



Sparke Bytes

Latest developments in technology,
privacy, AI, spam and cyber

DEC
2024

QUARTERLY

CONTENTS

03 Introduction

10 Privacy reform: key takeaways for directors

14 What should company directors be doing about Artificial Intelligence: A directors' guide to AI governance

18 The Cyber Security Legislative Package 2024 is finally here: what are the new obligations for businesses?

24 Optus v Robertson - Legal professional privilege: an ongoing consideration

28 What we do

31 Contact card

04 A year in review: reflecting on 2024 privacy reform

12 A year in review: the rapidly evolving AI landscape

16 Spam fines continue to increase

21 Resilience redefined: what businesses can learn from the CrowdStrike outage

26 The health sector as a prime target: snapshot of the last 12 months

30 Our promise to you

If you no longer wish to receive this publication, email sparkehelmorelawyers@sparke.com.au

Copyright 2024 © Sparke Helmore. This publication is not legal advice. It is not intended to be comprehensive. You should seek specific professional advice before acting on the basis of anything in this publication.

INTRODUCTION

Welcome to the inaugural edition of Sparke Bytes, a quarterly publication where we explore the latest legal developments in the rapidly evolving fields of technology, privacy, artificial intelligence (**AI**), spam and cyber. In this issue we look back on a landmark year for privacy reform, keep pace with the latest AI guidance and consultations, analyse trends in spam enforcement, and examine the CrowdStrike outage.

This year has also been significant for Sparke Helmore in the technology and privacy space. We have enhanced our comprehensive Technology, Cyber & Privacy offering by welcoming two new partners, **Hamish Fraser** and **Jason Kwan**, along with their teams. They join our existing partners **Chantal Tipene**, **Alexandra Wedutenko** and **Jehan Meta**.

Our Technology, Cyber & Privacy team has extensive experience in helping clients to navigate the rapidly evolving technology, data protection and privacy sectors. We act for a broad range of corporate and government clients across various industries including the financial services, energy and resources, health, manufacturing and consumer sectors.

We hope you find this publication of interest and if you have topics that you would like to see in our next quarterly update, please don't hesitate to contact one of our team.



A YEAR IN REVIEW: REFLECTING ON 2024 PRIVACY REFORM

Authors: Jason Kwan (Partner), Chantal Tipene (Partner), Stefanie Constance (Associate)



In 2024, Australia has seen significant advancements in privacy reform. This includes the release of a long-awaited first tranche of privacy reforms designed to bolster privacy protections, guidance from the ASX regarding data breach reporting, and OAIC guidance on privacy issues arising from the use of commercial AI.

Background

Privacy Act reform has been on the agenda since 2019 following the Australian Competition and Consumer Commission's (ACCC) 2019 *Digital Platforms Inquiry* final report which made several privacy recommendations to close the gap between the Privacy Act and significant advances in technology (noting the amount of personal information routinely collected and shared online).

In 2022, the Privacy Act Review Report was released. Following extensive public consultation (and 500 written submissions), the Australian Government's response to the Privacy Act Review Report was released on 28 September 2023 (**Government Response**). By the Government Response, the Government agreed to a number of proposed and agreed-in-principle to others (which will require further consultation).

Privacy Amendment Bill

The *Privacy and Other Legislation Amendment Bill 2024 (Bill)* was introduced into Federal Parliament on 12 September 2024. The Bill amends the Privacy Act and related legislation, implementing 23 out of the 25 legislative proposals that the Government 'agreed' to in the Government Response. The focus of these amendments is on enhancing consumer rights, improving data management standards, and strengthening enforcement measures.

Key reforms



Requirement to adopt operational security measures

The Bill clarifies that businesses are required to implement both operational and technical measures to comply with their obligations under APP 11 to protect personal information. Operational measures may include training employees on data protection and developing policies for the security of personal information. Technical controls will require APP entities to critically consider systems which store personal information and assess whether technical controls are appropriate to limit access to personal information to the minimum needed to undertake a specific activity. Technical controls should also include access and action logging and proactive audit controls.



Overseas data sharing 'White List'

A new mechanism allows the Government to prescribe countries that provide comparable privacy protections to the Australian Privacy Principles (**APPs**), facilitating cross-border data sharing and easing compliance for Australian entities who share data overseas as part of doing business.



Transparency in automated decision-making

Privacy policies must disclose any use of automated decision-making that could significantly impact individuals' rights, addressing the growing role of AI in decision-making.



Tort for serious invasion of privacy

The Bill introduced a new statutory tort allowing individuals to sue for serious invasions of privacy, with available remedies including compensation, and injunctions. Key exemptions apply to journalism and law enforcement.



Criminalisation of doxxing

A new offence was introduced that makes it a criminal act to maliciously expose personal data online. This is achieved by amending the *Criminal Code Act 1995* (Cth) to create two new offences. Penalties for these offences can be as severe as up to seven years in prison, particularly when the individual is targeted based on their race, religion, gender orientation and identification, ethnicity, disability or nationality.



Expanded enforcement powers and broader enforcement options

A new tiered approach to civil penalties and infringement notices was introduced, along with enhanced enforcement powers for the Office of the Australian Information Commissioner (**OAIC**). New tools include infringement notices for certain APP breaches and the ability to mandate corrective actions.



Online privacy code for children

The Australian Information Commissioner will develop a dedicated privacy code within 24 months of the Bill taking effect. This code will outline how to better protect children from online privacy risks and how the APPs apply to children's privacy online.

Key exclusions

The Bill does not go as far as many had anticipated (or hoped for) and omits several major reforms 'agreed in principle' in the Government Response. Notably:



Right to delete personal information—There is no formal right for an individual to request an organisation to delete personal data it has collected.



Small business exemption—The exemption from the Act for small businesses, defined as a business with turnover of less than \$3m, also remains intact.



Employee records exemption—Employee records held by organisations (but not agencies) remain largely exempt from the Privacy Act when handled in connection with the employment relationship, pending further consultation.



Fair and reasonable collection of personal information—A proposed obligation for organisations to collect, use and disclose personal information in a 'fair and reasonable' manner is absent from this round of reforms.

Law reform achieved

A significant milestone was reached on 29 November 2024 when the Bill was passed by both Houses of Parliament and is on its way to the Governor-General for royal assent. Once enacted, most changes will take effect immediately, with a 24-month delay for the automated decision-making requirements and a six-month delay for the privacy tort.

Some changes were made to the Bill following recommendations made by the Constitutional Affairs Legislation Committee and the Senate process.

One of those changes gives the OAIC another enforcement power, allowing the OAIC to issue compliance notices compelling entities to address certain privacy breaches before it takes further enforcement action. Compliance with a notice is not a finding (or concession) of having breached an Australian Privacy Principle (APP).

Failure to comply with a compliance notice can result in significant penalties, including fines of up to \$66,000 (200 penalty units) for individuals and \$330,000 (1,000 penalty units) for organisations.

Where to from here?

Looking ahead, the Attorney-General's Department is likely to commence preparing a draft amendment bill for the second tranche of reforms in the coming months.

Organisations should take this opportunity to review existing data collection and handling processes to ensure compliance and to safeguard against future changes and increased regulatory scrutiny. They should also establish a clear data and privacy performance framework to oversee and manage how the organisation uses and handles its data.

For further insights on practical steps APP entities can be taking now to ensure that they are Privacy Act compliant see [Privacy Act reforms :: Sparke Helmore](#)

Notifiable Data Breach Reports

The OAIC has released its Notifiable Data Breaches Reports for January to June 2024, highlighting a significant rise in data breach notifications due to cybercrime, human error, and supply chain vulnerabilities. From July to December 2023, there were 483 reported breaches, marking a 19% increase compared to the previous six months. The sectors most affected included health, finance, insurance, retail, and government sectors.

In the first half of 2024, the OAIC recorded 527 breaches, which is a 29% increase from the previous year and an 9% increase from last six months. The report attributes this trend to persistent cybersecurity incidents, with 38% of breaches arising from cyber events such as phishing, ransomware, and credential compromise.

Human error remains a significant contributor, responsible for 30% of breaches. Common mistakes include misdirected emails and improper use of BCC. Breaches linked to third-party providers exposed vulnerabilities in supply chains and cloud configurations highlighting the need for robust supplier management. The Report also pointed out serious issues with reporting in the Australian Government sector, where many breaches were reported more than 30 days after discovery due to internal delays. This delayed response suggests a need for more efficient incident management and streamlined processes across government entities.

To mitigate these risks, the OAIC recommends several strategies to strengthen access controls, improve monitoring, and enhance response mechanisms. Key measures include securing system access with multi-factor authentication (**MFA**) and strong passwords, as well as providing regular employee training to minimise human error. Additionally, robust third-party risk management is important, including strong vendor agreements and frequent audits of cloud security to prevent potential misconfigurations.

To build effective data protection, the OAIC advises organisations to implement layered security controls to prevent single points of failure, complemented by regular reviews of access permissions to minimise exposure. Furthermore, organisations are encouraged to adopt the Australian Signals Directorate's (**ASD**) Essential Eight baseline practices and additional security frameworks, such as the ASD Information Security Manual, NIST Cybersecurity Framework, or ISO 27001, to bolster cyber resilience. For further assistance, organisations should report incidents to the



Australian Cyber Security Centre for technical support.

The findings highlight the importance of organisations embedding privacy-by-design principles. The strategies recommended by the OAIC provide a pathway for organisations to achieve better compliance, build trust, and enhance data security as Australia's digital landscape becomes increasingly complex.

Digital Platform Services Inquiry

On 21 May 2024, the Australian Competition and Consumer Commission (**ACCC**) released Interim Report No 8 from its ongoing Digital Platform Services Inquiry (**Inquiry**). This Report examines potential competition and consumer issues related to the supply of data products and services by data firms in Australia.

The Report highlights risks associated with data use, privacy, and transparency, citing potential harm stemming from consumers' lack of control over their data and deceptive practices employed by data firms. The ACCC also raises concerns about exclusive data access agreements and mergers that consolidate data control, emphasising the need for stronger consumer protections in the digital landscape.

The Inquiry has released interim reports every six months, examining key factors shaping the digital platform services environment. Its central areas of focus include competition levels, the concentration of market power, entry barriers, and practices that may

impact consumers. Additionally, the Inquiry tracks changes in service offerings and monitors international trends that could affect the Australian market.

The ACCC is scheduled to deliver a final report to the Treasurer by 31 March 2025, with the aim of informing future regulatory responses in the digital sector.

ASX Guidance on managing and disclosing cyber incidents

In response to industry demand for guidance, and following several high-profile cyber incidents, the Australian Securities Exchange (**ASX**) updated Guidance Note 8 on 27 May 2024.

This update is designed to assist boards in managing disclosure obligations during cyber incidents. The guidance advises directors to ensure their disclosures are clear and comprehensive, to avoid using boilerplate language, and to prepare draft announcements as incidents unfold. The ASX also cautions against using trading halts as a workaround for continuous disclosure requirements and emphasises the importance of maintaining confidentiality for as long as possible.

These developments reflect Australia's growing commitment to robust data protection and outline a path for organisations to effectively manage privacy risks effectively in an era increasingly defined by data and innovation.



PRIVACY REFORM: KEY TAKEAWAYS FOR DIRECTORS

Author: Jason Kwan (Partner)

Advances in technology have made it easier for organisations to collect large volumes of data (including personal information) and to extract insights and value from that data. However, there is a growing responsibility on directors and boards to ensure that their organisations do so in a regulatory compliant manner and with appropriate governance oversight.

To discharge their duty of care and diligence directors need to be aware of key areas of regulation that apply to the company, its operations and key risks. This was highlighted in a recent Practice Statement by the Australian Institute of Company Directors (AICD).[1] Those regulations no doubt extend to privacy laws.

This article highlights some of the key changes included in the Privacy and Other Legislation Amendment Bill 2024 (the **Bill**) that was recently passed by both Houses of Parliament and that is before the Governor-General for royal assent, and the implications for directors.



Relevant privacy reforms

While recent changes proposed by the Bill may have fallen short of implementing many of the changes proposed by the Privacy Act Review Report, they still highlight the need for directors to take an increasing role in monitoring and ensuring a company's compliance with privacy laws. In particular:



Adopt operational measures

Businesses must take **operational** as well as technical measures to comply with their obligations to: (1) take reasonable steps to protect personal information it holds from misuse, loss and unauthorised access (APP 11.1); and (2) to destroy or de-identify information it no longer needs (APP 11.2).

Examples of operational measures include training employees on data protection and developing standard operating procedures and policies for security personal information.

The proposed amendment makes it clear that ensuring privacy compliance is not only IT's responsibility, but a broader responsibility of an organisation, and one that needs to be embedded into an organisation's structures and governance.



Broader enforcement options

The Bill introduces a new tiered approach to civil penalties and infringement notices. This includes new tiers and civil penalties for interferences with privacy not deemed 'serious' and for certain breaches of a more administrative nature.

The aim of the amendments is to address the gap where the Australian Information Commissioner can only seek civil penalties for the most serious or egregious interferences with privacy. It represents a material broadening of the scope of conduct captured by the civil penalty provisions and foreshadows and increased focus by regulators on enforcing privacy compliance.

These amendments all point to an increased regulator focus on privacy compliance and an enhanced ability and willingness to enforce such compliance. They are also just the initial tranche of reforms, with further changes foreshadowed in the Privacy Act Review Report, including those relating to maximum data retention periods for holding personal information; tighter requirements for notifying data breaches; and the requirement to appoint a senior employee with responsibility for privacy, yet to make their way into this tranche of reforms.



Expanded enforcement and review powers

The introduction of a range of new enforcement powers, including enhanced powers for the OAIC in relation to investigations into breaches of civil penalty provisions and expanded powers for the Federal Court of Australia (**FCA**) and Federal Circuit and Family Court of Australia (**FCFCOA**) to make a range of additional orders (e.g. for compensation).

The aim of the amendments is to ensure the OAIC has a robust regulatory framework to monitor compliance and enforcement protections in the *Privacy Act 1988* (Cth) and to give greater flexibility to the FCA and FCFCOA to make other appropriate orders, including orders to take steps to minimise further impacts to individuals impacted by the interference with privacy.

Key takeaways

With further reforms likely, directors should take the opportunity to ensure that their organisation's leadership and governance arrangements create a culture and operating environment that values and safeguards personal information. Practically, this may mean:

- revisiting existing **data collection and handling processes** to ensure compliance and to safeguard against future changes and increased regulatory scrutiny
- having in place a clear data and privacy **performance framework** to allow the board to exercise oversight and control over how the organisation uses and manages its data. This includes ensuring that the board is regularly briefed on the risks associated with the handling of data, in particular personal information
- appointing **key personnel responsible for oversight** of privacy (e.g. a privacy officer) and ensuring that they report into the Board, and
- **reviewing technical and organisational measures** currently in place to protect personal information that the organisation holds.

¹ Australian Institute of Company Directors, AICD Practice Statement: Director's oversight of company compliance obligations (October 2024).

A YEAR IN REVIEW: THE RAPIDLY EVOLVING AI LANDSCAPE

Authors: Jason Kwan (Partner) and Zach Smale (Associate)

Introduction

In 2024, the landscape of AI regulation is rapidly evolving as governments strive to keep pace with the swift advancements in the development and deployment of AI. The comments from the UK Government on AI regulation illustrate the challenge posed.

"...a recurring theme in the discourse on...AI risk is the mismatch between the pace of technological innovation and the development of governance structures...it is very difficult to fill such gaps...because by the time a regulatory fix is implemented it might already be outdated..."

Across the globe, regulatory initiatives are being rolled out to address key issues. Many of these initiatives aim to ensure transparency, accountability, and fairness in AI systems. At the same time, there is an increased emphasis on safeguarding privacy, preventing bias, and mitigating the negative societal impacts of automation. These developments reflect the complex balance that regulators must strike between promoting innovation and protecting public welfare in an era of unprecedented technological advancement.

Voluntary AI Safety Standard and Mandatory Guardrails

On 5 September 2024, the Department of Industry, Science and Resources (**DISR**) released a consultation paper on the introduction of mandatory guardrails, which would apply to developers and deployers of AI in high-risk settings. The push for regulation is driven by the potential harms associated with AI, including the risk of embedding human biases and amplifying algorithmic biases, as well as concerns about privacy breaches and potential IT vulnerabilities.

DISR emphasises specific risks arising from the use of general-purpose AI (**GPAI**) models such as GPT-n and DALL-E. These risks include undermining key

democratic values by generating and distributing misinformation, creating polarisation, and facilitating deception.

Whether AI is deemed high-risk will likely depend on factors such as the risk of adverse impacts to an individual's human rights, as well as physical and mental health or safety concerns for individuals or cultural groups.

The proposal outlines a set of ten mandatory guardrails that would apply to high-risk AI. These guardrails cover areas such as the establishment of governance and risk management frameworks, the testing and continual monitoring of AI models, ensuring human oversight of AI systems, and maintaining transparency with end users and organisations throughout the supply chain regarding the use of AI.

The proposed guardrails closely align with the Voluntary AI Safety Standards also released by DISR on 5 September 2024, which provide practical guidance for Australian organisations to develop and deploy AI safely and responsibly.

DISR is contemplating several regulatory options to mandate the guardrails that would apply to high-risk AI, including:



A domain specific approach—adapting existing regulatory frameworks to include the guardrails.



A framework approach—introducing framework legislation that will require other existing laws to be amended to the framework legislation to have effect.



A whole of economy approach—introducing a new cross-economy AI Act.

Approaches to AI regulation in the EU

The EU AI Act (**AI Act**) officially came into force on 1 August 2024, with many of its provisions progressively coming into effect. The AI Act takes a risk-based approach to regulating AI technologies. It prohibits certain categories of AI, including social credit scoring, emotion recognition systems used in the workplace and educational settings, untargeted scraping of facial images for facial recognition and biometric categorisation systems using sensitive characteristics.

While 'high-risk AI' is permitted, it will be subject to strict obligations before it can be put on the market. These obligations include the requirement for extensive technical documentation, clear instructions for use, and robust cybersecurity measures.

'Limited risk AI' is required to adhere to transparency obligations, ensuring that individuals are informed of its use, such as when they interact with AI systems like chatbots. Conversely, 'minimal-risk AI' (for example, AI-enabled video games) will remain unregulated to encourage market efficiency.

OAIC AI Privacy Guidance

The OAIC has provided valuable guidance for developers and deployers on how to address privacy risks when developing or training AI models, as well as when using commercially available AI products (respectively).

While incorporating customer data in an AI model may offer commercial benefits (such as for marketing purposes), it is essential for deployers of AI products to remember that privacy obligations apply to any personal information input into an AI system or any AI-generated outputs that contain personal information. This means that the use and disclosure of personal information (whether automated or not) should align with the primary purpose for which it is collected. If this is not the case, individuals must have provided consent or it must be shown that the secondary use would be reasonably expected by the individual. As a best practice, the OAIC recommends that organisations do not enter personal information—especially sensitive information like health or biometric information—into publicly available generative AI tools.

Similar considerations apply to organisations using personal data to train AI models. Developers must ensure they use accurate data sets for training

exercise caution when incorporating personal information to train AI models. Again, this means considering whether using personal information to train AI constitutes a primary purpose for which it was collected and if not, whether consent is required or a secondary purpose can be established. Additionally, developers should design AI systems to prevent the inadvertent disclosure of personal information, particularly in response to user prompts.

Consultation on Consumer Law and AI

The Australian Consumer Law (**ACL**) provides protections for both individual consumers and small businesses. This includes guarantees regarding the minimum quality of goods and services, which are designed to protect consumers and small businesses from unfair contract terms and providing recourse against manufacturers for safety defects.

In October 2004 the Australian Government issued a discussion paper seeking feedback on whether the existing ACL framework can effectively address the unique risks posed by AI, or if new consumer guarantees for example should be introduced.

One particular risk highlighted in the paper is the potential for AI to produce false or misleading representations. For instance, defects in AI products such as chatbots may lead to customers being misinformed about cancellation policies.

The paper further explores whether the current remedies for breaches of the ACL are suitable for consumers of AI-enabled goods and services, as well as whether they appropriately apportion liability between manufacturers and suppliers.

Closing thoughts

AI regulation in Australia is still in its early stages, as there is currently no comprehensive legal framework governing the development and use of AI. However, this situation is quickly changing with the emergence of industry guidance and consultations focused on the specific regulation of AI. Many businesses are understandably eager to leverage AI or to collaborate with third parties that use AI to remain competitive in their industries. As they do this, organisations must stay updated on this rapidly evolving landscape.

WHAT SHOULD COMPANY DIRECTORS BE DOING ABOUT ARTIFICIAL INTELLIGENCE: A DIRECTORS' GUIDE TO AI GOVERNANCE

Author: Hamish Fraser (Partner)

Artificial Intelligence (**AI**) is everywhere. From workplace desktops and email filters, to search engines and tools for drafting to the social media at home, AI has become integral to our daily lives. It powers facial recognition on smart phones, facilitates access to bank accounts, and enables banks to analyse spending patterns to detect fraud.

With AI becoming increasingly pervasive, boards must understand not only how to leverage AI for their business, but also how to implement appropriate safeguards to ensure its safe and responsible use.

It is well understood that directors have common law and statutory duties to their company. These include:

- Acting with the degree of due care and diligence in exercising their powers and carrying out their functions as a director, that a reasonable person would exercise.
- Exercising and discharging their duties in good faith, in the best interests of the company, and for a proper purpose.

Fulfilling these duties is an evolving challenge, as is the lens in respect of which they are to be interpreted. The rapid uptake of AI means it must now be on the agenda for every board.

Helpfully, the Australian Institute of Company Directors (**AICD**), in partnership with the Human Technology Institute at the University of Technology Sydney has published a suite of resources to help boards navigate the ethical and informed use of AI.

The suite comprises three key parts.

1

A Director's Introduction to AI—This guide helps directors understand key AI concepts, risks and obligations. The introduction contains three chapters:

1. An introduction to what AI is, how it's used and its relevance for directors.
2. Opportunities and risks of using AI.
3. An examination of the regulatory obligations in Australia and overseas relating to AI systems.

2

A Director's Guide to AI Governance—

This practical guide helps directors, particularly those in ASX300 entities, navigate the integration and deployment of AI within their organisation. It is recognised that AI is fast moving and the guide offers a framework for board oversight of the use of AI. The guide contains two sections:

1. Insights and implications related to AI governance for directors.
2. Elements of effective, safe and responsible AI governance – offering questions and tools to drill deeper, including case studies.

3

A governance checklist for SME and NFP directors—This checklist outlines

recommended steps for AI governance, tailored to smaller businesses and not-for-profit entities.

Summary of recommendations

The AICD guide provides a valuable starting point for boards uncertain about how to approach AI governance. No tool can serve as a one-size-fits-all solution, especially in such a rapidly evolving landscape as AI—consider that Chat GPT, the generative AI tool that changed the game, was only released by OpenAI in November 2022.

As mentioned, AI should be on the agenda of every board in Australia. This tool provides a helpful resource but also gives boards a reference point from which to begin their journey into using and managing AI.

Perhaps the best way to digest this beneficial resource is to briefly examine the eight elements of safe and responsible AI governance.

Practical steps for directors	
Roles and responsibilities	<ul style="list-style-type: none"> Consider whether decision-making processes incorporate consideration of AI risk and opportunity. Identify and document the businesses AI in use and those involved in AI system procurement, development and use across the business. Determine (and document) who at board and management level has responsibility (and is accountable for) AI use.
Governance structures	<ul style="list-style-type: none"> Determining whether existing or a new governance structure (board and management) would most appropriately support AI oversight. Reviewing board and management committee charters to determine whether and how they incorporate AI issues. Considering how external experts can be leveraged within existing governance structures. Consider the nature and frequency of management reporting to the board.
People, skills & culture	<ul style="list-style-type: none"> Confirm that management has assessed the skills required and invest in any training required. Consider the impact of AI on the workforce including future needs and skills development.
Principles, policies & strategy	<ul style="list-style-type: none"> Ensure AI is considered and, where appropriate, embedded, within the organisation's strategy. Avoid 'AI for AI's sake'. Adopt an AI use policy to ensure safe and responsible AI principles (refer the Australia's AI Ethics Principles) have been incorporated into relevant policies (such as privacy, governance, cyber security and procurement). A process to ensure policies are implemented and enforced (including across the supply chain).
Practices, processes & controls	<ul style="list-style-type: none"> A clear risk appetite statement and risk management framework. AI impact assessment capability and compliance process.
Supporting infrastructure	<ul style="list-style-type: none"> AI system and data inventory – where do we use AI and where and what data does it use. The data governance framework is in place and updated to account for AI used.
Stakeholder engagement & impact assessment	<ul style="list-style-type: none"> Ensure stakeholders understand AI's impact and that their expectations are managed accordingly. Ensure all appropriate accessibility and inclusion practices are properly managed. Are AI outcomes managed and appealing.
Monitoring, reporting & evaluation	<ul style="list-style-type: none"> Is a risk-based monitoring and reporting system in place for mission-critical and/or high-risk AI systems. Develop and implement a monitoring and reporting framework. Considering seeking internal and external assurance.

Key takeaway

The AI Governance Guidance is not meant to be comprehensive, but rather aims to provide boards with foundational knowledge of AI and a suggested framework for oversight of its use.

SPAM FINES CONTINUE TO INCREASE

Author: Hamish Fraser (Partner)

In 2020, the Australian Communications and Media Authority (**ACMA**) stepped up its enforcement of spam-related offences by issuing significant penalties to companies for breaches of the *Spam Act 2003* (Cth) (the **Act**). The Act aims to combat unauthorised marketing practices, which include sending of commercial electronic messages via email, SMS, multimedia message service, or instant messaging.

Since the ACMA began its increased enforcement actions, there has been a noticeable uptick in penalties issued. For example, Australian online retailer Kogan was fined \$310,800 in 2021, while Latitude Finance faced a penalty of nearly \$1.55 million in 2022. Enforceable undertakings accepted by the ACMA can be viewed on their [website](#).

The largest enforcement to date involved the Commonwealth Bank of Australia (**CBA**), which agreed to pay a \$7.5 million penalty for breach of the Act. The ACMA [found](#) that CBA had sent over 170 million marketing messages without a way to unsubscribe. Among these messages, more than 34 million emails were sent without having obtained the necessary consent.

Although these numbers may seem excessive and not directly impactful to most businesses, the growing accessibility of large datasets means that any business could face significant spam-related risks of this magnitude.

It is clear that the ACMA's enforcement strategy primarily focuses on two key issues: ensuring that consent is obtained and providing a functional unsubscribe option.

Why are we here?

Australia has had laws relating to spam since 2003. Until recently, the focus of the ACMA has been on compliance rather than strict enforcement. However, since 2022, the ACMA has included spam on its list of [enforcement priorities](#), particularly emphasising the unsubscribe rules. In 2019, the focus was more about obtaining consent.

When the ACMA investigates a potential regulatory breach, it has the authority to take regulatory action if a violation is confirmed. In determining whether a compliance breach has occurred, the ACMA considers a number of factors including but not limited to:

whether the conduct was deliberate, inadvertent, or reckless

whether it caused or may cause detriment to another person

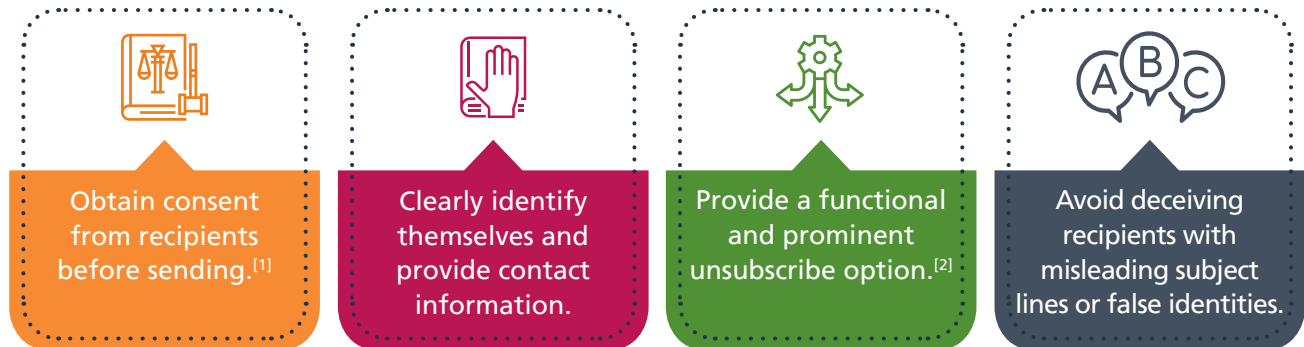
the nature, severity, and extent of the detriment

whether the person has prior compliance or enforcement action and the outcome of that action, and

whether the conduct indicated systemic issues that could pose ongoing compliance or enforcement issues.

What does the law say?

In summary, the Act aims to protect consumers from unwanted commercial electronic messages. Businesses that fail to comply with the Act can face significant fines enforced by the ACMA. The Act requires businesses to:



It is worth noting that if even one part of a message is intended to advertise or promote goods or services, it is likely to be considered a commercial electronic message. For example, in October 2023 a banner advertisement on event tickets sold by Ticketek led to the company facing scrutiny under spam regulations.

What you should do

If you are using any form of commercial electronic marketing to communicate with customers that includes advertising, follow this checklist of essential steps to comply with the Act:

- ✓ Ensure there is a functioning unsubscribe option that allows recipients to easily opt out from future communications.
- ✓ Keep a record of the consent received, which can be express (directly given) or inferred (based on existing relationships) and note how it was obtained.
- ✓ Include the necessary information to accurately identify the sender.

[1] The general rule for e-marketing, consent should be obtained before a message can be sent, including to a business that can be either inferred or express consent.

[2] The unsubscribe option should present clear instructions on how to opt-out of receiving messages, take effect within 5 working days, continue to function at least 30 days after sending the message, does not require the person to provide extra personal information or require a log in to an account to unsubscribe.

THE CYBER SECURITY LEGISLATIVE PACKAGE 2024 IS FINALLY HERE: WHAT ARE THE NEW OBLIGATIONS FOR BUSINESSES?

Authors: Hamish Fraser (Partner) and Jasmine Thai (Graduate)

The long-awaited Cyber Security Legislation Package has finally been passed. The Albanese Government passed the package just a week after the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) presented its advisory report. Senator Raff Ciccone, Chair of the PJCIS, remarked, "The Committee recognises that hardening Australia's cyber resilience and implementing the **2023–2023 Australian Cyber Security Strategy** is an urgent priority of the Government and this Parliament."



Background

The Federal Government set the ambitious goal for Australia to become 'a world leader in cyber security by 2030.' (See the [2023-2030 Australian Cyber Security Strategy](#))

On 9 October 2024, the Cyber Security Legislative Package was passed to the PJCIS for inquiry and report. The focus of this inquiry was to address risks associated with smart devices and the Internet of Things (**IoT**) compulsory ransomware notifications. An [Advisory Report](#) was published on 18 November 2024 with 13 recommendations from the PJCIS.

The package introduces three (3) Acts:

1	Cyber Security Act 2024 (the Act)
2	Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024
3	Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024

With the passage of the three Acts, new obligations are established for businesses, and the Government has stronger enforcement powers. Here's what businesses need to know to prepare for the new legislation.

1

Cyber Security Act 2024*Smart Devices Standard*

The Act grants the relevant Minister the authority to mandate security standards for devices defined in the Act as 'relevant connectable products.' These products include IoT devices such as smart TVs, smart watches, home assistants, and baby monitors. Manufacturers and suppliers of these 'relevant connectable products' will need to ensure their products meet the requirements that will be set out in the Standard and must provide a statement of compliance.

While the specific obligations in the Standard are yet to be determined, there is a clear move from Government to ease the burden on industries trading internationally and to align with international standards, such as the United Kingdom (UK).

Ransomware Payment Notification

New requirements will now mandate that businesses must report ransomware payments or benefits provided in response to a cybersecurity incident. A report must be submitted within 72 hours of any payment or benefit being given to the extorting entity. This reporting obligation also applies in circumstances where the reporting entity becomes aware that a related entity has made a similar payment. Affected businesses include owners of critical infrastructure asset and any non-government entity carrying on business in Australia with an annual turnover exceeding \$3 million, which aligns with the threshold set out in Privacy Act 1988.

The revised Explanatory Memorandum provides that a transition period of six months will be provided before enforcement will take effect. Businesses should ensure that they have the appropriate procedures and measures in place to ensure compliance with the new reporting obligations as failure to comply will result in 60 penalty units, which currently equates to \$19,800.

Cyber Incident Review Board

A new Cyber Incident Review Board (**CIRB**) will be established to conduct reviews following significant cyber security incidents. Businesses can be assured that these reviews will be conducted on a no-fault basis. The Board will have limited powers to gather information, only compelling organisations to respond if a voluntary request for information has not been successful.

'Limited Use' Obligations

Information shared to the National Cyber Security Coordinator (**NCSC**) regarding a cyber security incident will be protected and used solely for permitted cybersecurity purposes. While this information can be shared to other government agencies, however, it may only be used for the specific reason for which it was shared. Additionally, it is not admissible in regulatory proceedings and may not be used to initiate enforcement actions.

However, businesses should be aware that this arrangement does not provide a 'safe harbour' from legal liability. Law enforcement and regulatory bodies retain the authority to utilise their existing powers to gather information and conduct their own investigations.

2

Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024

The *Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024* amends the Intelligence Services Act 2001. It introduces a 'limited use' obligation for information that is voluntarily provided to the Australian Signals Directorate during a cybersecurity incident. This obligation mimics the 'limited use' obligation mentioned above when information is voluntarily shared with the NCSC.

3

Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024*Changes to the definition of asset*

The definition of 'asset' has been expanded to include 'business critical data' and will also extend to the definition of 'material risks.' Businesses will need to ensure that their data storage systems, which contain this business-critical data are protected from threat actors.

New all-hazards power

New legislation has been introduced to grant management powers for significant incidents. These powers are authorised by the Minister and can only be enforced as a last resort. Under this authority, the Minister can direct critical infrastructure entities regarding a cybersecurity incident, authorise the

disclosure of protected information, and gather information for consequence management in response to multi asset incidents. This information can be shared with other sectors of the economy, such as banks, to mitigate the flow on consequences of the cyber incident.

Stronger enforcement powers

Under the SOCI Act, regulators currently lack the authority to direct a responsible entity to address serious deficiencies in their Critical Infrastructure Risk Management Program (**CIRMP**). Responsible entities are required to develop and implement a CIRMP to ensure robust protections for their critical infrastructure assets. Recent changes have introduced stronger enforcement powers, allowing regulators to direct a responsible entity to rectify seriously deficiencies in their CIRMP.

Consolidation of Telecommunications Act 1997 into SOCI Act

Under the new reforms, existing obligations under Part 14 of the *Telecommunications Act 1997* will be consolidated into the SOCI Act. The purpose of this reform is to streamline the obligations for telecommunication carriers and carriage service providers. The enhanced security regulations for critical telecommunications assets include:

- A 'protect your asset' obligation, requiring all providers to safeguard their assets from all hazards, as far as it is reasonably practicable.
- A notification obligation that mandates responsible entities to notify relevant parties of certain changes and proposed changes to their service or system.
- Authority to implement a Telecommunications Security and Risk Management Program (**TSRMP**).

Closing thoughts

Businesses must review and update their security policies and frameworks to comply with the new obligations, including reporting requirements for ransomware payments, to enhance resilience against cyber security risks and threat actors.



RESILIENCE REDEFINED: WHAT BUSINESSES CAN LEARN FROM THE CROWDSTRIKE OUTAGE

Authors: Jason Kwan (Partner) and Stefanie Constance (Associate)

On 19 July 2024, a software update from the global cybersecurity provider CrowdStrike triggered an unprecedented global IT outage, severely disrupting businesses worldwide. In Australia, where the incident occurred during the workday, financial losses were estimated to exceed A\$1 billion.

Organisations faced operational paralysis as their systems crashed, forcing them to scramble to manage lost sales, restore operations, and address reputational damage. As recovery efforts were initiated, the incident sparked broader discussions around technology governance, vendor risk management, and digital resilience frameworks.

Key facts and figures

Date of Incident	19 July 2024.
Financial impact in Australia	Estimated at over A\$1 billion
Devices affected globally	Approximately A\$8.5 million
Cause	Bug in a software update.
Immediate effects	System failures, business interruptions, increased cyber risks (for example, phishing and fraud attempts).

The CrowdStrike outage underscored the vulnerabilities of interconnected IT systems and the risks businesses face when they heavily depend on third-party vendors. As organisations dealt with the immediate repercussions, including disruptions to core operations and customer-facing services, the extent of the damage was amplified by the sheer scale of the incident. Financial losses, estimated to be in the billions globally, exposed significant weaknesses in how businesses manage vendor relationships and highlighted the role of insurance in mitigating risk. For many organisations, this incident has prompted a re-evaluation of their procurement strategies and the adequacy of their existing legal and operational safeguards.



Insurance arrangements have come under scrutiny as businesses evaluated whether traditional business interruption or cyber insurance policies would cover the losses incurred. While business interruption insurance typically covers physical damage, cyber policies may offer coverage for outages resulting in non-physical damage, such as those caused by software errors. However, many organisations are now discovering gaps in their policies that leave them financially exposed. This situation has prompted renewed attention to the scope and limitations of cyber insurance and emphasised the importance of timely notification to insurers after such incidents.

A critical issue for businesses highlighted by the recent outage is their reliance on IT vendors and the contractual terms agreed to with those vendors. Vendors like CrowdStrike often limit their liability to a refund of fees paid and exclude recovery for consequential loss, such as lost revenue or loss arising from business interruption. While larger organisations with greater bargaining power may negotiate more favourable terms, smaller businesses often lack this ability. For small businesses, statutory protections—such as those provided under Australian Consumer Law—offer essential safeguards. These protections include guarantees that services must be delivered with due care and skill, which can help small businesses seek recourse for losses caused by vendor failures.

The recent outage has raised broader concerns about regulatory oversight of the IT industry in Australia. While general laws, such as the *Privacy Act* 1988 (Cth) and consumer protection regulations, apply to IT vendors, the absence of a dedicated regulatory framework has drawn criticism, particularly given the scale of disruption caused by the outage. By comparison, organisations in the financial services sector regulated by the Australian Prudential Regulation Authority (**APRA**) and must comply with additional frameworks such as APRA Prudential Standard CPS 230 (Operational Risk Management). This Standard requires APRA regulated entities to take additional measures to identify, assess and manage operational risks, including those associated with their service providers.

Regulators will likely prioritise addressing vulnerabilities linked to an over-reliance on service providers, inadequate software development practices, and limited disruption tolerance, all of which have been identified as major risks in the wake of the outage.



Key takeaways for organisations

The CrowdStrike outage provides valuable lessons for businesses seeking to safeguard against similar incidents in the future. Businesses should focus on key strategic areas to help strengthen resilience and ensure operational stability, such as:

- **Reassess IT vendor contracts**—Evaluate existing and new agreements to consider whether there is scope to push for more favourable liability positions, including whether the likely types of loss likely to be incurred in the event of an outage are recoverable.
- **Strengthen technology governance**—Adopt rigorous software testing, phased rollouts, and redundancy measures to mitigate operational disruptions caused by updates or outages.
- **Enhance digital resilience**—Refine incident response, business continuity, and disaster recovery plans to ensure preparedness for future IT outages.
- **Review insurance coverage**—Assess whether cyber insurance policies permit recovery for non-physical damage caused by business interruption and notify insurers promptly to preserve claims.
- **Monitor regulatory developments**—Stay informed about evolving standards and frameworks for operational resilience and third-party vendor management to ensure compliance and best practices.

The outage has sparked a deeper conversation about technology governance and operational resilience, extending beyond the immediate recovery concerns. The rapid pace of software updates, often prioritised to tackle evolving cyber threats or reduce costs, raises important questions about the adequacy of current testing and deployment practices.

For businesses, the message is clear: sound technology governance, coupled with robust incident response and disaster recovery plans, is crucial for minimising the operational impact of IT outages. By addressing these issues, businesses can bolster their digital resilience and better navigate the complexities of the modern digital landscape.



OPTUS V ROBERTSON – LEGAL PROFESSIONAL PRIVILEGE: AN ONGOING CONSIDERATION

Authors: Jehan Mata (Partner), Georgie Aidonopoulos (Lawyer), Shane Hashemi (Paralegal)

Legal Professional Privilege (**LPP**) has been a longstanding principle that protects confidential documents or communications between solicitors and clients. LPP extends to documents created for the primary purpose of giving advice or for current or anticipated proceedings (the **Dominant Purpose Test**). This privilege not only acts as an additional layer of protection for documents and correspondence but also maintains the trust and confidence clients have in their lawyers.

However the certainty surrounding LPP has come under scrutiny in recent times. With the unprecedented surge of cybersecurity threats looming over organisations day every day, it is essential to consider the legal implications of these threats on the protection of sensitive information. The recent case of *Optus v Robertson* [2024] FCAFC 58 highlights situations in which LPP may not apply to certain documents following a cyber breach.

The Decision

Optus v Robertson discusses the challenges faced by organisations that claim LPP over internal investigation reports, particularly when those reports could serve multiple purposes. In September 2022, Optus suffered a wide-scale data breach affecting 10 million customers. In response, Optus announced in a media release the following month that they were conducting an “independent external review of the recent cyber-attack and its security systems, controls and processes” with Deloitte (the **Deloitte Report**).

The report aimed to analyse and review the circumstances and root causes leading to the cyber incident, evaluate the appropriateness of the steps taken by Optus in response to the cyber incident, and to assess their cyber risk response policies and practices generally. Soon after this announcement, a class action proceeding was brought against Optus on behalf of individuals whose personal information was compromised during the breach. The class action group requested access to the Deloitte Report but Optus refused on the grounds that it was protected under LPP.

Justice Beech held that the report did not attract the protection of LPP because it did not satisfy the Dominant Purpose Test. His Honour based his decision, inter alia, on the following:

- The report was also created for other non-legal purposes, including identifying the circumstances and causes of the cyber incident for management purposes, as well as for reviewing Optus’s cyber risk management policies and practices.
- In the organisations media release, no specific purpose for creating the report was mentioned, including whether it was intended for legal purposes.
- At the time the report was commissioned, the purpose in the mind of Optus’s CEO was not a predominantly a legal one.
- Optus’s general counsel was also serving concurrently as the company’s secretary, which impacted the clarity of the report’s purpose.

Key takeaways

We consider this decision is very important, and there are four fundamental takeaways that companies and legal practitioners should keep in mind:

- **Don't blur the lines.** It is imperative to ensure that any documents produced or provided during a cyber incident are distinctly separated and used solely for the purposes of legal advice. As highlighted by the Optus decision, a report that serves multiple functions is unlikely to be protected by LPP. Even if a document can be used for other purposes, it must be clearly specified as being produced dominantly for providing legal advice. If a company wants to learn from a cyber incident and improve its current policies and systems, a separate investigation report should be produced, solely focused on the company's operations.
- **Differentiate between in-house and external.** Any documents or correspondence from an in-house counsel may present challenges in attracting LPP due to the dual role of serving as both a legal and business advisor. Consequently, it may be difficult to ascertain the dominant purpose for certain documents. When a company experiences a cyber incident, a more prudent approach would be to engage external lawyers to conduct the investigation and to report directly to executives. This approach clarifies the dominant purpose of any document created.
- **Increase awareness internally.** Given the anticipated rise in cyber incidents, companies should invest in educating their representatives about LPP, including what documents or correspondence it applies to. This understanding is particularly vital for employees who represent the organisation in media relations. By fostering awareness, companies can underscore the significance of LPP and reduce the risk of inadvertently waiving any applicable privilege.
- **Beware of the media.** Organisations must be cautious of their interactions with the media. Speaking too much about the purpose and findings of a report may undermine a claim for LPP or lead to inadvertent waiver of privilege. For the case of Optus, the CEO's statements to the media regarding the investigation report's purpose were a key consideration for the Court's ruling against them. To mitigate the risk of inadvertent waiver, it is essential to have legal and public relations oversight before any public statements are made.



THE HEALTH SECTOR AS A PRIME TARGET: SNAPSHOT OF THE LAST 12 MONTHS

Authors: Jehan Mata (Partner), Georgie Aidonopoulos (Lawyer)

The past 12 months have revealed a troubling trend in the health sector, as this industry continues to be one of the most frequent victims of cyber-attacks. The Office of the Australian Information Commissioner's (**OAIC**) reported that between January to June 2024, the health sector experienced 102 breaches, more than any other sector. Additionally, 66% of these breaches were caused by malicious or criminal attacks. To make matters more complicated, cyber-attacks on the health sector have steadily increased over the past few years, and we anticipate this trend will continue. For example, in the reporting period from January to June 2023, health service providers reported a total of 63 breaches or 15% of all notifications to the OAIC. In the July to December 2023 period, the health sector reporting 104 breaches, or 22% of all notifications to the OAIC. This data reinforces that the health sector remains a prime target for malicious or criminal attacks due to the sensitive and confidential information it holds.

Some of the notable cyber-events in the past 12 months include attacks on medical centres where medical records and patient data were extracted, medical practitioners' contact information was leaked, and sensitive data concerning patient reports involving family violence and sexual assault units

was compromised. Additionally, camera footage of patients was posted to the dark web. These incidents illustrate the types of data that threat actors are targeting and reinforces the significant privacy risks associated with such leaks.

Unfortunately, the trends observed in Australia mirror what is happening globally. In the past year, health sectors in various countries have faced similar cyber incidents. One notable attack involved 3TD of stolen data being released on the dark web in the United Kingdom, while a cyber-attack on Croatia's largest hospital caused significant disruptions and even resulted in patients being transferred to other facilities.

Our predictions

We believe that cyber-attacks on the health sector will continue over the next few years. The health sector will always remain an attractive target due to the valuable data it holds for threat actors. Therefore, it is imperative for the health sector to continue fortifying its IT systems against malicious attacks and to provide ongoing training for its employees to cultivate vigilance.





What we do
and who we are

What we do

Broad experience, driven and energetic

Our Technology, Cyber & Privacy team has extensive experience advising clients in the rapidly evolving technology, data protection and privacy space.

Whether in the course of large-scale digital transformation, uplift projects, or business as usual, we work collaboratively with clients to navigate the requirements of security and data protection including privacy compliance within the complex regulatory landscape of these dynamic areas of law.



Technology

IT Procurement & Contracting—Advising on high-value contracts, vendor agreements, cloud and other ‘as a service’ solutions and complex IT procurement processes.

Digital Transformation—Guiding organisations through digital strategy implementation, cloud services, and technology outsourcing.

Data & IP Management—Supporting IP licensing, software development, data transfer, storage and governance structures.

Emerging Tech & Innovation—Advising on AI, blockchain and Web3, fintech, quantum and other emerging and disruptive technologies, including rapidly evolving compliance and regulatory issues.

Assisting suppliers and buyers of telecommunications services, with high value, whole of business or redundancy management.



Cyber

Cyber coverage—Managing cyber coverage disputes (including serving as monitoring counsel), advising on risk management strategies and trends in the market, indemnity/claims issues regarding commercial contracts and projects, and drafting and reviewing cyber policies (both personal and company policies) for compliance and determining whether coverage exists.

Cybersecurity Strategy—Advising on regulatory compliance, risk assessments, and policy development for robust cybersecurity.

Incident Response & Crisis Management—Assisting with data breach responses, cyber-attack containment, and regulatory reporting requirements.

Cyber Risk & Insurance—Advising on risk mitigation and insurance policies specific to cyber threats and data loss.

Regulatory Compliance & Reporting—Ensuring alignment with APRA, ASIC, OAIC, and other regulatory guidelines on cyber resilience.



Privacy

Privacy Compliance & Data Protection—Supporting compliance with the Privacy Act and APPs including consent management, and cross-border data transfers.

Data Breach Management—Advising on NDB scheme obligations, breach response, and crisis communication.

Managing emerging privacy risks—advising on the privacy and cyber risks associated with automated decision making and artificial intelligence.

Employee Privacy & Surveillance—Navigating employee monitoring, privacy rights, and compliance with workplace privacy obligations.

Spam—Advising and assisting businesses with Spam compliance and complaint management.

Our promise to you



A client first approach

Your success is our success and we wouldn't have it any other way. With our client first commitment we adopt a long-term, mutually respectful approach to our relationship. We are committed to delivering high-quality, pragmatic and market relevant service.



National coverage

We are future ready. This means we can deliver genuine national capacity and expertise to our clients right now, and into the future. We are large enough to be a national commercial law firm, but small enough to have a local and personal touch, and believe we offer value with targeted and responsive legal support.



Pragmatic matter management

We work with you to understand your needs and the market you operate in. We develop pragmatic, timely and cost effective solutions with you. Our experience in and knowledge of the Hunter Region means we have an understanding of this market which is unparalleled.



The right team and capacity

Service consistency starts with the right combination of people, with the right experience, capacity and availability. We constantly review performance, including outcomes and client satisfaction to improve our service delivery. We will listen to you carefully, engage with you proactively to identify your needs and bring together the right team for your particular requirements.



A commitment to diverse and inclusive thinking

We want all our people to bring their whole selves to work, to be comfortable putting forward their opinions, and bringing fresh ideas to the table for the benefit of our clients.

Who we are

Technology, Cyber & Privacy team



Hamish Fraser
Corporate & Commercial
Partner
t: +61 2 9373 3616
e: hamish.fraser@sparke.com.au



Jason Kwan
Corporate & Commercial
Partner
t: +61 3 9291 2376
e: jason.kwan@sparke.com.au



Chantal Tipene
Government Public & Regulatory
Partner
t: +61 2 9260 2542
e: chantal.tipene@sparke.com.au



Alexandra Wedutenko
Projects & Government Commercial
Partner
t: +61 2 6263 6378
e: alexandra.wedutenko@sparke.com.au



Robert Watson
Projects & Government Commercial
Partner
t: +61 3 9291 2388
e: robert.watson@sparke.com.au



Jehan Mata
Commercial Insurance
Partner
t: +61 3 9291 2374
e: jehan.mata@sparke.com.au



Adam Payne
Projects & Government Commercial
Special Counsel
t: +61 2 9260 2410
e: adam.payne@sparke.com.au




Kelly Matheson
Government Public & Regulatory
Special Counsel
t: +61 2 6263 6309
e: kelly.matheson@sparke.com.au



Stefanie Constance
Corporate & Commercial
Associate
t: +61 3 9291 2277
e: stefanie.constance@sparke.com.au



Zach Smale
Corporate & Commercial
Associate
t: +61 2 9373 3596
e: zach.smale@sparke.com.au



Putting you at the heart
of everything we do.

www.sparke.com.au

adelaide | brisbane | cairns | canberra | darwin | melbourne | newcastle | perth | sydney | upper hunter