AUSTRALIA

Law and Practice

Contributed by:
Dennis Miralis, Jasmina Ceic, Liam MacAndrews and Pranamie Mandalawatta
Nyman Gibson Miralis see p.17

Contents

Contributed by: *Dennis Miralis, Jasmina Ceic, Liam MacAndrews and Pranamie Mandalawatta,* ***Nyman Gibson Miralis***

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 (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 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.

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.

Broadcasting and marketing

Broadcasting is governed under the Broadcasting Services Act 1992 (Cth) (Broadcasting Act) and the Enhancing Online Safety Act 2015 (Cth) (EOSA), which both regulate online content.

Marketing is regulated through prohibition of unsolicited material under the Spam Act 2003 (Cth) (Spam Act) and the Do Not Call Register Act 2006 (Cth) (Do Not Call Register Act).

Corporations, consumers and financial services

Cybersecurity aspects of:

- corporations may be 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).

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 Criminal Code Act 1995 (Cth) (Criminal Code), which provide for a variety of offences with maximum penalties ranging from two years 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 regulatory 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 Investment Commission (ASIC) regulates publicly listed corporations under the Corporations Act any may investigate issues which touch on cybersecurity.

The Australian Prudential Regulatory Authority (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 enforcement actions. 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 Court (FCC) 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.

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 oversee AFP activities; and
- the Inspector-General of Intelligence and Security (IGIS), which oversee 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 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

In December 2018, the UN General Assembly established two parallel processes to consider information security and norms of responsible state behaviour in cyberspace:

- the inaugural Open Ended Working Group on Developments in the Field of ICTs (OEWG), which is mandated to consider the application of international law, rules and norms to the behaviour of states in cyberspace and to discuss cyberthreats and response measures; and
- the sixth Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (UNGGE), which is the latest UN-mandated working group in the field of information security.

The OWEG is open to all UN member states and the UNGGE comprise of cyber-experts from 25 UN member states. Australia is currently participating in both of these processes.

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.

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 also been participating in the development of a Second Additional Protocol to the Budapest Convention dealing with trans-border access to information. This Protocol will further detail co-operation requirements between state parties on cybercrime information sharing.

1.5 Information Sharing Organisations

Data Protection

The OAIC work 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 over 200 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 rely 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.

There are also some key differences between the two systems. The GDPR is broader in scope, provides for 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

In 2020, the following key privacy proceedings were commenced.

On 9 March 2020, the OAIC commenced Federal Court proceedings against Facebook for repeated breaches of the Privacy Act in relation to the Cambridge Analytica Scandal, which saw the personal information of over 311,000 Australians disclosed to a third-party application; this case is the first privacy enforcement process of this kind in Australia and may pave the way for further privacy class actions.

In April 2020, a mass complaint was lodged with the OAIC against Optus, one of Australia's largest telecommunications companies, for breach of the Privacy Act; the complaint concerns the mistaken disclosure of customer data by Optus and is ongoing.

Further details on significant privacy proceedings are at **8.1 Regulatory Enforcement or Litigation**.

Cybersecurity Proceedings

In August 2020, ASIC commenced actions against RI Advice Group Pty Ltd (RI), a financial advisory company, for breach of Section 912A of Corporations Act, which requires corporations holding financial licences to have adequate risk management systems in place. ASIC has commenced proceedings on the basis that RI failed to implement adequate cybersecurity measures to prevent a series of cyber-attacks against the company's systems. This is the first time that ASIC has undertaken action against a corporation for inadequate cybersecurity.

Australia's 2020 Cyber Security Strategy

In August 2020, the Australian government released its 2020 Cyber Security Strategy (Cyber Strategy). The Cyber Strategy outlines actions required from government, businesses, and the community to improve cybersecurity and combat cybercrime.

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.

Data Protection and the Privacy Act

In 2019, the Australian Government announced that it will be pursuing major changes to the Privacy Act, including expanded powers for the OAIC and harsher penalties for misuse of personal information. In November 2020, the Australian Attorney-General's Department commenced a review of the Privacy Act to consider ways in which the law could be further updated to account for technological changes, strengthen privacy protections and to streamline compliance. This review will likely result in significant reform to Australia's privacy framework.

Cybersecurity and the SOCI Act

In December 2020, the Security Legislation Amendment (Critical Infrastructure) Bill 2020 was introduced to federal parliament and proposes to:

- expand the application of the SOCI Act to new classes of critical infrastructure, including in communication, data processing and technologies;
- impose new positive security obligations on owners and operators of critical infrastructure, including extra obligations on systems of national significance; and
- empower government to undertake "last-resort" type actions to intervene in cyber-incidents against critical infrastructure.

Cybercrime Reforms

US Clarifying Lawful Overseas Use of Data Act (CLOUD Act)

Australia is negotiating a bilateral crime co-operation agreement under the CLOUD Act, which will enable law enforcement and national security agencies from Australia and the USA to request certain communications data directly from private communication providers for law enforcement purposes.

The Telecommunications Legislation Amendment (International Production Orders) Bill, which was introduced to the

Australian federal parliament in March 2020, seeks to establish a domestic framework to facilitate agreements of this kind. If passed, the Bill will amend the TIA Act to enable Australian law enforcement agencies to issue international production orders directly to designated service providers in foreign countries for the purpose of investigating certain crimes including cybercrime.

Disruption warrants

In December 2020, the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 was introduced to federal parliament. If passed it will enable the AFP and ACIC to apply for disruption warrants, network activity warrants and account takeover warrants. These warrants will 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.

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. 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 and is detailed at **3.3 Legal Requirements**.

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 or Breach**, **5.2 Data Elements Covered**, **5.3 Systems Covered**, **5.7 Reporting Triggers** and **5.8 "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, which is largely similar to the Privacy Act;
- 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 regulate video surveillance, computer and data monitoring, GPS tracking and the use of listening devices on individuals.

Cybersecurity

Critical infrastructure

The SOCI Act currently regulates assets in the gas, electricity, water and ports sectors 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 empowers the Secretary of DoHA with an information-gathering power and the HA Minister with a directions power.

Part 5-1A of the TIA Act obliges Australian telecommunication service providers to collect and retain certain types of data for a minimum of two years 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 the internet and content services in Australia and prohibits offensive and illegal content.

The EOSA establishes complaint systems for cyberbullying of children and for non-consensual sharing of intimate images.

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, including in relation 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 and child abuse material and have maximum penalties ranging from one to 30 years imprisonment.

Part 10.7 of the Code deals with serious and other 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.

Other offences

Organisations should note that in addition to the Code:

- the TIA Act also makes it a federal offence for an individual to 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 2000 penalty units (approximately AUD444,000) or fines of up to AUD2.1 million (which may soon be increased to AUD10 million under privacy reforms).

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 50 penalty units (AUD11,100) or fines of up to AUD10,500 per day of contravention.

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, they 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 delivers information sharing 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.
- 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

DoHA is the lead cyberpolicy agency. DOHA develops cybersecurity and cybercrime law and policy, implements Australia's National Cyber Security Strategy and responds to international and domestic cybersecurity threats and opportunities, including in the areas of critical infrastructure and emerging technologies. DoHA also has responsibility for cybersecurity and cybercrime operational agencies including the AFP, ACIC, AUSTRAC and ASIO.

ASD

ASD is Australia's operational lead on cybersecurity and plays both a signals intelligence and information security role. 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. 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 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), which 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 the Privacy and Personal Information Protection Act 1998 (NSW) and Health Records and Information Privacy Act 2002 (NSW).
- 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 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, ACCC and APRA:

AISC, 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, 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, which regulates entities in the banking, insurance and superannuation sector, issued legal standards for information security under CPS 234 in 2019 (detailed in **3.3 Legal Requirements**).

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 (Archives Act) and TIA Act when creating standards for the collection, use and storage of particular information.

De facto standards

The OAIC's Privacy 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 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 2021.

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 cyberstrategies; 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**).

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

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 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 or Breach**, **5.2 Data Elements Covered**, **5.3 Systems Covered**, **5.7 Reporting Triggers** and **5.8 "Risk of Harm" Thresholds or Standards**).

Cybersecurity and the Cyber Strategy

In the 2020 Cyber Strategy, the Australian government has signalled that it will work with industry and businesses to develop legally binding minimum cybersecurity standards for

organisations generally. The 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 Sub Group. This group developed the APEC Privacy framework and meet biannually to discuss privacy issues.

Cybersecurity

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 practices 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**), 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**, 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.

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.

In July 2020, CDR rules were provided for the banking sector, which outline 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.

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 by:

- regularly monitoring and patching IT and website security systems;
- using a Content Delivery Network (CDN) or DDoS mitigation provider;
- safeguarding the entities "origin servers";
- running online services on separate infrastructure to critical systems; and
- having DoS-specific incident response plans.

4.5 IoT, 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

Under the 2020 Cyber Strategy, the government has proposed to develop a voluntary code of practice with 13 principles setting out the government's expectations for IoT consumer devices. The ACSC will seek to provide associated guidance on this code. The government has indicated that if a voluntary process is insufficient, additional regulation may be considered.

Supply Chain

In June 2019, ASD, in consultation with industry and government, developed the "Cyber Supply Chain Risk Management Practitioners guide", which provides technical guidance on key cybersecurity issues.

Furthermore, in the 2020 Cyber Strategy the government has proposed 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 to collaborate with businesses and industry to ensure that security is built into digital products, services and supply chains; and
- encouraging large businesses to share cybersecurity information and tools with small businesses.

5. Data Breach Reporting and Notification

5.1 Definition of Data Security Incident or Breach

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 where a reasonable person would conclude that unauthorised access to/disclosure of 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.

5.2 Data Elements Covered

The types of data covered by the NDB scheme, described immediately above, 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, eg, 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

My Health Records Act

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 generally would be personal information and would be covered by the NDB scheme detailed in **5.1 Definition of Data Security Incident or Breach** 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 or Breach** and **5.2 Data Elements Covered**.

5.6 Security Requirements for IoT

As noted above in the response to **4.5 IoT, Supply Chain, Other Data or Systems**, the Australian government's 2020 Cyber Strategy contains a proposal for a voluntary code of practice concerning IoT devices. Additionally, the government has indicated that it will establish a 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 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.

5.8 "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;
- 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. In fact, the ACSC's "Strategies to Mitigate Cyber Security Incidents" publication sets out a number of recommended measures (such as email/web content filtering and analysis, controlling removable storage media, etc) that involve a monitoring or active defensive component.

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 where done in

compliance with an employer policy of which the employee is aware and understands.

6.2 Intersection of Cybersecurity and Privacy or Data Protection

Although these issues can give rise to multi-faceted conflicts, two will be focussed upon here.

First, the operation of cybersecurity (eg, monitoring) measures in the workplace inevitably involves potential conflict with employee privacy. Whilst (as noted above) 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 the clearly set out company policy on these matters.

Second, relatively recent amendments to the Australian cybersecurity (and enforcement) legislative regime, through the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth) – whereby the government is able to force carriage service providers, for law enforcement purposes, to intercept and decrypt communications – were the subject of some public debate and controversy. In public consultation that preceded the enactment of this legislation, numerous submitters raised concerns about the implications of this (at that time) prospective law on individual privacy rights, due to the scope and extent of the powers it confers on law enforcement relating to the access and use of data.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information

Information Sharing under the Telecommunications Act

The Telecommunications Act contains broad obligations on carriers and carriage service providers 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. Plainly, this covers the sharing of cybersecurity information.

Other, more specific, requirements for provision of information include the issuing of technical assistance notices and technical capability notices under the Telecommunications Act (see **6.2 Intersection of Cybersecurity and Privacy or Data Protection** regarding the relevant legislative amendments). These notices can require the communications provider in question to do things such as removing security (eg, encryption) on particular data, providing technical information, or facilitating access to electronic services.

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 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 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 the Government's 2019 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

Facebook Litigation

In the past year, the most significant litigation involving the OAIC has been the commencement, in March 2020, of proceedings

in the Federal Court of Australia against Facebook resulting from the widely publicised Cambridge Analytica scandal. The OAIC has alleged that Facebook's Irish and American-based corporate entities committed "serious and repeated" breaches of Australian privacy law. In September 2020, the Federal Court dismissed Facebook Inc's application to disallow the OAIC's service of documents on a foreign company. The OAIC alleges that Facebook obtained and disseminated information from users of the platform whose "friends" installed a "This is Your Digital Life" app, despite most of those affected persons not installing the app themselves. The OAIC has further alleged that the information was sold for the use of political consulting firm, Cambridge Analytica. The litigation remains ongoing.

OAIC Determinations

Additionally, over the past 12 months, the OAIC has made numerous determinations of privacy complaints made against both public and private entities.

For example, in January 2021, the OAIC found that the DoHA had breached the Privacy Act with respect to over 9,000 individuals by mistakenly publicly releasing a spreadsheet in 2014, as part of a Detention Report, containing personal information of individuals then in immigration detention. The OIAC held that DoHA failed to put in place reasonable security safeguards in respect of personal information, and engaged in an unauthorised disclosure of personal information.

As an example of a determination concerning a private sector entity, in December 2020, the OAIC held that AustralianSuper Pty Ltd breached APPs 6 (re disclosure of personal information), 10.2 (failing to ensure use of accurate and up-to-date personal information), and 11.1 (failing to protect personal information from unauthorised use and disclosure). AustralianSuper had disclosed the complainant's personal information to former lawyers for the complainant in respect of an insurance claim, even though prior to doing so the complainant had informed AustralianSuper that those lawyers were no longer authorised to act for them.

During the preceding year, the OAIC also made a further 11 determinations of privacy complaints, finding breaches of the Privacy Act had occurred in each instance.

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 DoHA's unlawful disclosure of the personal information of persons in immigration detention, DoHA was ordered to apologise, and pay compensation to members of the class who had provided evidence and submissions as to loss suffered as a result of the wrongful disclosure of their information.

In the AustralianSuper matter referred to at **8.1 Regulatory Enforcement or Litigation**, the OAIC ordered an apology, the engagement of an independent auditor to assess relevant company procedures, corresponding with the OAIC regarding outcomes of the auditor's report, and compensation of AUD4,500 for the complainant.

Additionally, the OAIC has reported that, in 2020, a total of ten privacy complaints were resolved. The outcomes included apologies, records being amended, and compensation being paid.

Finally, whilst the OAIC also, from time to time, uses enforceable undertakings as a means of ensuring future compliance by erring entities with the Privacy Act, no such undertakings were given in the past year.

8.3 Applicable Legal Standards

Facebook Litigation

In the ongoing litigation against Facebook, detailed at **8.1 Regulatory Enforcement or Litigation**, the OAIC has asserted breaches of:

- APP 6 (concerning disclosure of personal information for a purpose other than that for which it was collected); and
- APP 11 (failure to take reasonable steps to protect personal information from unauthorised disclosure).

The OAIC has alleged that Facebook's actions concern a serious and repeated interference with privacy, a legal standard that (if proved) would attract a more severe penalty. It is understood that a live issue in the case is whether Facebook was carrying on business in Australia and holding personal information in Australia, which must be satisfied in order for the Privacy Act to apply to Facebook.

The OAIC's privacy determinations are made with reference to the APPs, specifically those principles that the applicant in each matter claims have been breached.

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. The introduction of such a private right would no doubt increase the instances of private litigation on this topic.

8.5 Class Actions

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

One recent example was a class action brought by approximately 100 New South Wales Ambulance workers on the basis of the Ambulance Service permitting access to health information concerning those workers. Rather than relying on the Privacy Act, this action was brought primarily in tort. Ultimately, the proceedings resolved in December 2019, with a settlement approved by the New South Wales Supreme Court.

Another example of class action litigation was the proceedings detailed at **8.1 Regulatory Enforcement or Litigation**, brought on behalf of over 9,000 individuals formerly in immigration detention, which led to a determination by the OAIC that DoHA had breached the Privacy Act. Rather than being a classic "class action", these proceedings were agitated through a "representative complainant" of the class.

9. Due Diligence

9.1 Processes and Issues

Due diligence processes should involve steps concerning technical assessments of the integrity or otherwise of cybersecurity features of the transaction's subject.

From a legal perspective, it is critical that parties to such transactions undertake a comprehensive assessment of whether the other party/ies is/are an APP entity, and therefore determine the flow-on effects for compliance with the Australian regulatory and legal framework regarding privacy issues.

9.2 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.

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 above in **5 Data Breach 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.

10. Other Cybersecurity Issues

10.1 Further Considerations Regarding Cybersecurity Regulation

In addition to the various international engagements outlined above in the area of cybercrime (see, for example, **1.8 Significant Pending Changes, Hot Topics and Issues** in relation to the US CLOUD Act and **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.

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. Its lawyers are experts in assisting companies and individuals who are the subject of cybercrime investigations. The investigation and prosecution of cybercrime is becoming increasingly international. Individuals and businesses may therefore become the subject of parallel criminal investigations and prosecutions, raising complex jurisdictional and procedural issues. The firm's team in Sydney has expertise in dealing with complex national and international cybercrime investigations and advising individuals and businesses of defence strategies that consider the global nature of cybercrime. It's 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 senior associate 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.

Liam MacAndrews is a senior lawyer who represents and advises clients on cross-border issues, including multi-jurisdictional cases. He has experience advising and representing clients in complex cybercrime investigations, white-collar crime matters, extradition, mutual legal assistance and INTERPOL cases. Liam liaises regularly with Australian and international criminal law enforcement agencies, and his matters have spanned countries throughout Asia, Europe, and North America. Prior to joining Nyman Gibson Miralis, Liam worked in international criminal law at the United Nations-backed Extraordinary Chambers in the Courts of Cambodia.

Pranamie Mandalawatta is an international criminal lawyer whose practice focuses on complex cross-jurisdictional matters, including financial crimes investigated by multi-agency taskforces involving the ATO, the ACIC, foreign regulators and global law enforcement agencies. She is experienced in all aspects of international criminal law – including cybercrime, extradition and mutual legal assistance – and national and international security law (including espionage and foreign influence). As a former senior legal adviser to the Federal Government of Australia within the Office of International Law, Pranamie is equipped to provide strategic advice to states, international organisations, multinational corporations and foreign public officials on international cyberlaw and other areas of international criminal law.

Nyman Gibson Miralis

Level 9
299 Elizabeth Street
Sydney NSW 2000

Tel: +61 2 9264 8884
Fax: (02) 9264 9797
Email: contact@ngm.com.au
Web: www.ngm.com.au