Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

Australia: Law & Practice
Dennis Miralis, Jasmina Ceic, Mohamed Naleemudee and Alexander Leal Smith
Nyman Gibson Miralis

Australia: Trends & Developments
Dennis Miralis, Jasmina Ceic, Kalina Ivanov and Jack Dennis
Nyman Gibson Miralis

practiceguides.chambers.com

AUSTRALIA

Law and Practice

Contributed by:
Dennis Miralis, Jasmina Ceic,
Mohamed Naleemudee and Alexander Leal Smith
Nyman Gibson Miralis see p.28

Contents

1. Basic National Regime

1.1 Laws

Australia has a broad system of federal, state and territory-based laws which govern data protection, cybersecurity and cybercrime. Further details on these laws are at **2.1 Key Laws**.

Data Protection

Privacy Act

Federally, data containing personal information is protected under the Privacy Act 1988 (Cth) (Privacy Act). Schedule 1 of the Privacy Act contains the Australian Privacy Principles (APPs), which regulate the way in which private organisations and federal agencies are required to handle personal information. The Privacy Act also requires mandatory reporting for certain APP breaches under the notifiable data breach (NDB) scheme. Breaches of the Privacy Act may result in investigation and enforcement action by the Office of the Information Commissioner (OAIC).

Health information

Health information recorded in Australia's online "My Health Records" system is protected under the My Health Records Act 2012 (Cth) (My Health Records Act).

States and territories

Australia also has various state and territory-based legislation which protects privacy and health information.

Cybersecurity

Cybersecurity laws in Australia are primarily governed under sector-specific federal laws.

Critical infrastructure

Critical infrastructure is regulated under the Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act), which imposes registration, reporting and notification obligations on owners and operators of critical infrastructure and empowers the Australian government to gather information and issue directions where there is a risk to security.

Telecommunications

Telecommunications is regulated under the Telecommunications Act 1997 (Cth) (Telecommunications Act), which imposes security and notification obligations on Australian telecommunications providers and empowers the Australian government to gather information and issue directions.

The Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act) also regulates telecommunications by prohibiting the interception of communication and access to stored communication data, except for certain law enforcement and national security purposes.

Corporations, consumers and financial services

Cybersecurity aspects of:

- corporations are regulated under the Corporations Act 2001 (Cth) (Corporations Act);
- consumers affairs are protected under the Competition and Consumer Act 2010 (Cth) (Consumer Act); and
- certain financial, insurance and superannuation entities are regulated through standards, including the Prudential Standard CPS 234 on Information Security (CPS 234), issued by the Australian Prudential Regulation Authority (APRA).

Cybercrime

Cybercrime offences in Australia broadly encompass two categories:

- offences that are directed at computers or other devices and involve hacking-type activities; and
- cyber-enabled offences where such devices are used as a key component of the offence, including in online fraud, online child abuse offences and cyberstalking.

Federally, cybercrime is criminalised under Parts 10.6 and 10.7 of the Schedule to the Criminal Code Act 1995 (Cth) (Criminal Code), which set out a variety of offences with maximum penalties ranging from fine-only through to life imprisonment.

Australian states and territories also have their own criminal laws which govern cybercrime offences.

1.2 Regulators

Australia has a range of federal, state and territory regulators which deal with cybersecurity. Further details of these regulators are at **2.2 Regulators**.

Data Protection

The OAIC is the federal privacy and information regulator with a range of functions and powers to investigate and resolve privacy complaints and enforce privacy compliance.

There are also state and territory privacy commissioners which administer state and territory-based privacy and health information laws.

Cybersecurity

There are a range of sector-specific federal regulators as outlined below.

Critical infrastructure

The Critical Infrastructure Centre (CIC) is the federal regulator of the SOCI Act and certain provisions of the Telecommunications Act with powers to investigate, audit and enforce on compliance matters.

Telecommunications, broadcasting and marketing

The Australian Communications and Media Authority (ACMA) is Australia's regulator for broadcasting, telecommunication and certain online content and provides licensing to industry providers. ACMA has specific regulatory powers under the Telecommunications Act, the TIA Act, the Spam Act, and the Do Not Call Register Act to investigate and resolve complaints and enforce compliance.

Additionally, the Office of the eSafety Commissioner (eSafety Commissioner) has powers to promote and regulate online safety with respect to telecommunications, broadcasting and other online industries.

Corporations, consumers and financial services

The Australian Securities and Investments Commission (ASIC) regulates publicly listed corporations under the Corporations Act and may investigate issues which touch on cybersecurity.

APRA regulates certain finance, insurance and superannuation entities and issued information security standards CPS 234.

The Australian Competition and Consumer Commission (ACCC) deals with consumer affairs, including consumer data protection and cyberscams.

Cybercrime

Cybercrime at the federal level is investigated and enforced by the Australian Federal Police

(AFP) and prosecuted by the Commonwealth Director of Public Prosecutions (CDPP).

State and territory-based police and prosecution agencies investigate, enforce and prosecute state and territory cybercrimes.

Law enforcement agencies may be supported by criminal intelligence agencies including the Australian Criminal Intelligence Commission (ACIC), Australian Security Intelligence Organisation (ASIO), Australian Signals Directorate (ASD) and Australian Transaction Reports and Analysis Centre (AUSTRAC).

1.3 Administration and Enforcement Process

Data Protection and Cybersecurity

Broadly, federal data protection and cybersecurity regulators handle complaints and commence their own investigations into non-compliance matters. These regulators will initially seek to collaborate with regulated entities and seek voluntary compliance. If these efforts fail, the regulators may consider taking enforcement action. Decisions made by these regulators can often be reviewed internally and can also be referred to certain federal tribunals and courts including the Administrative Appeals Tribunal (AAT), the Federal Circuit and Family Court of Australia (FCFCA), or the Federal Court of Australia (FCA). Complaints about federal regulators, including complaints about unfair treatment, can be referred to the Commonwealth Ombudsman.

Details regarding the specific administrative and enforcement powers of specific regulators are provided in **2.2 Regulators**.

Cybercrime

Law enforcement and intelligence agencies that deal with cybercrime have a broad range of investigative and enforcement powers, including investigative and disruption powers executed through warrants.

The passing of the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth) (SLAID Act) enabled law enforcement to obtain "data disruption warrants", which, if issued, permit law enforcement to intervene in order to frustrate the commission of cybercrime.

There are various oversight and review processes for decisions and actions undertaken by law enforcement and intelligence agencies, including through Australian courts and complaints to statutory bodies such as:

- the Commonwealth Ombudsman and the Australian Commission for Law Enforcement Integrity (ACLEI), which oversees AFP activities; and
- the Inspector-General of Intelligence and Security (IGIS), which oversees intelligence agency activities.

1.4 Multilateral and Subnational Issues

Australia engages in a variety of multilateral processes to address data protection, cybersecurity and cybercrime matters which are outlined below. Details of subnational issues are detailed at **2. Key Laws and Regulators at National and Subnational Levels**.

Data Protection

Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System

Australia acceded to the CBPR in 2018. The CBPR is a voluntary accountability framework and requires participating businesses to implement data privacy policies and practices consistent with the APEC Privacy Framework, a principle-based model for national privacy laws

that account for cross-border information flows. Business compliance with the CBPR is assessed by an independent Accountability Agent recognised by APEC. Non-compliance with the CBPR may result in a loss of CBPR certification, referral to government enforcement authorities and other penalties.

Cybersecurity

Norms of state behaviour in cyberspace

Australia participates in the UN General Assembly's two parallel processes, established in December 2018, to foster responsible state behaviour in cyberspace:

- the inaugural Open Ended Working Group on Developments in the Field of ICTs (OEWG), mandated to consider the application of international law, rules and norms to the behaviour of states in cyberspace and cyberthreats, which handed down its Final Substantive Report in 2021; and
- the sixth Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security (UNGGE).

A second OWEG was established by the UN General Assembly in 2020, concerning the security and use of information and communications technologies.

Australia, New Zealand, United States Security Treaty (ANZUS Treaty)

In September 2011, Australia and the USA agreed that the ANZUS Treaty could be invoked in response to a cyber-attack. The ANZUS treaty is a non-binding collective security agreement between Australia and New Zealand and between Australia and the USA, which facilitates state co-operation on military matters in the Pacific Ocean region.

Cybercrime

International crime co-operation

Australia engages in extradition, mutual assistance and international transfer of prisoners with other countries as part of its international crime co-operation efforts, which also apply in relation to cybercrime.

International crime co-operation relationships in Australia are regulated under bilateral and multilateral treaties, or through non-treaty arrangements with particular countries.

In December 2021, Australia and the USA entered an Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime. This Agreement enables law enforcement and national security agencies to issue orders directly to communications providers in the other country for the production of electronic data relevant to investigations or prosecutions of criminal activity.

Australia may also engage in direct police-to-police co-operation and intelligence information sharing in respect of cybercrimes.

Budapest Convention

Australia is party to the Convention on Cybercrime of the Council of Europe of 2001 (CETS No 185) (Budapest Convention), which provides for:

- standards for criminalising particular cyber-activities ranging from illegal access and interference to computer-related fraud and child pornography;
- procedural law tools for the investigation of cybercrime and the securing of electronic evidence more effective; and
- efficient international co-operation.

Australia has participated in the development of the Second Additional Protocol to the Budapest Convention that deals with trans-border access to information. With currently 34 state signatures, this Protocol further details co-operation requirements between state parties on cybercrime information sharing. The Protocol includes provisions regarding direct co-operation with service providers registrars in other jurisdictions to obtain registration and subscriber information, and government co-operation to obtain this data.

1.5 Information Sharing Organisations and Government Cybersecurity Assistance

Data Protection

The OAIC works collaboratively with public and private sector organisations to share information about privacy issues and encourage privacy compliance.

Cybersecurity and Cybercrime

The Australian Cyber Security Centre (ACSC) facilitates information and collaboration across private, public and non-government (NGO) sectors to develop collective cyber-resilience and to respond to cyber-incidents. In this regard, the ACSC has commenced:

- a partnership programme, which brings participants from the private, public, and NGO sectors together to enable information sharing and network hardening; and
- an alert service, which provides information on recent cyberthreats as well as prevention and mitigation advice.

The Joint Cyber Security Centres (JCSC) are state-based agencies which collaborate with organisations across the private, public and NGO sectors on cybersecurity and cybercrime threats and response options.

1.6 System Characteristics

Data Protection

Australia's privacy framework is largely centralised under the Privacy Act and involves a principle-based approach to privacy. The centralised principle-based model is similar to the approach undertaken by the EU's General Data Protection Regulation (GDPR) and can be contrasted to the US approach to privacy laws, which relies on less centralised privacy governance.

The GDPR and Australia's privacy framework share some commonalities including:

- the use of privacy principles as a framework for obligations;
- the adoption of transparent information handling practices; and
- the use of similar concepts on the type of information that should be protected.

However, the GDPR is broader in scope, provides more robust enforcement mechanisms and affords additional privacy rights to individuals (such as the right to be forgotten).

Cybersecurity and Cybercrime

Australia's approach to cybersecurity and cybercrime governance appears largely consistent with global governance trends, in which we see more and more states focus on:

- broadening government powers in relation to cyber-investigations, interventions, oversight and enforcement;
- increasing state offensive and defensive cybercapabilities;
- building technical cybercapabilities across private and public sectors;

- establishing legal frameworks and other standards for cybersecurity; and
- improving user awareness and promoting cyber-education programmes.

1.7 Key Developments

Data Protection and Privacy Proceedings

On 6 February 2023, a class action was launched against Medibank Private Limited in the wake of a cyberattack in October 2022, during which hackers reportedly accessed 9 million current and former members' personal data and 470,000 of their health claims information.

Further significant privacy proceedings are set out at **8.1 Regulatory Enforcement or Litigation**.

Cybersecurity Proceedings

The recent Federal Court matter of Australian Securities and Investments Commission v RI Advice Group Ltd (2022) FCA 496 (ASIC v RI Advice) is one of Australia's most significant enforcement proceedings regarding cybersecurity obligations. Further information is also set out at **8.1 Regulatory Enforcement or Litigation**.

Australia's Cybersecurity Policy Initiatives

In December 2022, the Australian government announced a new cybersecurity strategy (2023-2030 Cyber Strategy), which is understood to replace the 2020 Cyber Security Strategy. Further details are yet to be disclosed; however, a new Expert Advisory Board was appointed to oversee its development. The objectives of the new strategy are to:

- protect Australians through whole-of-nation cyber effects;
- protect critical infrastructure;
- build sovereign capabilities to address cyberthreats;
- strengthen and expand Australia's international engagement; and
- grow and sustain Australia's cyber workforce.

Separately, the Australian government is establishing a permanent taskforce consisting of officers from the AFP and the ASD. This joint standing operation is tasked with responding to cybercrimes and targeting ransomware groups and is to work with international agencies, including the FBI and Interpol, to collect intelligence and identify individuals, networks, and infrastructure of cybercriminals prior to the occurrence of cyber-incidents.

1.8 Significant Pending Changes, Hot Topics and Issues

The Australian government has proposed significant changes to data protection, cybersecurity and cybercrime legislation in the coming year.

Project REDSPICE

In 2022, the ASD launched Project REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers). This project will receive AUD9.9 billion in funding from the Australian government, with aims such as enhancing intelligence gathering; developing asymmetric strike capabilities and offensive cyber for the ADF; and strengthening Australia's cyber defence.

Disruption warrants

As noted in **1.3 Administration and Enforcement Process**, the SLAID Act allows law enforcement to apply to obtain "data disruption warrants". These warrants enable law enforcement agencies to engage in a range of disruption and takeover activities to combat cybercrime and cyber-enabled crime, including activities undertaken on the dark web. The Attorney-General's Surveillance Devices Act 2004 Annual Report 2021-22, published 30 November 2022, disclosed that the

first two data disruption warrants were issued in FY22.

2. Key Laws and Regulators at National and Subnational Levels

2.1 Key Laws

Data Protection

The Privacy Act

The Privacy Act regulates the handling of personal information federally.

"Personal information" under the Privacy Act is defined broadly as information or an opinion about an identified or reasonably identifiable individual. It is not required to be true or recorded in a material form. Personal information also includes "sensitive information", which includes information or opinions on an individual's race, ethnicity, politics, religion, sexual orientation, health, trade associations and criminal records. Sensitive information is often afforded a higher level of protection than other personal information.

The Privacy Act applies to "APP entities" which, subject to some exceptions, include federal government agencies, private sector organisations with an annual turnover of over AUD3 million and smaller entities with data-intensive business practices (including private health providers, businesses that sell or purchase personal information and service providers to the federal government).

Schedule 1 of the Privacy Act sets out 13 APPs, which provide minimum standards for the processing of personal information; it is detailed at **3.3 Legal Requirements and Specific Required Security Practices**.

NDB scheme

In February 2018, the Privacy Act was amended to include the NDB scheme, which requires APP entities to notify affected individuals and the OAIC where there are reasonable grounds to believe that an "eligible data breach" has occurred.

Further details on the NDB scheme are at **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**, **5.2 Data Elements Covered**, **5.3 Systems Covered**, **5.8 Reporting Triggers** and **5.9 "Risk of Harm" Thresholds or Standards**.

Other data protection laws

Entities dealing with personal information in Australia should also be aware of their obligations with respect to:

- privacy legislation enacted at the state and territory level;
- the My Health Records Act, which imposes specific obligations for health information collected and stored in Australia's national online health database;
- state and territory health records legislation enacted in New South Wales (NSW), Victoria (Vic) and the Australian Capital Territory (ACT); and
- federal, state and territory surveillance legislation, which regulates video surveillance, computer and data monitoring, GPS tracking and the use of listening devices on individuals.

Cybersecurity

Critical infrastructure

The SOCI currently regulates assets in various fields, including communications, data storage, financial services, energy and the defence industry by requiring owners and operators of such assets to register with the Register of Critical

Infrastructure Assets and provide ownership and operational information.

The SOCI Act includes:

- an information gathering power for the Secretary of the Department of Home Affairs (DoHA) to monitor compliance; and
- a directions power for the Home Affairs Minister (HA Minister) to direct regulated entities to do or not do a specified thing that is reasonably necessary to protect critical infrastructure from national security risks.

Telecommunications

The Telecommunications Act regulates the use of personal information by carriers, carriage service providers and intermediaries and prohibits disclosure of certain telecommunications data. Amendments to this Act in 2017, known as the Telecommunication Sector Security Reforms (TSSR), provide for:

- positive security obligations that require regulated entities to protect against access and interference of telecommunications networks and systems, including through maintaining "competent supervision" and "effective control"; and
- notification obligations that require regulated entities to notify government of changes which may affect their security obligations.

The TSSR also endows the Secretary of DoHA with an information-gathering power and the HA Minister with a directions power.

Chapter 5 of the TIA Act obliges Australian telecommunications service providers to collect and retain certain types of data for a minimum of two years, to build systematic capabilities to intercept such data, and to provide law enforcement and security agencies with access to such data for certain law enforcement and national security purposes.

Broadcasting and marketing

The Broadcasting Act regulates broadcasting services through internet and other means in Australia and enables the creation of industry codes of practice regulating the content of such services.

The OSA establishes complaint systems for cyberbullying of children, non-consensual sharing of intimate images, cyber-abuse of adults, and the online/social media availability of content that would be subject to broadcasting classifications (restricted or age 18+).

The Spam Act prohibits the use of electronic communications for the purpose of sending unsolicited marketing materials to individuals.

Similarly, the Do Not Call Register Act prohibits unsolicited telemarketing calls being made to phone numbers registered on a Do Not Call Register.

Corporations, consumers and financial services

Regulations governing the corporate sectors deal with cybersecurity in certain circumstances. For example:

- Section 180 of the Corporations Act imposes a director's duty to exercise "care and diligence", which would apply in the context of cybersecurity;
- Section 912A of the Corporations Act requires corporations holding financial licences to have adequate risk management systems, which would include those relating to cybersecurity;

- Part IVD of the Consumer Act, detailed at **4.2 Material Business Data and Material Non-public Information**, provides for the Consumer Data Right (CDR), which seeks to regulate how business can share consumer data; and
- CPS 234, detailed at **3.1 De Jure or De Facto Standards**, regulates information security standards for APRA-regulated financial, insurance and superannuation entities.

Cybercrime

Criminal Code

Part 10.6 of the Criminal Code provides for federal offences regarding the misuse of telecommunication networks and "carriage services" (a term encompassing the internet and online, wired and mobile services). These include offences relating to dishonesty, interference with telecommunications, harassment, child abuse material, making threats, or causing menace/harassment/intimidation and have maximum penalties ranging from one to 30 years' imprisonment. This Part of the Criminal Code also places obligations on providers of content or hosting services to notify the AFP as to the existence of material displaying "abhorrent violent conduct" (if occurring in Australia) and, in any event, to expeditiously remove or cease to host such material.

Part 10.7 of the Criminal Code sets out computer offences. Serious offences include the misuse of data to commit serious offences or impair data security and the impairment of electronic communications. These offences carry maximum penalties ranging from five to ten years', as well as life, imprisonment. Other computer offences include preparing for or engaging in unauthorised access and modification or impairment of data, which carry maximum penalties of two to three years' imprisonment.

Other offences

Organisations should note that in addition to the Criminal Code:

- the TIA Act also makes it a federal offence for an individual to (without authorisation) intercept or access private telecommunications without the knowledge of those involved; and
- state and territory laws criminalise computer offences similar to those criminalised under the Criminal Code (eg, Part 6 of the Crimes Act 1900 (NSW) provide for multiple computer offences regarding unauthorised access, modification or impairment of restricted data and electronic communications).

2.2 Regulators

Data Protection and the OAIC

Federally, the OAIC administers the Privacy Act and the My Health Records Act and also has a range of powers regarding privacy considerations under the Telecommunications Act and the TIA Act. The OAIC can investigate breaches of these acts that arise from privacy complaints and NDBs under federal privacy laws. The OAIC can also investigate federal privacy law breaches of its own volition.

The OAIC has powers under the Privacy Act to investigate, resolve complaints, make determinations and provide remedies for breaches under the NDB scheme. The remedies range from enforceable undertakings to civil penalties of 2,000 penalty units (approximately AUD444,000). As part of its review of the Privacy Act, the Australian government is considering introducing legislation that would increase maximum fines for serious and repeated breaches of privacy to the greater of AUD10 million, three times the value of any benefit obtained through misuse of the information in question, or 10% of the entity's annual Australian turnover.

Cybersecurity

Critical infrastructure

The CIC sits within the DoHA. The CIC assists with the administration of the SOCI Act and certain provisions of the Telecommunications Act and has certain investigative and auditing powers to ensure compliance with these acts. The CIC also has the ability to make recommendations to DoHA and the HA Minister on whether their information-gathering powers and directions powers should be exercised. The CIC also has enforcement powers which allows it to issue penalties for non-compliance that range from performance injunctions, enforceable undertakings and civil penalties of up to 250 penalty units (AUD55,500).

Telecommunications, broadcasting and marketing

ACMA has powers under the Telecommunications Act, TIA Act, Broadcasting Act, Spam Act, and the Do Not Call Register Act to undertake discretionary administrative action. In dealing with non-compliance, ACMA is empowered to issue warnings, infringement notices, enforceable undertakings and remedial directions. ACMA is further able to cancel or impose conditions on licences and accreditations. ACMA also has the ability to commence civil proceedings or refer matters for criminal prosecution.

The eSafety Commissioner has powers to investigate online content that promotes, incites, or instructs in crime. However, the Commissioner cannot investigate matters of cybercrime. Penalties range from takedown notices and blocking directions.

Corporations, consumers and the finance services

Relevant regulators are detailed at **2.5 Financial or Other Sectoral Regulators**.

Cybercrime

The below intelligence organisations assist federal and state law enforcement agencies in investigating cybercrime.

- ACIC is Australia's national criminal intelligence agency; it has broad investigative and coercive powers and shares information between all levels of law enforcement.
- AUSTRAC is the domestic watchdog for Australia's anti-money laundering and counter-terrorism measures; it supports law enforcement operations involving cybercrime financing.
- ASIO investigates cyber-activity involving espionage, sabotage and terrorism related activities; ASIO also contributes to the investigation of computer network operations directed against Australia's systems.
- The ASD sits within the Department of Defence and has responsibility for foreign signals intelligence, cybersecurity and offensive cyber-operations; ASD provides assistance and advice to law enforcement and can collaborate with police forces on national security matters including on cyber-attacks and cyberterrorism.

2.3 Over-Arching Cybersecurity Agency

DoHA

The DoHA is the lead government department for cyberpolicy. The DoHA develops cybersecurity and cybercrime law and policy, implements Australia's national cybersecurity strategy and responds to international and domestic cybersecurity threats and opportunities, including in the areas of critical infrastructure and emerging technologies. The DoHA also has responsibility for cybersecurity and cybercrime operational agencies including the AFP, ACIC, AUSTRAC, and ASIO.

ASD
The ASD is Australia's operational lead on cybersecurity and plays both a signals intelligence and information security role. The ASD undertakes cyberthreat monitoring and conducts defensive, disruption and offensive cyber-operations offshore to support military operations and to counter terrorism, cyber-espionage and serious cyber-enabled crime. The ASD also advises and co-ordinates operational responses to cyber-intrusions on government, critical infrastructure, information networks and other systems of national significance.

The ACSC
The ACSC sits within the ASD. It drives cyber-resilience across the whole Australian economy including with respect to critical infrastructure, government, large organisations and small to medium businesses, academia, NGOs and the broader Australian community. The ACSC provides general information, advice and assistance to Australian organisations and the public on cyberthreats and it collaborates with business, government and the community to increase cyber-resilience across Australia.

The ACSC also runs the Computer Emergency Response Team (CERT), a "computer emergency response team" that provides advice and support to industry on cybersecurity issues affecting Australia's critical infrastructure and other systems of national significance.

2.4 Data Protection Authorities or Privacy Regulators
As detailed in **1.2 Regulators** and **2.2 Regulators**, the OAIC administers federal privacy and health information laws.

The OAIC also acts as the privacy regulator for territory-based privacy complaints in the ACT.

Apart from the ACT, other states and territories have their own privacy regulators who administer state and territory laws governing personal and health information. For example:

- the NSW Information and Privacy Commission administers, inter alia, the Privacy and Personal Information Protection Act 1998 (NSW) and Health Records and Information Privacy Act 2002 (NSW); and
- the Office of the Victorian Information Commissioner administers the Privacy and Data Protection Act 2014 (Vic) and the Office of the Health Services Commissioner administers the Health Records Act 2001 (Vic).

2.5 Financial or Other Sectoral Regulators
Credit Reporting
The OAIC regulates the aspects of the Privacy Act which deal with credit reporting obligations and the credit reporting code, which imposes certain conditions on entities that hold credit-related personal information.

Corporations, Consumers and Financial Services
As referred to in **1.2 Regulators**, corporate, consumer and financial regulators include ASIC, the ACCC and APRA.

ASIC
ASIC, which is Australia's corporate, market and financial services regulator, is empowered under the Corporations Act to investigate and bring actions against corporations, directors and officers for non-compliance with the Corporations Act, which, in some circumstances, may involve cybersecurity issues.

ACCC

The ACCC, which is Australia's competition regulator and consumer protector, may, where appropriate, undertake enforcement action against breaches of the Consumer Act, including breaches involving cybersecurity and cybercrime issues.

The ACCC administer the CDR (detailed at **4.2 Material Business Data and Material Non-public Information**) and also hosts the SCAMwatch website, which provides public information, alerts and access to complaints mechanisms on a wide range of consumer scams, including scams perpetrated online.

APRA

APRA, which regulates entities in the banking, insurance and superannuation sector, issued legal standards for information security under Prudential Standard CPS 234 in 2019 (detailed in **3.3 Legal Requirements and Specific Required Security Practices**).

APRA has powers to supervise, monitor and intervene in matters of cybersecurity for regulated entities and has a range of enforcement powers to deal with breaches of its standards. Such powers involve APRA issuing infringement notices, providing directions or enforceable undertakings, imposing licensing conditions, disqualifying senior officials and commencing court-based action.

2.6 Other Relevant Regulators and Agencies

In addition to the regulators and agencies detailed at **1.2 Regulators** and **2. Key Laws and Regulators at National and Subnational Levels**, the following agencies deal with cybersecurity and cybercrime.

- The AFP have a dedicated Cybercrime Operations team comprising investigators, technical specialists and intelligence analysts who operate across multiple jurisdictions to conduct cyber-assessments and to triage, investigate and disrupt cybercrime.
- The Attorney-General's Department (AGD) advises government on cybersecurity policies and law, including in relation to human rights, privacy, protective security, international law, administration of criminal justice, and oversight of intelligence, security and law enforcement agencies.
- The Department of Defence (Defence) contributes to Australia's whole-of-government cybersecurity policy and operations and houses ASD; it also houses the Information Warfare Division, which develops information warfare capabilities for the Australian Defence Force (ADF).
- The Department of Foreign Affairs and Trade (DFAT) advances Australia's international cyber-affairs agenda, which includes digital trade, cybersecurity, cybercrime, international security, internet governance and co-operation, human rights and democracy online, and technology for development.

3. Key Frameworks

3.1 De Jure or De Facto Standards

Data Protection Standards

De jure standards

Organisations should have regard to their obligations under the Privacy Act, Archives Act 1983 (Cth) (Archives Act), and TIA Act when creating standards for the collection, use, and storage of particular information.

De facto standards

The OAIC's Privacy Management Framework, detailed at **3.2 Consensus or Commonly Applied Framework**, may be considered a de facto standard for data protection.

Cybersecurity Standards

De jure standards

In July 2019, APRA issued Prudential Standard CPS 234 on Information Security. This regulation requires APRA-regulated financial, insurance and superannuation entities to comply with legally binding minimum standards of information security, including by:

- specifying information security roles and responsibilities for the entities' board, senior management, governing bodies and individuals;
- implementing and maintaining appropriate information security capabilities;
- maintaining tools to detect and respond to information security incidents in a timely way; and
- notifying APRA of any material information security incidents.

These standards provide that an entity's board is ultimately responsible for information security and that the board must ensure that its entity maintains information security in a manner that is commensurate with the size and vulnerability of that entity's information assets.

APRA-regulated entities are required to externally audit their organisation's compliance with CPS 234 and report to APRA in a timely manner.

If organisations are non-compliant, they may be required to issue breach notices and create rectification plans. If organisations are unable to comply with the standards following this process, APRA may undertake a more formal enforcement process which may include enforceable undertakings or court proceedings.

De facto standards

ISO/IEC 27001 is an international standard on management of information security. While the Australian government recommends that organisations comply with this standard, it is not mandatory.

ASIC's "Cyber reliance good practices" provides guidance to Australian corporations on information security. The guide includes recommendations for:

- periodic review of company cyber strategies;
- using cyber-resilience as a management tool;
- engaging in responsive cybersecurity governance, collaboration and information sharing;
- third-party risk management; and
- implementing continuous monitoring systems.

The Australian Government Information Security Manual (ISM) outlines a voluntary cybersecurity framework for organisations based on ACSC advice and includes security protection principles for designing, implementing, and reviewing appropriate security systems, policies, and practices.

3.2 Consensus or Commonly Applied Framework

Data Protection

The Privacy Act APPs provide a legally binding framework for APP entities with respect to the collection, processing, use, storage, and dissemination of personal information (details of which are outlined at **3.3 Legal Requirements and Specific Required Security Practices**).

APP entities are obliged to take "reasonable steps" to implement policies, practices and systems to ensure compliance with APPs. The "Privacy Management Framework", developed by the OAIC, provides governance steps that APP entities should undertake to meet their privacy compliance obligations including by embedding a privacy compliant culture and by establishing and evaluating privacy practices and systems.

Cybersecurity

De facto cybersecurity frameworks are detailed at **3.1 De Jure or De Facto Standards**.

3.3 Legal Requirements and Specific Required Security Practices

Data Protection and the APPs

The Privacy Act APPs comprise legally binding obligations for APP entities with respect to:

- managing personal information openly and transparently (APP1);
- permitting individuals the right to anonymity/pseudonymity (APP2);
- collecting solicited personal information (APP3);
- dealing with unsolicited personal information (APP4);
- notifying individuals about their collected personal information (APP5);
- using or disclosing personal information (APP6), including for direct marketing (APP7);
- disclosing personal information overseas (APP8);
- using government-issued identifiers of individuals (APP9);
- ensuring the accuracy, currency completeness of personal information (APP10);
- securing personal information (APP11); and
- permitting individuals to access (APP12) and correct (APP13) their personal information.

Breaches of these APP's may be subject to reporting under the NDB scheme (as detailed in **2.1 Key Laws**, **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**, **5.2 Data Elements Covered**, **5.3 Systems Covered**, **5.8 Reporting Triggers** and **5.9 "Risk of Harm" Thresholds or Standards**).

Cybersecurity and the Cyber Strategy

Following the 2020 Cyber Strategy, the Australian government developed legally binding minimum cybersecurity standards for organisations generally. The 2020 Cyber Strategy notes that these standards may result in:

- changes to data protection, privacy and consumer laws;
- additional obligations on company directors; and
- baseline cybersecurity requirements for critical infrastructure and systems of national significance.

Refer to **1.1 Laws**, **2.1 Key Laws**, **3.1 De Jure or De Facto Standards** and **4.3 Critical Infrastructure, Networks, Systems** for details on sector-specific cybersecurity legal requirements and standards.

3.4 Key Multinational Relationships

Data Protection

Australia is a member of the APEC Data Privacy Subgroup. This group developed the APEC Privacy framework and meets biannually to discuss privacy issues.

Cybersecurity

The "Five Eyes" is an intelligence sharing alliance between Australia, the USA, the United Kingdom, Canada and New Zealand. These countries are party to the UKUSA Agreement, which is a treaty for joint signals intelligence co-

operation. The cybersecurity representatives of Five Eyes collaborate on joint cyber-incident response. In September 2020, Five Eyes published a best practice guide for cyber-incident investigation and responses.

Australia also engages in a range of other international groups to address cybersecurity issues including the UNGGE and OWEG (as detailed at **1.4 Multilateral and Subnational Issues**), the East Asia Summit and the ASEAN Regional forum. Australia also undertakes cybercapacity building efforts and knowledge sharing in the Pacific Region.

Cybercrime

Parties to the Budapest Convention, including Australia, are members of the Cybercrime Convention Committee (T-CY), which currently is the most relevant intergovernmental body dealing with cybercrime.

4. Key Affirmative Security Requirements

4.1 Personal Data

As referred to in **3.3 Legal Requirements and Specific Required Security Practice** s, APP11 deals with the security of personal information and requires APP entities to actively take "reasonable steps in the circumstances to protect personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure". An APP entity must also take reasonable steps to destroy or de-identify information that is no longer needed.

"Reasonable steps" will vary according to each APP entity and will depend on circumstances that include:

- the size, complexity and business model of an APP entity;
- the sensitive nature of the personal information;
- the possible adverse consequences of a privacy breach; and
- practical implications of implementing security measures.

The OAIC's Guide to Securing Personal Information provides further discussion of affirmative personal information security. The OAIC is currently in the process of updating this guide.

4.2 Material Business Data and Material Non-public Information

Part IVD of the Consumer Act provides for the Consumer Data Right (CDR), which seeks to regulate how business can share consumer data. Implementation of the CDR will occur progressively by industry. The CDR has been rolled out to the banking and energy sectors.

In July 2020, CDR rules were introduced for the banking sector, outlining how CDR laws apply in relation to consent, privacy, accreditations, and data standard aspects of consumer data sharing.

4.3 Critical Infrastructure, Networks, Systems

SOCI Act

The SOCI Act requires owners and operators of critical infrastructure to register under the Register of Critical Infrastructure Assets (a non-public register) and disclose particular information to the Secretary of the DoHA.

"Responsible entities", which are the entities that hold the relevant licensing or approvals to operate critical infrastructure, must provide operational and asset information to DoHA.

"Direct interest holders", which are entities that own at least 10% of the critical infrastructure asset, must provide interest and control information. Any updates to this information must occur within 30 days. Failure to fulfil these reporting obligations may result in a penalty of up to 50 penalty units.

The SOCI Act also requires critical infrastructure owners and operators to comply with Ministerial directions or Secretarial requests for information where necessary. In March 2022, the SOCI Act was amended to oblige responsible entities to create and maintain a critical infrastructure risk management programme. This amendment also included a new framework for enhanced cybersecurity obligations for operators of systems of national significance.

Telecommunications Act

The Telecommunications Act requires network operators to safeguard Australian communications from unauthorised access or interference that might prejudice Australia's national security.

4.4 Denial of Service Attacks

There are no legally mandated requirements with respect to securing against denial of service (DoS) or distributed DoS (DDoS) attacks. The ACSC recommends that organisations can prevent such attacks through steps such as:

- regularly monitoring and patching IT and website security systems;
- using a Content Delivery Network (CDN) or DDoS mitigation provider; and
- having DoS-specific incident response plans.

4.5 Internet of Things (IoT), Software, Supply Chain, Other Data or Systems

The Australian government is developing measures for securing internet of things (IoT) devices and supply chain management under its 2020 Cyber Strategy.

IoT

The government has developed a voluntary code of practice with 13 principles, which set out the government's expectations for IoT consumer devices. The ACSC provides associated guidance on this code, providing practical examples for individuals and businesses. The government has indicated that if a voluntary process is insufficient, additional regulation may be considered.

Supply Chain

The ACSC has released numerous publications as part of its "Cyber Supply Chain Guidance". These include publications concerning risk identification, management of security, and issues when engaging a managed service provider, all of which provide technical guidance on key cybersecurity issues.

Furthermore, in the 2020 Cyber Strategy the government attempted to uplift businesses' cybersecurity capabilities by:

- adopting a security-by-design approach to supply chains;
- promoting further innovation in sovereign cybersecurity research and development;
- establishing a Cyber Security Best Practice Regulation Task Force; and
- encouraging large businesses to share cybersecurity information and tools with small businesses.

In 2021, the DoHA published "Critical Technology Supply Chain Principles", outlining ten agreed principles for supply chain security, categorised under the following three pillars:

- security-by-design;

- transparency; and
- autonomy and integrity.

4.6 Ransomware

The ACSC regularly publishes guidance and advice to assist with preparing for and responding to a ransomware attack. The ACSC recommends to never pay a ransom in the case of a ransomware attack.

Business owners that hold sensitive information or form part of a government supply chain are obliged to report data breaches under the Notifiable Data Breaches scheme in the Privacy Act. This extends to instances of ransomware attacks. The NDB scheme is outlined in further detail at **2.1 Key Laws** and **5. Data Breach or Cybersecurity Event Reporting and Notification**.

5. Data Breach or Cybersecurity Event Reporting and Notification

5.1 Definition of Data Security Incident, Breach or Cybersecurity Event

NDB Scheme

As outlined in **2.1 Key Laws**, Part IIIC of the Privacy Act sets out a scheme for "notification of eligible data breaches". In short, as per Section 26WE(2) of the Privacy Act, an "eligible data breach" occurs where:

- there is unauthorised access to/disclosure of personal information and a reasonable person would conclude that this "would be likely to result in serious harm to any of the individuals to whom the information relates"; or
- personal information is lost in circumstances where a reasonable person would conclude that unauthorised access to/disclosure of it is likely to occur and, were it to occur, it "would be likely to result in serious harm to any of the individuals to whom the information relates".

However, Section 26WF of the Privacy Act creates an exception to reporting such an incident, where the entity in question takes remedial action to ensure that the breach does not cause serious harm to the individuals concerned.

The ACSC provides an overarching definition for cybersecurity events in its Guidelines for Cyber Security Incidents. In the guidelines, a cybersecurity event is "an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security". While there is no general legislative definition of a cybersecurity event, the SOCI Act, at Section 12M, provides a limited definition.

5.2 Data Elements Covered

The types of data covered by the NDB scheme, described in **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**, are all those falling within the definition of "personal information".

"Personal information" is defined in Section 6 of the Privacy Act to mean "information or an opinion about an identified individual, or an individual who is reasonably identifiable". It does not matter whether the information/opinion is true or is recorded "in a material form". Personal information also includes sensitive information as outlined in **2.1 Key Laws**.

5.3 Systems Covered

The systems covered by the NDB scheme are those:

- administered by APP entities holding personal information (see **5.2 Data Elements Covered**);
- administered by credit reporting bodies holding credit reporting information (including, for example, personal solvency information, and repayment history information);
- administered by credit providers (eg, banks) holding credit eligibility information; and
- administered by file number recipients holding Tax File Number information (ie, anyone in possession or control of a record containing tax file number information).

5.4 Security Requirements for Medical Devices

Information that is covered by the specific data breach notification scheme set out in section 75 of the My Health Records Act is not included in disclosure obligations under the Privacy Act scheme.

Under Section 75 of the My Health Records Act, any compromise (including potential compromise) or unauthorised collection/disclosure of data held under a My Health Record requires reporting to the relevant system operator and/or the OAIC. Subsequently, all "affected healthcare recipients" must also be notified of the compromise or unauthorised disclosure.

Other than those data breaches to which the My Health Records Act applies, medical data would generally be personal information and covered by the NDB scheme detailed in **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event** and **5.2 Data Elements Covered**.

5.5 Security Requirements for Industrial Control Systems (and SCADA)

Please see **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event** and **5.2 Data Elements Covered**.

5.6 Security Requirements for IoT

As noted in the response to **4.5 Internet of Things (IoT), Software, Supply Chain, Other Data or Systems**, in 2020, the Australian government introduced a voluntary code of practice concerning IoT devices. In 2021, the government established the Cyber Security Best Practice Regulation Task Force "to work with businesses and international partners to consider options for better protecting customers by ensuring cyber security is built into digital products, services and supply chains".

5.7 Requirements for Secure Software Development

The voluntary code of practice for the IoT, as outlined in **5.6 Security Requirements for IoT**, sets out requirements which apply to the security software lifecycle. Principle 3 of the code generally sets out requirements for ensuring software is securely updated. Additionally, the code requires that devices and services operate on the "principle of least privilege" and requires all certifications be managed securely.

The ACSC's ISM chapter on Guidelines for Software Development provides detailed, technical guidance on the development of a secure software lifecycle for traditional, mobile and web applications.

5.8 Reporting Triggers

The relevant reporting "trigger" is belief that an "eligible data breach" (see **5.1 Definition of Data Security Incident or Breach**) has occurred.

When such a breach occurs, the entity must report to both the OAIC (detailing the breach, the kind/s of information concerned, and recommendations for steps individuals should take in response to the breach) as well as individuals whose data has been subject to the breach. If

it is not practicable for the entity to notify the individuals concerned, it must publish (including on its website) a copy of the aforementioned statement to the OAIC concerning the breach.

The reporting "trigger" threshold is consistent across all entities relevant to the "notification of eligible data breaches" scheme, both public and private.

It is also noted that (pursuant to Section 26WH of the Privacy Act) where an entity merely suspects (but doesn't necessarily believe) that an eligible data breach has occurred, it has 30 days to "carry out a reasonable and expeditious" assessment of the matter, in order to determine whether its reporting obligations are enlivened.

5.9 "Risk of Harm" Thresholds or Standards

As noted above, to meet the legislative threshold necessary to trigger mandatory reporting obligations, a data breach must be "likely to cause serious harm".

The meaning of the phrase "serious harm" is informed by a list of factors set out in Section 26WG of the Privacy Act. Those factors include:

- the kind of information involved;
- the information's sensitivity;
- whether the information is protected by security measures (and, if so, the nature of such security);
- the kinds of persons who might have obtained the information;
- the likelihood of persons who obtain the information having harmful intent towards any persons to whom the information relates; and
- the nature of harm in issue.

6. Ability to Monitor Networks for Cybersecurity

6.1 Cybersecurity Defensive Measures

In general, Australia has no laws that restrict the capacity for network monitoring and taking other defensive cybersecurity measures. The ACSC's "Strategies to Mitigate Cyber Security Incidents" publication sets out a number of recommended measures that involve a monitoring or active defensive component, such email/web content filtering and analysis.

Data Protection in Employment

In the employment context, regulation varies between state and territory jurisdictions. New South Wales is a jurisdiction that regulates such monitoring. The Workplace Surveillance Act 2005 (NSW) stipulates that employees must be given 14 days' notice before surveillance can be conducted at the workplace. Computer surveillance must only be carried out when in compliance with an employer policy of which the employee is aware and understands.

6.2 Intersection of Cybersecurity and Privacy or Data Protection

These issues can give rise to multi-faceted conflicts, which includes the operation of cybersecurity (eg, monitoring) measures in the workplace inevitably involving potential conflict with employee privacy. Though there is no comprehensive or consistent legal position across Australia on this matter, the Commonwealth Fair Work Ombudsman – in seeking to ensure the appropriate balance is struck – recommends that it is best practice for employers to adhere to the APPs and to clearly set out company policy on these matters.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information

Information Sharing under the Telecommunications Act

The Telecommunications Act covers the sharing of cybersecurity information. Under the Act, carriers and carriage service providers have broad obligations relating to the provision of assistance to the government. Specifically, Section 313(3) of the Telecommunications Act requires those entities to provide Commonwealth, state, and territory governments with "such help as is reasonably necessary for" purposes primarily connected to criminal law enforcement, "protecting the public revenue", and protection of national security.

The Telecommunications Act also includes a provision regarding the issuing of technical assistance notices and technical capability notices. These notices can require the communications provider in question to do things such as removing security (eg, encryption) on data, providing technical information, or facilitating access to electronic services.

Information Sharing under the Security of Critical Infrastructure Act (SOCI Act)

The amendments to the SOCI Act in December 2021 included the introduction of compulsory information gathering provisions. The Minister can only utilise this power if cybersecurity event has been triggered, which requires the following conditions to be met (Section 35AB(1)):

- a cybersecurity incident has occurred, is occurring or is imminent;
- that incident has or is likely to have a "relevant impact" on a "critical infrastructure asset"; and
- there is a material risk to social/economic stability, defence or national security of Australia.

If a cybersecurity event is triggered, the Minister of Cybersecurity may authorise the Secretary to issue information gathering directions in relation to the incident and/or impact to the relevant entity for the impacted asset or another specified "critical infrastructure sector asset" (Section 35AB(5)). The Minister must only authorise the issuance of information gathering directions if the Minister is satisfied that the directions "are likely to facilitate a practical and effective response to the incident" (Section 35AB(6)).

Government Information Sharing

In terms of information sharing within government departments and agencies, those entities may authorise the ACSC to carry out "network protection" activities on their behalf. When that occurs, the TIA Act authorises information to be collected by the ACSC as part of the network protection.

The ACSC also has a variety of other information gathering powers, including via ASIO (including action related to the collection of foreign intelligence) and the AFP, such as seeking the sharing of information obtained by warrant.

7.2 Voluntary Information Sharing Opportunities

Voluntary Disclosure to the ACSC

In addition to the legislative arrangements outlined in **7.1 Required or Authorised Sharing of Cybersecurity Information**, voluntary sharing of information remains a major avenue through which the ACSC gathers information. As noted at paragraph 36.40 of the government's 2020

Comprehensive Review of the Legal Framework of the National Intelligence Community, "the ACSC relies on organisations it is assisting to voluntarily provide critical information – such as data samples and log files – that might help uncover the extent of a compromise of their cyber security, or that might assist the ACSC to attribute a cyber security incident to a particular malicious actor".

Telecommunications Act

It is worth noting that, in addition to the technical assistance and capability notices regime noted in **7.1 Required or Authorised Sharing of Cybersecurity Information**, the Telecommunications Act also indemnifies communications providers from civil liability relating to voluntary assistance to, and at the request of, the Director-General of Security, the ASIS, the ASD, the AFP, the ACIC, or any state/territory police force.

8. Significant Cybersecurity and Data Breach Regulatory Enforcement and Litigation

8.1 Regulatory Enforcement or Litigation

RI Advice Litigation

In a major development for the Australian financial market, the Federal Court in Australian Securities and Investments Commission v RI Advice Group Pty Ltd (2022) FCA 496, found that RI Advice breached its Australian financial services licence (AFSL) obligations to act efficiently and fairly when it failed to have adequate risk management systems to manage its cybersecurity risks.

By way of background, between June 2014 and May 2020, a significant number of cyber-incidents occurred at RI Advice's authorised representatives. The incidents resulted in the potential compromise of confidential and sensitive personal information of several thousand clients and other persons.

ASIC successfully argued that the AFSL core obligations under Section 912A of the Corporations Act extended to cybersecurity, and required licensees to have strategies, frameworks, policies and other processes in place "that were adequate to manage risk in respect of cybersecurity and cyber-resilience for itself and across its network of authorised representatives". ASIC demonstrated that RI Advice had not met these obligations.

RI Advice was ordered to engage a cybersecurity expert to identify and implement what, if any, further measures are necessary to adequately manage cybersecurity risks across RI Advice's authorised representative network.

Medibank Class Action

A class action has commenced in the Federal Court against Medibank in respect of a data breach which occurred in October 2022.

The claims against Medibank include allegations of breach of contract, contraventions of the Australian Consumer Law, and breach of equitable obligations of confidence.

Medibank is currently considering whether to seek a stay until the OAIC concludes its investigation into whether Medibank breached its obligations under the Privacy Act.

OAIC Determinations

Over the past 12 months, the OAIC has made eight determinations regarding privacy complaints made against both public and private entities.

For example, in July 2022, the OAIC found that the Civil Aviation Safety Authority (CASA) had contravened the Privacy Act by breaching APP 5. CASA breached Principle 5 by failing to notify or otherwise ensure that the complainant was aware:

- CASA's APP privacy policy contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information (Principle 5.2(g)); and
- CASA's APP privacy policy contains information about how the individual may complain about a breach of the APP, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complain (Principle 5.2(g)).

As an example of a determination concerning a private sector entity, in 16 June 2022, the OAIC held that Serco Group Pty Ltd breached APP 6 (redisclosure of personal information). On two separate occasions, Serco was found to have disclosed the complainant's personal information to a third party without the complainant's consent or prior notification.

8.2 Significant Audits, Investigations or Penalties

Penalties under OAIC Determinations

In respect of the OAIC's determination, as discussed at **8.1 Regulatory Enforcement or Litigation**, regarding CASA's breach of Principle 5, CASA was ordered to send a written apology to the complainant acknowledging the breach of APP 5 within 30 days of receiving the complainant's address (which may be an email address).

In the Serco Group matter referred to at **8.1 Regulatory Enforcement or Litigation**, the OAIC ordered Serco to not repeat or continue this act and pay the complainant AUD2,500 for non-economic loss to the complainant, within 60 days of the complainant notifying Serco of their bank details.

Additionally, the OAIC has reported that, between 2021-22, a total of 14 privacy complaints were resolved. The outcomes included apologies, records being amended, and compensation being paid. Finally, the OAIC also, from time to time, uses enforceable undertakings as a means of ensuring future compliance by erring entities with the Privacy Act.

8.3 Applicable Legal Standards

This is not relevant in this jurisdiction.

8.4 Significant Private Litigation

No significant private litigation has been recently conducted in Australia concerning data security incidents and breaches. It should be noted that, in 2019, the ACCC recommended that the Privacy Act be reformed to introduce a direct right of action for persons against those who are alleged to have interfered with their privacy.

8.5 Class Actions

There is not a great deal of class action litigation activity in Australia concerning alleged data breaches.

Class action litigations concerning the Medibank data breach have begun to unfold, and will continue to develop over the coming year. Following Medibank's data breach in October 2022, the company is now facing four separate class action lawsuits, with Baker McKenzie being the most recent firm to file a class action.

9. Cybersecurity Governance, Assessment and Resiliency

9.1 Corporate Governance Requirements

As detailed in **3. Key Frameworks**, the Australian regulatory framework has a number of mandatory requirements, such as the APP, which establish minimum standards for corporate cybersecurity governance.

The ASIC v RI Group litigation discussed in **8.1 Regulatory Enforcement or Litigation** is likely to see an expansion of ASIC's minimum requirements for corporation's cybersecurity governance and cyber-resilience. It is yet to be seen if the litigation has resulted in an increase in corporations developing comprehensive frameworks that include audits, testing and enhanced resilience to cyber-incidents.

10. Due Diligence

10.1 Processes and Issues

Due diligence processes in Australia involves parties to transactions undertaking a comprehensive assessment of any aspects of the transaction that may have flow-on effects on parties' liabilities and obligations for compliance with the Australian regulatory and legal framework regarding cybersecurity and privacy issues. It is important that this assessment is holistic, covering the following.

- Whether the other parties are APP entities.
- The targeted entities' contemporary (formal and informal) policies and practices in dealings with cybersecurity, data (particularly personal information) and risk management.
- Whether the targeted asset constitutes personal information. This aspect is particularly important for the selling entity's disclosure obligations.
- The targeted entities' public and private history in respect of cybersecurity and privacy issues, and if their response was adequate to any previous breaches. To properly assess this aspect, a proper understanding of the policies and practices of a target entity is necessary (eg, their procedures in identifying, investigating, classifying and handling any potential/actual cybersecurity and privacy issues).
- Whether cybersecurity insurance and professional liability policies are in place for the target company or are otherwise required.

For avoidance of doubt, the above list is not exhaustive.

Additionally, for any foreign or cross-border transactions, Australian parties should also consider the applicability of any other relevant foreign laws (eg, whether the target entity is subject to any international/foreign obligations such as the EU GDPR).

10.2 Public Disclosure

A general obligation of care and diligence is imposed on company directors in the discharge of their duties, under Section 180 of the Corporations Act. Plainly, this would appear to cover taking necessary and adequate steps to protect the company from cybersecurity threats.

Additionally, an organisation that misrepresents its cybersecurity profile may be liable to proceedings for misleading and deceptive conduct under the Australian Consumer Law.

Separately, if an entity holds an Australian financial services or Australian credit licence, a cyber-

security issue may constitute a "reportable situation" and ASIC may need to be notified.

Moreover, companies listed on the Australian Stock Exchange have a continuing obligation of disclosure concerning any information that is reasonably expected to have an effect on the price of their shares: the strength or otherwise of a company's cybersecurity profile would arguably (and, in some circumstances, almost certainly) fit that criterion.

Further, and as detailed in **5. Data Breach or Cybersecurity Event Reporting and Notification**, the occurrence of an eligible data breach can enliven an obligation on the entity in question to make public details of the breach incident.

11. Insurance and Other Cybersecurity Issues

11.1 Further Considerations Regarding Cybersecurity Regulation

In addition to the various international engagements outlined above in the area of cybercrime (eg, **3.4 Key Multinational Relationships** in relation to the Five Eyes alliance), Australia also takes a regional approach to this issue. In particular, the AFP leads a cybercrime awareness programme called Cyber Safety Pasifika, engaging with authorities from Pacific Island nations on the topics of cybercrime and cybersafety.

Cybersecurity insurance, while not mandatory, is taking on a more prominent role in the cybersecurity landscape as the risk of cyberthreats and cybercrime increases. APRA has begun implementing greater regulations and governance regarding general insurers, to ensure the development of secure cyber-insurance practices and accountability. This is a unified step by government agencies to continue developing the government's "cyber-resilience first" approach in tackling cybersecurity threats.

Nyman Gibson Miralis is a market leader in all aspects of general, complex and international criminal law and is widely recognised for its involvement in some of Australia's most significant cases. The firm's team in Sydney has expertise in dealing with complex national and international cybercrime investigations and advising individuals and businesses who are the subject of cybercrime investigations. Its expertise includes dealing with law enforcement requests for information from foreign jurisdictions, challenging potential extradition proceedings as well as advising and appearing in cases where assets have been restrained and confiscated worldwide.

Authors

Dennis Miralis is a partner at Nyman Gibson Miralis and a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional investigations and criminal prosecutions. His areas of expertise include cybercrime investigations, anti-bribery and corruption, global tax investigations, proceeds of crime, anti-money laundering, worldwide freezing orders, national security law, INTERPOL Red Notices, extradition and mutual legal assistance law. In 2021 Dennis was awarded a certificate of completion for the "Cybersecurity: The Intersection of Policy and Technology" Program, January 2021, John F. Kennedy School of Government at Harvard University, Executive Education.

Jasmina Ceic is a partner at Nyman Gibson Miralis and an accomplished criminal trial advocate. She advises and acts in complex criminal law matters at all levels of the court system, with a specialist focus on serious matters that proceed to trial in the superior courts, as well as conviction and sentence appeals heard in the Court of Criminal Appeal. Jasmina works closely with some of Australia's leading barristers and plays a pivotal role in formulating and executing comprehensive trial defence strategies. She has represented persons charged with cybercrime, murder, sexual assault, complex international fraud, transnational money laundering and global drug importation.

Mohamed Naleemudee is a criminal defence lawyer whose practice focuses on domestic and international white-collar crime investigations. Mohamed previously worked for the United Nations Assistance to the Khmer Rouge Trials in Cambodia and is completing a Master's in Public and International Law.

Alexander Leal Smith is a criminal defence lawyer working in the firm's White Collar Crime team. Alex previously worked in the District Court as a Judge's associate and before that as a legal researcher for criminal law barristers

Nyman Gibson Miralis

Level 9
299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Fax: +61 2 9264 9797
Email: contact@ngm.com.au
Web: www.ngm.com.au

Trends and Developments

Contributed by:
Dennis Miralis, Jasmina Ceic, Kalina Ivanov and Jack Dennis
Nyman Gibson Miralis see p.37

Introduction

Australia's cybersecurity and cyber-resilience were existentially threatened over the previous year. The high-profile data breaches of the private entities, Optus and Medibank, raised serious questions about Australia's cybersecurity laws and the government's ability to protect its citizens from malicious actors. These incidents have eroded public trust, which was already low due to the surge of cybercrimes targeting individuals and small businesses and the ineffective government response to these smaller incidents.

The Australian government has taken several steps over the last few months to recover from these breaches. The government's steps to strengthen cybersecurity and develop cyber-resilience remain largely consistent with its three-tier framework, addressing cybersecurity at the national, regional and international level.

An Overview of the Increased Risk of Cyber Threats

Throughout 2022, there was an increase in the number and complexity of cyber threats. Cyber threats' growing presence poses a risk not only against businesses and individuals, but the Australian State itself.

In November 2022, the Australian Cyber Security Centre (ACSC) announced in its Annual Cyber Threat Report 2021-22 that it had received over 76,000 cybercrime reports, which was a 13% increase from the previous financial year. The most frequently reported cybercrimes were online fraud (26.90%), online shopping (14.40%), online banking (12.60%), and investment (12.20%).

The ACSC identified key trends, including the following.

- State warfare–The cyber theatre is featuring more in modern offensive and defensive warfare. Australia continues to be a target of persistent cyber-espionage, which the ACSC states "is often conducted or directed by foreign intelligence services". In response to Russia's invasion of Ukraine, the ACSC in conjunction with the US, Canada, the UK and New Zealand released a joint Cybersecurity Advisory titled "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure".
- Increasing targets – In a similar vein to the above, the ACSC reports that malicious actors are increasingly targeting worldwide, critical infrastructure.
- Common targets – The ACSC also reports that for FY22 cybercrimes directed at individuals remained among the most common, and Business Email Compromise (BEC) trended towards targeting high value transactions (eg, property settlements). The majority of significant incidents reported to the ACSC were from organisations that have a lack of or an insufficient patching (ie, software and operating system updates). Medium-sized businesses (ie, those with 20 to 199 employees) had the highest average loss per cybercrime report where a financial loss occurred.

- Most harm – Notwithstanding that ransomware only constituted 0.59% of reported cybercrime in FY22, the ACSC assessed that it "remains the most destructive cybercrime threat" because of its dual impact on victim organisations (ie, disruption and reputational damage) and disruption to the wider customer base.
- Sector analysis – Acknowledging that government sectors have additional reporting obligations, the ACSC disclosed that the sectors reporting the highest number of cybersecurity incidents during FY22 included the Commonwealth government (24%); State/territory/local governments (10%); the health care and social assistance sectors (9%); and the information, media and telecommunications sector (8%).

High-Profile Incidents

Optus data breach

In September 2022, telecommunication provider Singtel Optus Pty Limited (Optus) announced that it was the victim of a cyber-attack. As a result, more than 11 million current and former customer personal details were disclosed.

It was reported that attackers obtained the personal data as Optus' application programming interface (API) was not secured and did not require authorisation or authentication to access customer data. In this instance, any user with knowledge and experience of using devices that connect to an information-exchange network could have accessed information on Optus' API.

Shortly after the cyber-attack, the attackers issued a ransom demand of USD1 million to be paid within seven days to avoid pushing data. Optus did not meet the ransom demand. The attackers then proceeded to publish 10,000 records of data on an online hacking forum, BreachForums. Soon after, the attackers published a post in which they apologised and claimed all the stolen data had been deleted.

Optus advised customers that the exposed information included personal information such as name, date of birth, contact details and specific details of ID documents including driver's licence numbers and passport numbers. However, no financial information or passwords have been accessed.

The Australian Federal Police (AFP) has announced that it was working with overseas law enforcement to identify the offenders behind the attack and to protect the Australian community.

Operation Hurricane was launched to identify the attackers behind the Optus breach and to help shield Australians from identity fraud. The operation was supported by the following:

- the establishment of AFP-led JPC3, which is a joint partnership between law enforcement, the private sector and industry to combat the growing threat of cybercrime;
- co-operation between the AFP and overseas law enforcement, including the FBI; and
- collaboration between the AFP and the Australian Signals Directorate, whose functions include the collection and communication of foreign signals intelligence and the prevention and disruption of offshore cybercrime.

Following the cyber-attack, there has been a paradigm shift in viewing the corporation's role as a custodian of personal information on behalf of customers. The Australian Information Commissioner, Angelene Falk, noted that the "regulatory framework need to shift the dial to place more responsibility on organisations who are the

custodians of Australians' data, to prevent and remediate harm to individuals caused through the handling of their personal information".

Medibank cyber-attack

In October 2022, healthcare provider, Medibank Private Pty (Medibank), announced it was a cyber-attack victim. As a result, 200 gigabytes of data from 9.7 million current and former customers were disclosed.

It was reported that the cyber-attack was caused when a user with high-level access to Medibank's systems had their credentials compromised. The information was obtained by one party which subsequently sold the data to a third-party forum. The forum issued a ransom demand of USD10 million to avoid publishing data and removal of data. Medibank did not pay the ransom.

Medibank advised customers that the exposed information included personal information such as name, date of birth, contact details, policy numbers and claims data. The claims data disclosed included location of where medical services were received and codes relating to the diagnosis and procedure. However, no primary identity documents, such as driver's licence, credit card and banking details, have been accessed.

In December 2022, the Office of the Australian Information Commissioner (OAIC) announced that it had commenced an investigation into Medibank's personal information handling practices concerning the cyber-attack. The investigation will assess whether Medibank:

- took reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure; and
- took reasonable steps to implement practices, procedures and systems to ensure compliance with the Australian Privacy Principles.

In November 2022, the Australian Minister for Home Affairs and Cybersecurity, Clare O'Neill, announced that the government was considering laws prohibiting ransom payment. It is unknown where this reform will sit within the legal framework and whether reforms will occur to the Privacy Act or Criminal Code. The government may decide to criminalise the payment of ransom through amending the Corporations Act 2001 (Cth) and Commonwealth Criminal Code by making it an offence to pay ransom. As a result, the company and its directors will be liable if the company commits the offence.

Facial recognition technology scandals

The use of facial recognition technology (FRT) has exponentially increased both globally and in Australia. Financial institutions, telecommunication organisations, international terminations and law enforcement agencies use facial recognition for identity verification.

The issue has come to the fore following a number of incidents in which Australia's largest retailers deployed FRT to profile customers. The retailers cited increased security and targeting theft as reasons for the use of FRT. However, the use of the technology has been halted after public outcry and criticism from civil society groups spurred an OAIC investigation into the retailers' practice.

Civil society groups have been calling upon the Australian Attorney-General to regulate technology urgently, as existing privacy laws do not

capture the threats posed by emerging technology.

The University of Technology Sydney (UTS) Human Technology Institute's report titled "Facial recognition technology: Towards a model law" proposed a model law for FRT. The proposed law aims to "protect against the harmful use of this technology" and "foster innovation for public benefit".

The proposed law would impose obligations on companies developing, distributing, and deploying FRT to adopt assessment processes, provide safeguards and oversight mechanisms, and prohibit the use of FRT in high-risk settings unless certain conditions are satisfied.

The model law also includes the following:

- prohibits police and intelligence agencies from using FRT unless a minimum seriousness threshold is satisfied;
- FRT developers and deployers must complete a human rights risk assessment to assess an FRT application's overall human rights risk level;
- FRT developers and deployers would be required to implement a two-step facial recognition impact assessment process for their FRT application prior to its deployment and use, including a risk assessment declaration and a risk management declaration, and these assessments are required to be registered with the OAIC;
- development of technical standards for FRT;
- empowers the OAIC to regulate FRT; and
- empowers the OAIC to impose civil penalties on FRT developers and deployers if they fail to comply with the requirements of the FRT impact assessment.

The Australian government has not indicated whether FRT reform will be introduced in 2023.

Key Legislative Reforms

Australia has seen a flurry of legislative reforms regarding key data, privacy and cybersecurity regimes in Parliament since the Optus and Medibank data breaches in late 2022.

These reforms have included amendments to the critical infrastructure regime and the telecommunications regime. This follows the Privacy Act 1988 (Cth) (Privacy Act) being supplemented by significant amendments in late 2022. The Privacy Act will likely see further amendments following the release of the Australian Attorney-General's Department's (AG) highly anticipated review of the Act on 16 February 2023.

Development of the critical infrastructure regime

The Security of Critical Infrastructure Act (2018) (SOCI Act), which regulates the critical infrastructure regime, was subject to two substantial amendments in the past two years. This package of legislative amendments involves significant cybersecurity reforms.

The amendments in 2021 expanded the SOCI Act's application to new classes of critical infrastructure (including in communication, data processing and technologies). It also introduced new positive security obligations on owners and operators of critical infrastructure (including extra obligations on systems of national significance). Additionally, it empowered the government to undertake "last resort" type actions to intervene in cyber-incidents against critical infrastructure, and introduced a government assistance scheme.

The amendments in 2022 came into effect on 1 April 2022 and sought to supplement the 2021 amendments. The latest amendment further expanded the scope of the SOCI Act and empowered the Minister for Home Affairs (Minister) to declare critical infrastructure assets as systems of national significance.

Soon thereafter, the Minister finalised the Security of Critical Infrastructure (Application) Rules (SOCI Rules). The SOCI rules introduced an asset register and "responsible entities" have mandatory reporting obligations for cyber security incidents, and from 8 October 2022, they were required to provide information to the Register of Critical Infrastructure Assets.

These amendments have resulted in further obligations on market players and impacted how cyber-incidents are recorded and reported by ACSC.

Telecommunication Act

In the wake of high profile cyber-attacks in Australia during 2022, the Australian government passed amendments to the Telecommunications (Interception and Access) Act 1979. Under this amendment, telecommunications carriers and carriage service providers are allowed to share certain types of customer information with financial services entities and government bodies, if so requested. There are specific safeguards on requests made by financial services, such as that the request must meet certain form and content requirements (eg, in writing) and also be accompanied by a written commitment to the Australian Competition and Consumer Commission about the dealings with the requested information.

These changes are intended to allow telecommunications carriers and carriage service providers to liaise with financial services entities and government bodies where there are legitimate circumstances that require disclosure in the public interest, for example, to better protect their customers in the event of any future cyber-attacks.

The regulations contain sunset clauses of 12 months. Therefore, they are expected to automatically repeal on 12 October 2023.

Privacy Act–enforcement

On 13 December 2022, the Privacy Act's amendments came into force.

A major amendment is that the Privacy Act's extraterritorial scope is extended by the addition of an "Australian link". Previously, for an overseas business to be caught within the scope of the Privacy Act, the business would need to carry on a business in Australia (or external territory) and collect/hold personal information in Australia (or an external territory). This second requirement has been removed. Now, broadly put, an entity will have an "Australian link" if it was formed in Australia, has its central management and control in Australia, or is otherwise carrying on a business in Australia.

This amendment to the extraterritorial scope of the Privacy Act in itself strengthens the investigatory and enforcement powers of the OAIC. However, the Enforcement Act also provides new and enhances existing powers of OAIC in respect of information-gathering (eg, the OAIC Commissioner may request information from an APP entity about an actual/suspended eligible data breach and conduct assessment of entities' compliance) and enforcement methods (eg, require persons to engage independent advisers to review complaints). It also introduced new information-sharing powers for OAIC and the

Australian Communications and Media Authority (ACMA), to increase the efficiency and effectiveness of cross border cooperation. Finally, the Enforcement Act also increased the maximum penalties for serious or repeated breaches.

Privacy Act–Towards a GDPR-inspired approach

The AG's "Privacy Act Review Report" (Report), which includes 116 recommendations under 30 areas, proposes significant reform to the treatment of individual's privacy and data in Australia. The implementation of these recommendations will bring Australia's legislative framework closer to the European Union's General Data Protection Regulation (GDPR).

The comprehensive document proposes reforms targeting several areas of the Privacy Act, including broadening the scope of who is captured by the Act and their obligations, the data that is protected by the act, the rights of affected individuals, and the powers of the regulator.

Under the reforms, the Privacy Act's remit would expand to include small businesses, if certain conditions are met. Further, new safeguards would be added regarding the use of data by political parties.

The Report proposes several obligations on private and public entities captured by the Privacy Act. A key reform would be the introduction of a positive obligation on captured entities that personal information is to be handled fairly and reasonably. This reform is supplemented by reforms which include entities having to implement privacy risk assessment frameworks, provide individuals greater control over their personal and information and strengthen privacy protections for children and people experiencing vulnerabilities. These steps provide greater protection to individuals while shifting the burden of protecting this information and provision of access to data to the entities themselves.

The Report proposes the introduction of a number of GDPR-inspired rights and protections for individuals. A notable recommendation includes individuals having the right to object to the collection, use or disclosure of information. Further, individuals would have the right to request erasure of personal information and to de-index online search results containing sensitive information, excessive detail or "inaccurate, out-of-date, incomplete, irrelevant, or misleading" information.

The Report also seeks to strengthen the response to breaches of privacy. The reforms are three-pronged, increasing individual's access to legislative remedies, strengthening the Regulator's enforcement powers and improving the reporting scheme. These reforms include introducing criminal charges for certain privacy breaches and strengthening the Notifiable Data Breaches scheme.

The Report has had a limited response due to being released recently. However, the OAIC and civil society groups have praised the Report for taking significant steps to protect individual's data and placing an onus on entities to positively protect information and data. However, there has been some criticism for the Review's failure to remove the exemption for political parties.

International Involvement

International Counter Ransomware Taskforce

Over the last year, Australia has continued to be a key player in the global efforts to strengthen cybersecurity and combat cybercrime. Australia's continued commitment was recently displayed when it was appointed as the Interna-

tional Counter Ransomware Taskforce's (ICRTF) inaugural chair and co-ordinator.

The ICRTF is a multi-state task force that was launched on 23 January 2023 by the International Counter Ransomware Initiative (CRI). The CRI is a United States-led initiative that consists of 37 member states from around the world. The Initiative seeks to enhance international co-operation to combat the growth of ransomware, build cross border and disrupt and defend against malicious cyber actors.

The CRI envisions the ICRTF to combat ransomware by translating research findings and policy discussions into cross-sectoral tools, cyber threat intelligence exchanges and collective best practice guidance for countering ransomware. The ICRTF's cybersecurity projects will be initiated in response to requests for assistance from members, including to support the coordinated disruption of malicious actors. Additionally, the ICRT will act as a medium for CRI and its member-states to connect with industry for defensive and disruptive threat sharing actions.

The CRI and ICRTF will also serve Australia and its member states' geopolitical purposes by demonstrating a united front against states that utilise cyberwarfare and cyber-attacks, or enable groups/individuals that do engage in those acts. The initiative and its taskforce's deterrent effects on state backed cyber-attacks will be keenly followed. If the ICRTF is successful, it will likely drive non-member states to participate in similar initiatives, actively information-share and strengthen their cybersecurity frameworks to protect their national security or economy.

The CRI initially announced the creation of the taskforce and Australia's role as chair during its summit in November 2022. During this announcement, it stressed that the Taskforce was one part of a comprehensive set of initiatives which also included building its member states' capacity to counter illicit finance ransomware, mitigating ransomware actors from using cryptocurrency to garner payment, improving information sharing between the public and private sectors, building co-ordinated cyber capacity, and building programmes to combat ransomware.

The CRI and ICRTF are among several steps that Australia has taken at the international level to contribute to global efforts to strengthen cybersecurity. Australia also continues to be an active member of the Quad Senior Cyber Group (QSCG), which facilitates regular meetings of expert leaders from Australia, India, Japan, and the United States. The QSCG works to guide and expand cybersecurity co-operation. It also aims to strengthen cyber-resilience and critical infrastructure protection in the Indo-Pacific.

At the regional level, Australia's Cyber and Critical Tech Cooperation Program works across the Indo-Pacific to strengthen cyber and critical tech resilience through capacity building projects. The programme is one of Australia's multi-faceted approaches to develop the region's cybersecurity capabilities and resilience. Australia also utilises regional, multi-state and bilateral agreements to capacity-build, develop co-operation and enhance information and intelligence sharing. It is hoped that the efforts at the international level and regional level will consolidate Australia's domestic cybersecurity framework.

Nyman Gibson Miralis is a market leader in all aspects of general, complex and international criminal law and is widely recognised for its involvement in some of Australia's most significant cases. The firm's team in Sydney has expertise in dealing with complex national and international cybercrime investigations and advising individuals and businesses who are the subject of cybercrime investigations. Its expertise includes dealing with law enforcement requests for information from foreign jurisdictions, challenging potential extradition proceedings as well as advising and appearing in cases where assets have been restrained and confiscated worldwide.

Authors

Dennis Miralis is a partner at Nyman Gibson Miralis and a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional investigations and criminal prosecutions. His areas of expertise include cybercrime investigations, anti-bribery and corruption, global tax investigations, proceeds of crime, anti-money laundering, worldwide freezing orders, national security law, INTERPOL Red Notices, extradition and mutual legal assistance law. In 2021 Dennis was awarded a certificate of completion for the "Cybersecurity: The Intersection of Policy and Technology" Program, January 2021, John F. Kennedy School of Government at Harvard University, Executive Education.

Jasmina Ceic is a partner at Nyman Gibson Miralis and an accomplished criminal trial advocate. She advises and acts in complex criminal law matters at all levels of the court system, with a specialist focus on serious matters that proceed to trial in the superior courts, as well as conviction and sentence appeals heard in the Court of Criminal Appeal. Jasmina works closely with Australia's leading barristers and plays a pivotal role in formulating and executing comprehensive trial defence strategies. She has represented persons charged with cybercrime, murder, sexual assault, complex international fraud, transnational money laundering and global drug importation.

Kalina Ivanov is a criminal defence lawyer. Kalina assists the partners in complex international and domestic white collar crime investigations involving the ATO, ASIC, AFP and the CDPP. She completed her practical legal training with Nyman Gibson Miralis and has acquired niche capabilities in white collar defence investigations.

Jack Dennis is a criminal defence lawyer and part of the International White Collar Crime team at Nyman Gibson Miralis, assisting the partners with international and domestic criminal investigations. Jack has significant international, corporate and tax experience gained from working at a top-tier corporate law firm, advising on cross-border transactions and disputes, involving foreign and domestic entities and high net worth individuals, across the software, financial services and crypto industries. Jack's practice also focuses on public international law.

Nyman Gibson Miralis

Level 9
299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Fax: +61 2 9264 9797
Email: contact@ngm.com.au
Web: www.ngm.com.au

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com