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.

AUG22

W+K INSIGHTS

INTERACTIVE PDF

TOP RANKED Chambers Asia-Pacific 2022 Wotton + Kearney

Australasian Lawyer 2021 5-STAR CYBER LAWYERS

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

Issue 2, August 2022

In this month's wrap-up of relevant news for insurers, brokers and their customers doing business in Australia and New Zealand in the cyber, tech and data, we look at cyber issues, including the treatment of COVID-related data, ransomware developments, insurance premium trends, significant cases, and government and regulatory cyber-related activity in Australia and New Zealand. We also share some tips to help IT providers avoid or minimise liability following cyber incidents.

For more information about any of these stories, please contact a member of our cyber, privacy and data security team.

Contents

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

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

Australia – Cyber

New OAIC Guidance - Retention and deletion of data collected in response to COVID-19

During the pandemic, many organisations have collected information they wouldn't normally have about employees (e.g. COVID-19 vaccine certificates) or about customers or visitors (e.g. contact tracing information).

New guidance issued by the Office of the Australian Information Commissioner (OAIC) suggests organisations may now need to delete that information or risk being in breach of the Australian Privacy Principles (APPs).

The OAIC's guidance does not represent a new legal development; it highlights the ongoing obligations of organisations subject to the APPs. Specifically, under APP 11.2, an APP entity must destroy or de-identify information held about an individual if:

- the entity no longer needs the information for any purpose for which it was collected (for example, if it was collected to comply with public health orders that no longer exist)
- the information is not contained in a Commonwealth record, and
- the entity is not required to keep the information under an Australian law, or by order of a court or tribunal.

Under APP 11.2, APP entities are also required to take reasonable steps to protect personal information they hold from misuse, interference, loss, unauthorised access, modification or disclosure.

While the APPs and these specific obligations apply broadly, COVID-related information provides a clear illustration of the principles. For example, in its guidance, the OAIC recommends that organisations should:

- consider whether there is an ongoing need or legal basis for the continued collection or retention of COVID-related personal and sensitive information – this may require entities to check whether there are still public health orders or other laws in place that provide a basis for the collection or retention of information
- consider whether the information is reasonably necessary for their functions or activities – this may include considering workplace laws and contractual obligations
- if there is no requirement to retain the information, take reasonable steps to destroy or de-identify the information held, and
- if the information is required to be retained for a period of time, ensure that they have systems and processes in place to regularly review whether retention is still necessary.

In practice, different sets of information may need different treatments and ongoing review. Compliance may be complicated by the fact that some organisation-specific or industry-specific public health orders, while no longer strictly required, have not been withdrawn by the issuing agencies.

Organisations' data is often held by service providers under cloud-based arrangements. This means that as part of their 'post COVID' data tidy-up, organisations will need to consider their outsourced arrangements, including terms dealing with data access, storage and deletion, as well as risk allocation provisions.

The OAIC's guidance has not changed 'what good looks like' in this space. The key mitigation for minimising the risk of privacy breach (as called out by the OAIC) and avoiding regulatory scrutiny, as well as minimising the risk and 'blast zone' of data breach and cyber incidents, remains for organisations to regularly review and understand their data storage and retention arrangements.

Ransomware Q2 roundup

According to Coveware's latest report:

- While the average ransom payment increased +8% from Q1 2022 (being pulled up by several outliers), the median ransom payment actually decreased 51% from Q1 2022. Coveware has attributed this downward trend to two factors:
    - a shift of RaaS affiliates and developers towards the mid-market (where the risk to reward profile of attack is more consistent and less risky than high profile attack), and
    - "an encouraging trend among large organizations refusing to consider negotiations when ransomware groups demand impossibly high ransom amounts".
- Exfiltration of data remains prolific (occurring in approximately 86% of ransomware cases), and payment of ransom seldomly results in exfiltrated data being destroyed by threat actors.
- Professional services has emerged as the leading industry impacted by ransomware attacks, which is consistent with the W+K cyber team data.

Cyber insurance premiums continue to rise

According to an *Insurance News* article about a recent S&P report, the global cyber cover premium pool is set to increase 25% a year, reaching $US22.5b ($32.49b) by 2025. However, the S&P report predicts profitability in the insurance line will continue to be a challenge.

According to the report, cyber premium prices will fluctuate going forward due to new risk differentiation models, emerging cybersecurity standards and improvements in cybersecurity systems. S&P further comments: "clear policies with precise wording are key to developing a sustainable cyber insurance market, requiring a deeper understanding of how ransomware drives losses, improvements in scenario modelling, better management of risk accumulation and disciplined underwriting".

Australia joins the Global Cross-Border Privacy Rules Forum

In a joint statement, the Attorney General Mark Dreyfus and Australia's Trade Minister recently announced that Australia has joined the Global Cross-Border Privacy Rules (Global CBPR) Forum. The forum was established in April 2022 with the aim to "support the free flow of data and effective data protection globally" and to "establish an international certification system that will help companies demonstrate compliance with internationally recognised data privacy standards."

TikTok trigger sees Government put strengthening privacy laws back on the table

The Australian Government has again put strengthening Australia's federal privacy laws back on the agenda by recently announcing that privacy laws in Australia should give Australians confidence that their personal information and data is protected, as well as empower them to understand how their data is being used by digital platforms.

Proposed amendments to the *Privacy Act 1988* (Cth) have been part of the Government's ongoing review of the Australian privacy law framework since 2019. This was on the back of the UK parliament declaring the Chinese-owned social media platform TikTok to be a "data harvester" and subsequently deleting its official account in late July 2022. TikTok has recently faced a flurry of negative press after it was disclosed that some of its staff could access data from overseas users, including those in Australia.

The Australian Signals Directorate (Australia's cyber intelligence agency) also advised some Australian MPs that they should (generally speaking) have a second mobile phone for social media apps, in light of the extensive data collection practices undertaken by these apps.

Further, in early August 2022, Internet 2.0 (a Canberra-based cybersecurity and intelligence firm) suggested that TikTok engages in questionable and excessive data practices (such as checking its users' location at least hourly), under broad privacy settings enabled by users. On this basis, Internet 2.0 stressed that TikTok should be more open and transparent about its data practices, and that users should review their privacy settings intermittently. In response, the OAIC is considering Internet 2.0's report as part of its regulatory action policy.

Throughout 2021, the OAIC focused its attention on large organisations' privacy practices and non-compliance with the APPs. Its orders have ranged from the implementation of data destruction and deletion policies, and information security and incident response plans, to the destruction of personal information and ceasation of practices that breach the APPs. These determinations highlight the need for all organisations doing business in Australia – whether based in Australia or not – to comply with the APPs and commit to good privacy practices.

Directors and cybersecurity: where will the RI Advice proceedings take us?

In August 2020, in the first case of its kind, ASIC commenced proceedings against RI Advice Group Pty Ltd (RI Advice) for alleged breaches of its statutory obligations as an Australian financial services licensee for failures surrounding adequacy of its cybersecurity. We reported in more detail on the implications of the RI Advice proceedings in this article.

Following an out-of-court settlement between ASIC and RI Advice, on 5 May 2022, the Federal Court delivered its judgment. It made declarations of contraventions of section 912A(1)(a) and (h) of the *Corporations Act 2001* (Cth) (Corporations Act) and ordered RI Advice to conduct a cybersecurity audit and to pay a contribution of $750,000 towards ASIC's costs. As the judgment relied on the facts agreed between ASIC and RI Advice as part of the settlement, relatively little weight can be placed on the findings. It remains to be seen what cybersecurity standards courts will look to when proceedings like this reach trial.

ASIC released its new Corporate Plan this month which places cybersecurity at the forefront, including intentions to take enforcement action against companies for cybersecurity failings.

The spectre of further regulatory activity by ASIC as it pursues its Corporate Plan, combined with the absence of regulatory or judicial guidance in respect of minimum cybersecurity standards, makes this a challenging area for directors and officers. This is particularly the case when ASIC has shown a propensity in the past to use a company's breach as a 'stepping stone' to establishing personal breaches of care against directors and officers. This uncertainty inevitably creates risk and is an issue insurers and insureds should be alive to so it can be appropriately managed.

> This uncertainty inevitably creates risk and is an issue insurers and insureds should be alive to so it can be appropriately managed.

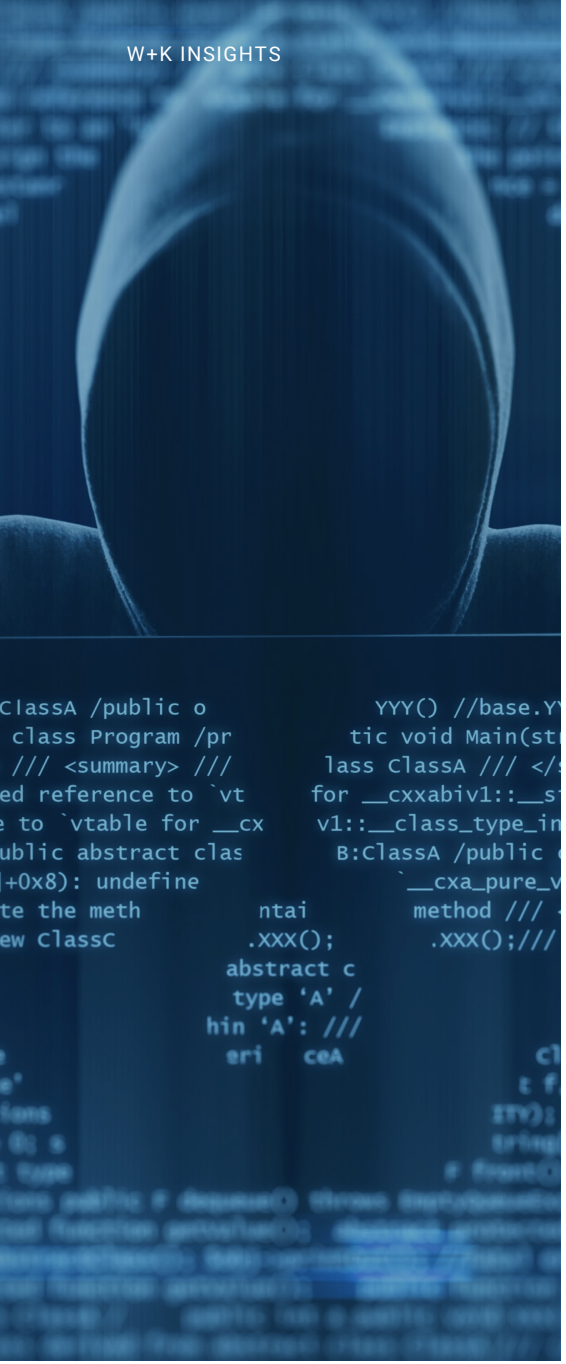
Google $60m penalty decision illustrates heightened risk climate for data collection in Australia

On 12 August 2022, Justice Thawley of the Federal Court of Australia ordered that Google LLC and Google Australia Pty Ltd (Google) pay $60m in damages for misrepresentations about the collection, use and storage of location information gathered from users of android mobile devices[1].

The Google case illustrates the high penalties and alternative means of prosecution available to Australian regulators for inadequate disclosure of data collection and handling practices. It is also evidence of the heightened regulatory and risk environment around data and management of privacy obligations generally.

Read our discussion of the implications of the Google case for organisations that collect data and their insurers here.

[1] *Australian Competition and Consumer Commission v Google LLC & Anor (No. 4)* [2022] FCA 942.



Conti ransomware: is your organisation still a target?

Global ransomware attacks increased 24% in Q2 2022 from Q1 2022, according to Avast's Q2-2022 Threat Report. Conti ransomware has stood centre stage of this development since it launched in the summer of 2020 after replacing the notorious Ryuk ransomware.

Conti was the biggest ransomware strain by revenue in 2021, extracting at least $180m from victims[2]. However, in Q4 2021 and Q1 2022, there was a decrease in Conti ransomware (and global ransomware activity more broadly) after a Ukrainian security researcher leaked over 170,000 internal chat conversations belonging to the gang, along with the source code for the Conti ransomware encryptor. This development coincided with Conti's public announcement that it was siding with Russia over its invasion of Ukraine. Conti officially shut down its operation in May 2022 and took key infrastructure offline, including the Tor admin panels used by members to perform negotiations and publish "news" on their data leak site. Other internal services, such as its rocket chat servers, are being decommissioned.[3]

Experts are now asking whether the recent downfall of the Conti brand signals an end to the malicious double extortion techniques and sophisticated capabilities of Conti actors.

The leaks, which were translated and published by Krebs On Security, provide significant insight into Conti's organisational structure and the rationale behind its choice of victims – and can, in turn, give some insight into how other similar groups may conduct their operations. By extension, insurers and businesses can have a better understanding of how other threat groups work and what they might look for when targeting victims. For insurers specifically, the leaks show that the availability of cyber cover is only one factor when a threat group seeks out a new victim.

The leaked records suggest that Conti sets its ransom demands as a percentage of a victim's annual revenue, based on information found within a victim's systems or on publicly available information. It appears Conti generally relies on open-source intelligence tools, such as Crunchbase Pro and Zoominfo, for this purpose. These subscription service tools provide detailed information on millions of companies, such as how much insurance a company maintains, their latest earnings estimates, and the contact information of executive officers and board members.[4]

It is worth noting that these tools are usually only partially accurate for most companies. More often than not, this inaccuracy means smaller and medium-sized companies can be on the receiving end of ransom demands that far exceed their capacity to pay.

It is evident that groups like Conti are not necessarily fully informed about many of their small and medium-sized ransomware targets before launching their attack, and they may simply be taking a gamble that the targets have the capacity to pay or that there is cyber cover in place.

Conti was particularly known for double extortion, which has been on a steady rise in recent years. Before Conti detonates ransomware within an entity's systems, it will search for and steal critical files, in the hope that the threat of that data being published will elicit a payment from the victim. In some cases, Conti will sift through a potential victim's data using generic search terms to better understand their capacity to pay a ransom demand, as well as determine the sensitivity of files that they can use to put pressure on the target to pay – including, relevantly for cyber insurers, finding copies of the victim's cyber insurance policy.

While Conti operations have now shut down, Advanced Intel's Yelisey Boguslavskiy told BleepingComputer that only the Conti brand has shut down. It appears the syndicate has continued operating, with the group perhaps splitting off into smaller cells or taking over other groups. According to Advisen, former Conti members have now branched off to create new ransomware groups, like Black Basta and Karakurt, or may have joined other existing groups, such as Hive, AvosLocker, BlackCat, Hello Kitty or Quantum. This movement is causing an uptick in activity after what was a short-lived lull.[5]

[2] https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf
[3] https://www.bleepingcomputer.com/news/security/conti-ransomware-shuts-down-operation-rebrands-into-smaller-units
[4] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry
[5] https://www.advisen.com/tools/fpnproc/fpns/articles_new_35/P/442193087.html?rid=442193087&list_id=35

Federal Court decision underscores the need for cyber-specific insurance

While there has been much talk over the years about the potential for 'silent cyber' risks to fall for cover under other policies, Justice Jagot's decision handed down on 1 August 2022 in *Inchcape Australia Limited v Chubb Insurance Australia Limited* [2022] FCCA 883 shows the importance of insureds purchasing cyber-specific cover and not relying on other policies they might hold.

Inchcape was targeted by a ransomware attack that had significant impact, including the encryption of its servers and deletion of its backups. Inchcape did not hold a cyber insurance policy and looked to claim its costs of recovering from the ransomware attack under its Chubb electronic and computer crime insurance policy instead. This, however, was a case of 'fitting a square peg in a round hole', with disagreement about what, if any, costs triggered the crime policy.

While the decision addresses the construction of many aspects of the policy wording, a key issue addressed was whether the costs Inchcape incurred were direct financial losses resulting from damage or destruction of data within the terms of the policy. These are common concepts in fidelity and financial crime policies.

Of particular note, Her Honour found that the terms of the crime policy, when read together, meant any costs that involved the intervening step of Inchcape deciding to incur that cost were not direct enough so as to fall for cover – including the costs of manually processing customer orders or investigating and preventing further effects of the ransomware attack. Rather, Her Honour found that the scope of cover was limited to those costs every insured would necessarily and inevitably incur as a result of damaged data and no more.

Her Honour's findings necessarily turned on the specific policy wording in question. However, the judgment exemplifies the careful approach that can be necessary when analysing the question of causation for individual claimed losses – including the extent to which an insured's own decisions may constitute an intervening cause in each case.

While Inchcape was able to find some cover under its electronic and computer crime policy for its losses, it was left without the other benefits specific cyber insurance can often provide – for example, the help of an insurers' expert panel of vendors and incident responders.

> While there has been much talk over the years about the potential for 'silent cyber' risks to fall for cover under other policies, *Inchape Australia Limited v Chubb Insurance Australia Limited* [2022] FCCA 883 shows the importance of insureds purchasing cyber-specific cover and not relying on other policies they might hold.

Australia – Technology Liability

Ten ways IT professionals can avoid the blame game after a cyber breach

Australia is suffering from a ransomware 'epidemic'. In recent times, there has been a major increase in the frequency of claims, the scale of demands, the size of ransoms paid and the frequency of multi-party incidents. Often, these attacks also involve 'double extortion', as theft of data now accounts for 86% of incidents.

Given the volume of incidents, it's not surprising that IT providers are increasingly being affected by both platform/supply chain and direct attacks.

Platform/supply chain attacks involve threat actors exploiting the software supply chain process, supplier trust and open source vulnerabilities. They achieve large-scale impact with multiple victims through a single initial compromise that creates a snowball effect.

IT providers (in particular managed services providers) are also an attractive target for direct attacks given the potential knock-on impact to their clients and a likely increased motivation to pay the ransom.

These attacks are increasingly leaving IT providers at risk of claims made by clients who are victims of the breach. Claims can arise from allegations of negligence/duty of care, breach of contract or breaches of consumer law, such as misleading/deceptive conduct or consumer guarantees.

To avoid becoming the legal scapegoat following a direct or indirect cyber breach, there are 10 ways IT providers can help protect their positions:

1) Get the contract right
2) Be careful and skilful
3) Document all client conversations
4) Check automated security and retention processes
5) Contact the insurer or broker quickly
6) Don't rely on the limitations of liability clauses
7) Take positive steps to support the client after a breach
8) Take other mitigation steps
9) Say no
10) Plan for the worst

For more detail on the 10 ways IT providers can help protect their positions, read our detailed article here.

> IT providers are an attractive target for direct attacks given the potential knock-on impact to their clients and a likely increased motivation to pay the ransom.

New Zealand

New report highlights the importance of Māori data sovereignty

Māori data sovereignty has been thrown into the spotlight again following a report by Te Kāhui Raraunga, which commented on the acceleration of the New Zealand Government's 'cloud first' policy.

The policy, which was first adopted in 2012, has seen the Government emphasise the adoption of cloud services in the public sector. The new report by Te Kāhui Raraunga, led by Professor Tahu Kukutai, questions the use of these cloud services and asks whether the approach sufficiently accounts for Māori data sovereignty.

One of the unique features of Aotearoa's legal landscape is the obligations under Te Tiriti o Waitangi (the Treaty of Waitangi). One of the principles under Te Tiriti is partnership. It is accepted in law that partnership requires the Crown (and its agencies) and Māori to work together in the governance, design, delivery and monitoring of their various services.

One of the key criticisms in the report is that most agencies are not implementing data initiatives with meaningful engagement with Māori and are instead relying too heavily on cost-benefit analysis. The report suggests that a more considered and integrated approach to data governance and protection is needed.

This could include strategic investment in locally hosted solutions to give effect to Māori data sovereignty and enhance the public sector drive for digital transformation.

The report is yet another important reminder that Māori data sovereignty (which to date has been defined by reference to six high-level principles) is an important part of New Zealand's data and privacy regulatory framework. We expect it to become increasingly integrated with, and relevant to, the country's statutory framework over the coming years.

> One of the key criticisms in the report is that most agencies are not implementing data initiatives with meaningful engagement with Māori and are instead relying too heavily on cost-benefit analysis.

OPC issues consultation paper on use of biometric information

The Office of the Privacy Commissioner (OPC) has issued a consultation paper regarding the use of biometric information, including facial recognition technology, in New Zealand. The paper follows the position paper on biometric information issued by the OPC in October 2021.

The position paper acknowledged the need to consider specific regulatory requirements for biometric information in New Zealand. In this latest consultation paper, the OPC acknowledges the "strong case for further action to ensure that the use of biometrics is subject to appropriate privacy protections".

The OPC is considering options to provide greater clarity around biometrics, including implementing various non-legislative options (such as further guidance and standards on the use of biometrics), issuing a biometrics code of practice under the Privacy Act, or advocating for legislative change. Early indications from the consultation paper are that a draft code of practice of the Privacy Act, if pursued, would be released in 2023. Regardless of which avenue is recommended following the consultation, we anticipate the rules around handling and securing biometric information will tighten in the short to medium-term.

Submissions on the consultation paper are due by Friday, 30 September 2022.

New Privacy Commissioner highlights his priorities

In a recent webinar, Michael Webster, New Zealand's new Privacy Commissioner, set out his priorities in taking on the role. These included the recent reform of the public healthcare sector, the regulation of biometric data, Te Tiriti o Waitangi and Māori co-governance, and compliance and enforcement.

In the webinar, the new Privacy Commissioner highlighted that:

- Mandatory breach notification remains a work in progress – while there had been an uplift in reporting, the Commissioner suspected not all agencies were notifying appropriately and that this issue is something that has to be taken very seriously.
- The healthcare sector may be in line for increased scrutiny – the Commissioner commented on the range of changes taking place in the healthcare sector, including the creation of Health New Zealand and the Māori Health Authority. He pointed out that the OPC's role went beyond mere observation and it plans to be actively involved in promoting privacy within these organisations.
- Privacy is for everyone – the Commissioner wants to see privacy understood and valued at all levels of a business or entity – not just at the top. The OPC intends to increase its focus on leveraging the 'ecosystem' of privacy in New Zealand and resources where it can.

Many of these sentiments mirror those espoused by the previous commissioner. Whether we see a material change in the OPC's focus will become clear in time but, as matters stand, the course seems steady. Agencies should continue to notify privacy breaches in a timely manner and focus on protecting privacy throughout their organisations, not simply making it an issue for the privacy officer or management.

Agencies should continue to notify privacy breaches in a timely manner and focus on protecting privacy throughout their organisations, not simply making it an issue for the privacy officer or management.

Global

AILA Conference – International Keynote address by Patrick Hill, DAC Beachcroft

W+K was pleased to welcome our Legalign Global colleague and DAC Beachcroft's Head of Financial Lines Patrick Hill to Sydney in August.

Patrick gave the W+K sponsored international keynote address at the 2022 Australian Insurance Law Association (AILA) conference in Sydney, providing a Northern Hemisphere perspective on emerging issues facing the financial lines insurance market. The session was opened by Nicole Gabryk, Special Counsel in W+K's Cyber team – pictured below with Patrick.

Our Head of Cyber & Technology Kieran Doyle also took part in a cyber panel session working through the insured and uninsured risks, the first response to an incident and the outcomes in a cyber claim.

Kieran Doyle and Patrick Hill provide a video update on the global issue of the payment of ransomware demands

The payment of ransom after a ransomware attack continues to be a global issue of significant importance. Kieran Doyle (W+K) and Patrick Hill (DAC Beachcroft) provide commentary on some of the issues relevant to the payment of ransom, as well as the different regulatory approaches to the payment of ransomware.

You can watch the update here or below.

Legalign Global insights

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

Cain Jackson
Financial Lines Practice Leader (Melbourne)
T: +61 3 9604 7901
cain.jackson@wottonkearney.com.au

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

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

Ebony Reckless
Associate (Sydney)
T: +61 2 9071 1909
ebony.reckless@wottonkearney.com.au

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

Maxine Betty
Paralegal (Sydney)
T: +61 2 9064 1842
maxine.betty@wottonkearney.com.au

Cecilia Askvik
Cyber Practice Coordinator (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

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
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
AUSTRALASIAN Lawyer