occurs when personal information held by an organisation is lost, or is accessed or disclosed without authorisation. (To recap, the *Privacy Act* 1988 (Cth) defines personal information as "information or an opinion about an identified individual, or an individual who is reasonably identifiable".)

A data breach can be accidental, caused by a malicious third party, or caused by a failure in security/information handling systems. It can also cause harm to individuals whose personal information is disclosed as a result of the breach (for example, financial loss due to financial fraud). Examples of data breaches include an employee sending an email containing personal information to the wrong person, or a threat actor accessing personal information stored in an organisation's systems through the deployment of ransomware.

It's important to note that not all data breaches are reportable. The Notifiable Data Breach Scheme (NDB Scheme) under the Australian Privacy Act requires organisations to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals if there has been an 'eligible data breach' (EDB). These are the more 'serious' data breaches.

An EDB occurs when:

- personal information held by an organisation is lost, or accessed or disclosed without authorisation
- it is likely that individuals who have had their personal information compromised in the data breach are at risk of serious harm, and
- the organisation cannot prevent the likely risk of serious harm to the affected individuals by taking remedial action.

If an organisation has reasonable grounds to believe that an EDB has occurred, it must notify the OAIC and affected individuals as soon as possible.

An organisation that doesn't know whether an EDB has taken place, but has reasonable grounds to suspect that it may have, needs to investigate, and seek to complete that investigation within 30 days. If an EDB is confirmed, the organisation must then move quickly to notify affected individuals and the OAIC.

These investigation and notification obligations don't apply if the organisation is able to take remedial action that successfully prevents the likely risk of serious harm to individuals.

Specialist legal advice will usually be needed to assist with identifying and assessing EDBs, and the resulting notification obligations, and regulatory engagement.

Biometric data – novel application to high school vandalism tests the limits of the law

As discussed in our July 2022 issue, the use of facial recognition technology and sensitive biometric data (such as fingerprint scanning) remains controversial, with the OAIC commencing several investigations into uses of this type of personal information.

In a recent, novel application of the technology, Moorebank High School in Sydney has come under scrutiny for implementing a biometric fingerprint scanning system for students to access the bathrooms. The school's deployment of the technology to reduce persistent vandalism has been criticised as being "unreasonable and disproportionate"[6].

The *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIP Act) governs how NSW public sector agencies (in this case, the NSW Department of Education) manage personal information.[7] The Information Protection Principles (IPPs) in Part 2 of the PPIP Act set out how such personal information is to be collected, held, accessed and disclosed.

Taking a few key principles from the IPPs and applying them to the use of fingerprint scanning technology in the Moorebank High School case raises some interesting issues relevant to the use of biometric data generally.

The IPPs require that, among other things, the collection of personal information (including biometric information) is:

- **for a lawful purpose directly related to the organisation's function or activities, and reasonably necessary for that purpose** – In this case, Moorebank High School would argue that protecting the school's property from vandalism met that test. The counter to that argument is that there is a real question about whether it can be reasonably necessary (or directly enough related to a school's function or activities) to collect and use children's biometric data to prevent vandalism. These principles will be harder to satisfy when other means of performing a function or activity (in this case, minimising vandalism) are available and arguably as effective.
- **not excessive, and does not unreasonably intrude into the personal affairs of the individual** – Using fingerprint scanning to stop graffiti and damage involves a high level of surveillance of children and the use of biometric information. It inherently invites criticism that it is disproportionate to the harm. In simple terms, Moorebank High School's actions attracted the media's criticism because they failed the 'pub test' on whether or not the school was taking excessive measures to combat an annoying and expensive problem (but, not a problem so serious that it should be addressed by any means necessary or represented a fundamental health and safety issue).

The IPPs also require that personal information is protected against loss and unauthorised access, misuse and disclosure. A further concern with schools using technology like fingerprint scanners is whether the collection and storage of students' fingerprints, which may be held with other types of personal information, may increase the risk of serious harm (such as identity fraud) if a data breach occurred in future. Arguably, a higher level of security would also be required for storage of biometric data, given its sensitivity.

Given the types of issues flushed out by the Moorebank High School example, public sector agencies and other organisations considering the use of biometric data should conduct a thorough privacy impact assessment to assess whether the collection and use of such data is appropriate and proportionate. They should also ensure their privacy policies and consent mechanisms are robust and appropriately tailored. As a general observation, use cases for facial recognition and fingerprint scanning technology involving children, or where there are other means of achieving an objective, will raise material questions about whether the collection and use of the data is reasonable and necessary, and outweighs the possible risks. The benefit being sought will need to be thoughtfully weighed against the higher risk of regulatory attention, investigation and, ultimately, censure and penalty.

[6] https://www.theguardian.com/australia-news/2022/sep/06/sydney-schools-use-of-fingerprint-scanners-in-toilets-an-invasion-of-privacy-expert-says

[7] https://www.ipc.nsw.gov.au/privacy/nsw-privacy-laws/ppip; Section 4(2) of the PPIP Act clarifies that individuals' fingerprints are classified as 'personal information'.

14%

decrease in the number of breaches reported to the OAIC compared to last financial year

$98m

increase in financial losses due to business email compromise incidents

ACSC and OAIC reports

ACSC's *Annual Cyber Threat Report*

The ACSC released its *Annual Cyber Threat Report (June 2021 – July 2022)* recently, which highlights concerns about key cyber security trends the ACSC has identified during the last financial year. Some of the key trends are:

- ransomware remains the most destructive cybercrime
- the rapid exploitation of critical public vulnerabilities is becoming the norm and critical infrastructure networks globally are being targeted at significant rates by cybercriminals, and
- malicious state actors continue to persistently target Australia by engaging in malicious cyber operations as a part of their political and economic espionage.

Even though ransomware accounted for a small percentage of the total cybercrime reports received during FY21 – 22 (0.59%), it remains the most destructive cybercrime threat, according to the ACSC. A ransomware attack disrupts the victim organisation's business by encrypting data. It also poses a risk of reputational damage if stolen data is sold or released, which the latest highly publicised cyberattacks has brought attention to.

Fraud, shopping and online banking were the top reported cybercrime types, accounting for 54% of all reports received.

OAIC's *Notifiable Data Breaches Report*

The OAIC also released its *Notifiable Data Breaches Report (January – June 2022)* recently. The Privacy Commissioner emphasised that the results in the report, together with the significant impact of recent high-profile data breaches, highlight the importance of having robust information handling practices and incident response plans in place. The Commissioner also said that a "key focus for the OAIC is the time taken by entities to identify, assess and notify us and affected individuals of data breaches."

The OAIC's *Notifiable Data Breaches Report* highlights:

- malicious or criminal attacks remain the leading source of data breaches (63%) and human error is the second biggest source of data breaches (33%)
- 41% of all data breaches resulted from cyber security incidents, and the top sources of cyber security incidents were ransomware, phishing and compromised or stolen credentials (method unknown), and
- the OAIC has seen an increase in larger-scale data breaches (reportedly impacted a larger number of Australians) – there was also an increase in breaches affecting multiple entities.

Due to aspects such as the Small Business Exemption under the Privacy Act, these statistics and reports are not entirely reflective of the true picture and scale of incidents affecting Australian businesses. Further reforms to the Privacy Act will be important in providing greater clarity on the devastating impact of cyberattacks on small businesses and exempted industries in Australia.

Technology Liability – Global

Snapchat's alleged liability for drug deaths

On 13 October 2022, the families of eight deceased youths (aged 14 to 20 located in California, Michigan and Minnesota) filed a suit in Los Angeles County Superior Court against Snap Inc. (the Snapchat app's parent company). They claimed that the social media platform's unique privacy features promote and facilitate the sale of illegal drugs to teenagers and young adults.[8]

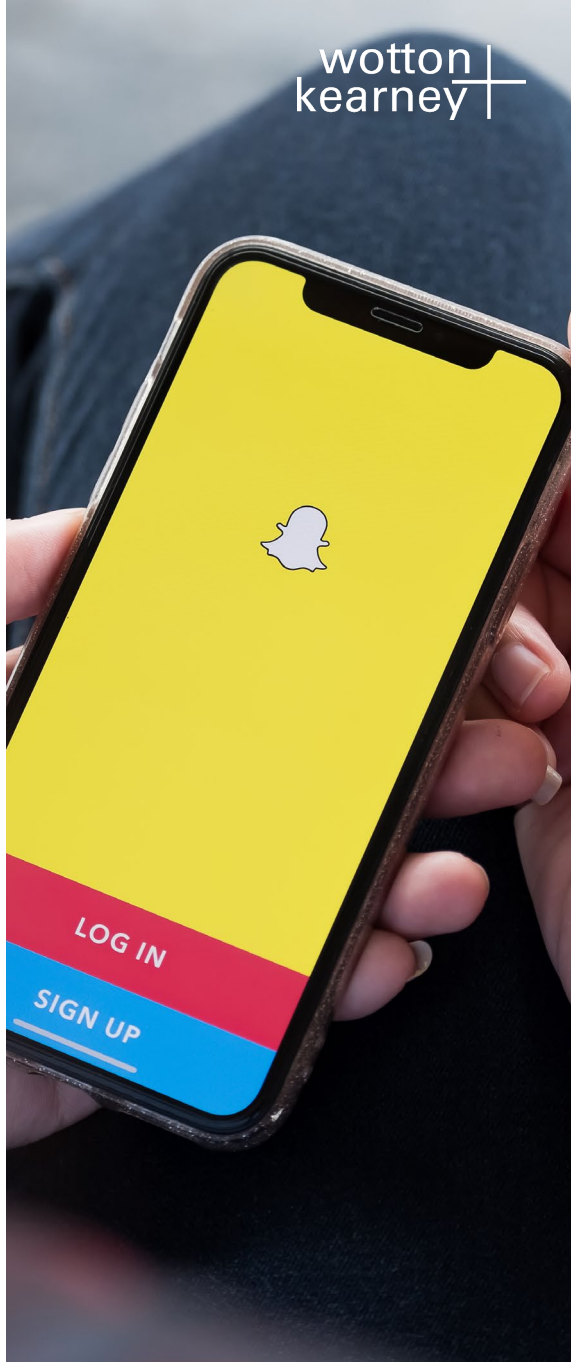
All eight victims allegedly believed they were purchasing prescription medications like Percocet or Xanax, but the pills were in fact laced with fentanyl, which is an inexpensive, synthetic opioid that is strong enough "to kill multiple people with a single dose"[9] and looks like the prescription medications.

The families have made various allegations against Snap Inc., including design defects, negligence, failure to warn, breaches of consumer protection laws, and invasions of privacy.

In response, Snap Inc. has vehemently denied the allegations and has emphasised that it has implemented "cutting-edge technology" to locate and terminate drug dealers' Snapchat accounts and remove in-app search results for drug-related terminology – instead, directing users to warning statements about the dangers of drugs such as fentanyl.

Before the deaths of the eight victims, Snap Inc. announced new and improved measures to combat drug dealing on the app, following deaths connected to drugs sourced on the app and a US CDC warning in late 2021 that fentanyl overdoses in youths had spiked significantly.[10]

This lawsuit raises serious questions about the liability of third parties (in particular, large social media companies like Snap Inc., TikTok and Instagram) for conduct of their users engaging in illegal activities. Practically, it would be unreasonable to expect Snap Inc. to monitor every user's actions and every exchange that takes place on the Snapchat platform. It will be interesting to see whether the judgment sheds light on whether Snap Inc.'s (and other third parties) implementation of various measures to make its platform safer reduces its liability for the victims' deaths.



[8] https://www.law360.com/cybersecurity-privacy/articles/1541050/snapchat-blamed-for-facilitating-sale-of-drugs-that-killed-8
[9] Ibid.
[10] https://www.theguardian.com/technology/2022/jan/20/snapchat-steps-combat-drug-dealing-on-platform

Liability issues in the metaverse

Have you heard of the 'metaverse'? If not, you will.

The metaverse can be loosely defined as "an integrated network of 3D virtual worlds"[11] that is "focused on social connection"[12]. It can be accessed via virtual reality (VR) headsets and navigated by users' eye/head movements, voice commands and controllers. Users can generate avatars to represent themselves to traverse the metaverse's virtual world for fun, to build out different communities, as part of multiplayer video games (such as Horizon Worlds), to shop for physical and virtual goods, and/or to accumulate digital assets (i.e. digital currencies and other virtual objects).

Approximately $13 billion was invested in the metaverse by way of capital and private equity funding in 2021. It is expected that the metaverse could generate up to $5 trillion in revenue by 2030.

While the buzz over the metaverse and its role in our future is exciting, its growth and evolution creates a whole new arena of legal issues and litigation to navigate.

Privacy issues

The broad spectrum of privacy concerns that exist outside of the metaverse seems likely to extend into the metaverse, which is saturated with user-generated content and digital footprints.

The advanced technology integrated into the metaverse can capture more extensive personal data than the information input by users via a basic keyboard and computer. For example, VR headsets record users' eye movements and emotions, and may even be used to identify a user's gender, health status, age and personality traits.[13]

Metaverse platforms also have the functionality to track what users say, what they do, who they are with, and where they go.[14] As security protocols on metaverse platforms are not entirely known or understood at this point in time, there is concern over the many opportunities for avatar identity theft and data breaches to transpire.

To deal with the propagation of these incidents, governments around the globe must first consider whether privacy rights are inherent or 'optional' in the metaverse. They also need to tackle which country's privacy/data laws (for example, the GDPR) will apply to protect users from the risk of harm. Given the current lack of regulation and standards, urgent consideration must be given to these privacy concerns to protect users from these unencumbered and imminent risks.

Financial fraud

As the metaverse expands and offers more opportunities for businesses and consumers, it also gives rise to fraud risks[15]. Given the metaverse's relative infancy, it is difficult to define the exact scope of what fraud will look like on the metaverse. However, as metaverse users commonly buy and sell assets, and employ digital currencies to facilitate payment of these assets, this presents many opportunities for cybercriminals to exploit.

[11] https://dl.acm.org/doi/10.1145/2480741.2480751
[12] https://en.wikipedia.org/wiki/Metaverse
[13] https://www.law.com/nationallawjournal/2022/06/06/plaintiffs-firms-eye-metaverse-as-growth-target-for-litigation/?slreturn=20220919235032
[14] https://bigthink.com/the-future/metaverse-fraud-digital-twins
[15] https://theconversation.com/we-need-to-anticipate-and-address-potential-fraud-in-the-metaverse-186188

Blockchain technology (which is largely decentralised, unregulated, and which facilitates untraceable payments) remains at the core of transactions on the metaverse – which cybercriminals have consistently used to launder money, commit identity fraud, and conduct scams.[16]

Other criminal activity on the metaverse will likely include what has been described by the North American Securities Administrators Association as the "same old financial scams simply dressed in new clothes"[17], such as fake giveaways, phishing attacks, malware/hardware hacking, and other social engineering hazards. These are commonly used to conduct identity and/or financial theft. Further, unidentified security issues on developing metaverse platforms and the lack of regulation make it easy for fraudsters to commit crimes and remain hidden (under the guise of their fake, untraceable digital identities).

Accordingly, to minimise risk of fraud, users should ensure that they act prudently when deciding whether or not to click on links, provide personal information, or transact on the metaverse.

In the event that fraud occurs, a question arises as to whether the technology companies behind the metaverse might be liable for the customers' financial loss.

Antitrust issues

Some jurisdictions are considering updating legislation and regulations to cater for competition and potential antitrust issues on digital platforms[18].

There is concern that mega metaverse companies (such as Meta and Microsoft) could collaborate to constrain their users' choices, and inflate prices if they eventually dominate the market.[19] For example, in July 2022, the US Federal Trade Commission (FTC) filed a Federal Court suit against Meta to prevent it from acquiring a company called Within Unlimited and its VR dedicated fitness app, Supernatural. The FTC alleges that Meta, as a key player in the existing VR fitness sector[20], is attempting to "illegally … buy market position instead of earning it on the merits", which will subsequently "eliminate the prospect of [Meta's independent] entry, dampening future innovation and competitive rivalry" for dedicated fitness VR apps.[21]

The FTC has since dropped its allegations that the merger would reduce direct competition between Meta and Within Unlimited, but has maintained that the deal could diminish potential competition.[22] While the legal battle ensues, this case demonstrates that metaverse companies will need to keep pre-metaverse competition law issues in mind.

Intellectual property issues

Intellectual property (IP) will likely become one of the most common and complicated legal issues arising from the metaverse, as there is uncertainty as to which IP laws from different jurisdictions apply, whether or not such laws can even apply to unique features of the metaverse, and what happens when users are part of various different metaverse platforms.

A key question regarding patents might be whether inventions created on the metaverse for the metaverse infringe patents outside of the metaverse, and vice versa.[23]

Another question is whether companies need to consider expanding their brands onto the metaverse and safeguard their IP rights on the metaverse (such as, trademarking any goods/services sold on the metaverse).

For example, Nike has now submitted several trademark applications to sell virtual sneakers and apparel on the metaverse and recently filed a metaverse-related lawsuit against StockX (a shoe resale platform). In this suit, Nike made various allegations, including trademark infringement and unfair competition for StockX's use of a non-fungible token (NFT) series that included digital images of Nike branded sneakers that are linked to physical Nike sneakers kept in StockX's facility.[24] While this lawsuit has not yet been resolved, its outcome will help shape how IP rights relating to the metaverse will be treated in the future.

[16] https://seon.io/resources/metaverse-fraud
[17] https://www.investmentexecutive.com/news/from-the-regulators/metaverse-is-ripe-for-scams-nasaa
[18] For example, the UK and the EU. https://www.morganlewis.com/pubs/2022/08/metaverse-a-jumpstart-guide-to-intellectual-property-antitrust-and-international-considerations#ip-considerations
[19] https://www.coindesk.com/policy/2022/10/19/eu-antitrust-officials-are-worried-about-competition-in-the-metaverse
[20] Meta owns Beat Saber, one of the most popular VR apps of all time, which is used for fitness. https://www.ftc.gov/legal-library/browse/cases-proceedings/221-0040-meta-platforms-incmark-zuckerbergwithin-unlimited-ftc-v
[21] https://www.ftc.gov/news-events/news/press-releases/2022/07/ftc-seeks-block-virtual-reality-giant-metas-acquisition-popular-app-creator-within
[22] https://www.law360.com/technology/articles/1541846/ftc-says-meta-buries-vr-fitness-data-in-merger-suit
[23] https://www.foley.com/-/media/files/insights/news/2022/03/metaverse-roundup-3-9-2022.pdf?la=en
[24] https://onpractice.law.com/4054359/ip-rights-metaverse-evolving-virtual-world?slreturn=2022-10-24T02:15:58+00:00

Personal injury risks

While the metaverse is an immersive virtual world, some individuals have become physically injured while using their VR headsets in reality.

The headsets, such as Meta's Oculus Quest, are noise cancelling and limit sight. They have left some users unable to detect hazards in their real-world surroundings, such as windows, walls and stairs, and caused injuries.[25]

Morgan & Morgan, the self-proclaimed largest personal injury law firm in the US, has stated that in some instances, "users have attempted to climb onto an elevated surface in the meta world and fallen on their faces because the surface doesn't actually exist, which has resulted in disfigurement and expensive hospital bills for these individuals."[26]

There may also be an influx of cases relating to personal injuries to individuals' minds, for example, alleging that the metaverse's realistic, violent simulations traumatise users, resulting in post-traumatic stress disorder.[27]

In general, metaverse-related personal injuries raise interesting questions about liability, for example, whether or not liability for an individual's injury/injuries be attributed to the metaverse platform and/or the VR headset manufacturer for causing or contributing to their injury/injuries. However, the ambiguity of liability for metaverse injuries will only dissipate over time as more and more lawsuits unfold.

As is the case with most technological advancements, the metaverse has grown exponentially over a short period of time and policymakers, regulators and courts are scrambling to catch up with the suite of legal issues and lawsuits that continue to arise.

It will be important for lawmakers to take initiative to ensure that they can quickly adapt to the range of legal issues and lawsuits created by the metaverse.

The European Commission has led the way by proposing new legislation, the *Digital Services Act* (approved by European Parliament on 5 July 2022), which seeks to create a framework to be implemented across the EU as a series of regulations, aimed at increasing the safety, accountability, and transparency of digital platforms (such as the metaverse) for users, while encouraging business growth and development. As stated by the rapporteur, Christel Schaldemose, the *Digital Services Act* "will put an end to the digital Wild West. We will enhance consumer protection, give users better rights, and regulate the core of the platforms' business model. All in all, what is illegal offline will also be illegal online."[28]

"It will be important for lawmakers to take initiative to ensure that they can quickly adapt to the range of legal issues and lawsuits created by the metaverse.

[25] https://beincrypto.com/metaverse-injuries-maimed-in-virtual-worlds-sue
[26] Ibid.
[27] https://guden.av.tr/metaverselaw
[28] https://www.europarl.europa.eu/news/en/press-room/20220613IPR32814/internal-market-committee-endorses-agreement-on-digital-services-act

Cryptocurrency – the Wild West of cyberspace

Cybercrime and cryptocurrency go hand in hand in the Wild West of cyberspace. Regulation and judicial consideration have struggled to keep pace with rapid developments in decentralised blockchain technology.

Once hailed as the frontier for a secure, trust-less, and anonymous financial ecosystem, decentralised finance has become a hotbed for financial fraud, scams and rug pulls. One case has illuminated the difficulties of sheeting home legal liability to developers of open source and decentralised software.

Tulip Trading Ltd v Bitcoin Association for BSV & others is the first decision in a common law jurisdiction that considers the duties of blockchain software developers. The High Court of England and Wales rejected the argument that developers owed duties to protect blockchain users by, for example, patching the network or re-establishing access to stolen assets.

The decision has since been appealed. The outcome of that appeal could have wide-ranging implications for developers and could inform the position likely to be taken by Australian courts if a similar matter arises in the jurisdiction.

Tulip Trading Ltd v Bitcoin Association for BSV & others

Tulip Trading Limited (Tulip) alleged that it owned bitcoin valued at approximately $4.5 billion, which was lost following a hack on the home computer of its CEO, Dr Craig Wright, during which the private keys needed to control the bitcoin were deleted.

Tulip claimed that the bitcoin was stored on several blockchain networks controlled by the 16 defendants, who were the core developers of those networks (Developers).

Key factual issues

Tulip claimed that the Developers had control over various forked versions of bitcoin, and that they had the ability to propose amendments to the underlying source code to give Tulip control over the bitcoin. Tulip claimed that the Developers owed it tortious and fiduciary duties, which compelled them to do this.

In response, the Developers argued they were part of a considerable, shifting group of contributors, which was decentralised in nature and devoid of any organisation or structure. Additionally, any change they were able to make would be ineffective, as the bitcoin miners (parties who validate bitcoin transactions) could/would refuse to run the updates.

Decision

On 25 March 2022, Justice Falk of the High Court dismissed Tulip's claim that the Developers owed any duty of care to users of their open source system. Justice Falk found that:

- software developers are a fluctuating body of individuals – as such, it could not be argued that they owe continuing obligations to remain as developers and make updates whenever it is in the best interest of owners of crypto assets, and
- the Developers were not in breach of a duty of care for failing to provide the means to recover stolen private keys in their software.

Commentary

Justice Falk considered whether developers involved with the development and custodianship of their software's underlying digital assets owed either fiduciary duties, or a duty of care, to those using their software.

Despite finding against Tulip on the alleged duty of care, Justice Falk accepted that, in certain circumstances, a more limited duty of care could conceivably be owed. For example, her Honour held that developers might have a duty to take reasonable care not to introduce a malicious software bug, or some other action that might compromise the integrity of the software system.

Appeal

The UK Court of Appeal has since granted Tulip permission to appeal the High Court's decision. The Court of Appeal will now examine the question of whether developers of cryptocurrencies and other blockchain assets owe a duty of care to investors using their technology.

In granting the appeal, Lady Justice Andrews alluded to consideration of whether a duty of care should be imposed and, if so, the nature and scope of such duties.

Given the similarities between the UK and Australian common law jurisdictions, the findings of the appeal will likely inform how a court would consider such a novel issue in Australia.

“Given the similarities between the UK and Australian common law jurisdictions, the findings of the appeal will likely inform how a court would consider such a novel issue in Australia.

Legalign Global

Informed Insurance 2022/2023

Resilience – new emerging threats challenge insureds and insurers

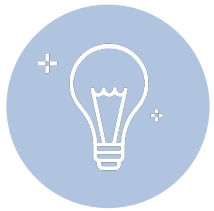
Many emerging threats are becoming critical operational issues, including greenwashing, supply chain issues, rising numbers of insolvencies, cyberattacks and ransomware. For insurers, these present important challenges to address for their clients and for society.

This report by our Legalign Global alliance partners, which features commentary by Wotton + Kearney's Head of Cyber + Technology Kieran Doyle, looks at why these emerging threats represent huge opportunities for insurers who can get a handle on them.

There are three additional *Informed Insurance 2022/23* reports that take a deeper dive into the issues of resilience, sustainability, and collaboration. You can also view all Legalign Global thought leadership on the *Informed Insurance* microsite.

Supply chain breaches

The OAIC's recent *Notifiable Data Breaches Report* drew attention to a marked increase in breaches affecting multiple entities. This article by our Legalign partner, DAC Beachcroft, usefully highlights key issues faced in supply chain breaches.



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
Special Counsel (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

Zoe Bennett
Senior Associate (Sydney)
T: +61 2 9071 1946
zoe.bennett@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

Kaila Hart
Associate (Sydney)
T: +61 2 8273 9838
kaila.hart@wottonkearney.com.au

Ronny Raychaudhuri
Associate (Sydney)
T: +61 2 9064 1833
ronny.raychaudhuri@wottonkearney.com.au

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

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

Jordan Chen
Paralegal (Sydney)
T: +61 2 9064 1875
jordan.chen@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

New Zealand Cyber, Privacy + Data Security contacts

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

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

David Smith
Associate (Auckland)
T: +64 9 377 1881
david.smith@wottonkearney.com

Keely Gage
Solicitor (Wellington)
T: +64 4 280 7921
keely.gage@wottonkearney.com

Mathew Harty
Solicitor (Auckland)
T: +64 22 162 1582
mathew.harty@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

Brigid Allen
Special Counsel (Melbourne)
T: +61 3 9116 7810
brigid.allen@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
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
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