International
Comparative
Legal Guides

Cybersecurity

2024

Sixth Edition

Contributing Editor:
Edward R. McNicholas
Ropes & Gray LLP

glg Global Legal Group

Expert Analysis Chapters

Q&A Chapters

Australia


Dennis Miralis


Jasmina Ceic


Mohamed Naleemudeen

Nyman Gibson Miralis

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction: hacking; denial-of-service attacks; phishing; infection of IT systems with malware; distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime; possession or use of hardware, software or other tools used to commit cybercrime; identity theft or identity fraud; electronic theft; unsolicited penetration testing; or any other activity adversely affecting or threatening the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

In Australia, unauthorised access to computer systems is criminalised by both State and Federal legislation. In the Federal jurisdiction, hacking is criminalised under the *Criminal Code Act 1995* (Cth) ('**Criminal Code**'). Most commonly, persons suspected of engaging in cybercrime are charged pursuant to the Criminal Code, given its universal application in all States and Territories in Australia.

Persons suspected of unauthorised access to computer systems are charged pursuant to section 478.1 of the Criminal Code, which provides for the offence of 'Unauthorised access to, or modification of, restricted data'. The offence comprises of three elements. The first element is 'a person causes any unauthorised access to, or modification of, restricted data'. The second element is 'the person intends to cause the access or modification'. The third element is 'the person knows that the access or modification is unauthorised'. The maximum penalty for a contravention of section 478.1 of the Criminal Code is two years' imprisonment. For the purposes of this offence, 'restricted data' means data held in a computer to which access is restricted by an access control system associated with a function of the computer.

Part 6 of the New South Wales' ('**NSW**') *Crimes Act 1900* (NSW) ('**NSW Crimes Act**') is an example of state-based legislation in Australia that criminalises the hacking of private computer systems. Part 6 of the NSW Crimes Act relates to 'Computer Offences' and sets out multiple offences pertaining to unauthorised access, modification, or impairment of restricted data and electronic communications.

Denial-of-service attacks

Denial-of-service attacks ('**DoS attacks**') or distributed denial-of-service attacks ('**DDoS attacks**') are criminalised by section 477.3 of the Criminal Code, which provides for the offence of 'Unauthorised impairment of electronic communication'.

This offence comprises of two elements. The first element is 'a person causes any unauthorised impairment of electronic communication to or from a computer'. The second element is 'the person knows that the impairment is unauthorised'. The maximum penalty for a contravention of section 477.3 of the Criminal Code is 10 years' imprisonment.

Phishing

Phishing is a form of online fraud that is criminalised by the Criminal Code in instances where the victim is said to be a Commonwealth entity. When the victim is a member of the public, charges are brought under parallel State or Territory legislation. In NSW, charges could be brought under section 192E of the NSW Crimes Act, which criminalises the general offence of fraud.

Prosecutions for Commonwealth fraud could encompass a wide variety of offending conduct, including phishing-style offences that would affect a Federal government body. The following charges are available depending on the financial gain or loss suffered after the activity:

- Section 134.2(1) – obtaining a financial advantage by deception.
- Section 135.1(1) – general dishonesty – obtaining a gain.
- Section 135.1(3) – general dishonesty – causing a loss.
- Section 135.1(5) – general dishonesty – causing a loss to another.

For the charge to be proven, the prosecution must establish that the accused obtains or causes a financial advantage, gain or loss by way of deception or dishonesty. The maximum penalty for each offence is 10 years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The infection of IT systems with malware is criminalised by section 478.2 of the Criminal Code, which provides for the offence of 'unauthorised impairment of data held on a computer disk etc'.

The offence comprises of three elements. The first element is 'a person causes any unauthorised impairment of the reliability, security or operation of data held on a computer disk, a credit card or another device used to store data by electronic means'. The second element is 'the person intends to cause the impairment'. The third element is 'the person knows that the impairment is unauthorised'. The maximum penalty is two years' imprisonment.

As an example of state-based offences of this nature, such conduct would likely be encompassed by the 'modification or impairment' aspects of Part 6 of the NSW Crimes Act.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime is criminalised by section 478.4 of the Criminal Code, which provides for the offence of 'producing, supplying or obtaining data with intent to commit a computer offence'.

The offence comprises of two elements. The first element is 'a person produces, supplies or obtains data'. The second element is 'the person does so with the intention that the data be used, by the person or another person, in committing an offence against Division 477 of the Criminal Code or facilitating the commission of such an offence'. The maximum penalty for a contravention of section 478.4 of the Criminal Code is three years' imprisonment.

Possession or use of hardware, software or other tools used to commit cybercrime

Possession or use of hardware, software or other tools used to commit cybercrime is criminalised by section 478.3 of the Criminal Code, which provides for the offence of 'possession or control of data with intent to commit a computer offence'.

The offence comprises of two elements. The first element is a 'person has possession or control of data'. The second element is 'the person has that possession or control with the intention that the data be used, by the person or another person, in committing an offence against Division 477 of the Criminal Code or facilitating the commission of such an offence'. The maximum penalty for a contravention of section 478.3 of the Criminal Code is three years' imprisonment.

Examples of state-based offences of this nature are sections 308F and 308G of the NSW Crimes Act.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity crime, namely identity fraud offences, are criminalised by Division 372 of the Criminal Code. Specific acts that are criminalised include dealing in identification information, dealing in identification information that involves use of a carriage service, possession of identification information, and possession of equipment used to make identification information.

The offence of 'Dealing in identification information that involves use of a carriage service' is most relevant to cybercrime. This conduct is criminalised by section 372.1A of the Criminal Code and comprises of four elements. The first element is 'a person deals in identification information'. The second element is 'the person does so using a carriage service'. The third element is 'the person intends that any person will use the identification information to pretend to be, or to pass the user off as, another person (whether living, dead, real or fictitious) for the purpose of committing an offence or facilitating the commission of an offence'. The fourth element is 'the offence is an indictable offence against the law of the Commonwealth, an indictable offence against a law of a State or Territory or a foreign indictable offence'. The maximum penalty is five years' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft is criminalised by section 478.1 of the Criminal Code. This offence is committed if a person modifies restricted data. Modification is defined in the Criminal Code as the alteration or removal of the data held in a computer, or an addition to the data held in a computer. As such, the unauthorised copying of data from a computer would contravene this offence provision.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Penetration testing activity without authority could be captured by section 478.1 of the Criminal Code, which provides for the offence of '[un]authorised access to, or modification of, restricted data'.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Part 10.6 of the Criminal Code creates offences related to telecommunication services. These include offences relating to dishonesty with respect to carriage services and interference with telecommunications.

Additionally, Part 6 of the NSW Crimes Act would likely be an example of state-based legislation that could capture these types of activities.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Extended geographical jurisdiction applies to offences under Part 10.7 of the Criminal Code (Divisions 477 and 478).

A person will not commit offences under that Part unless: the conduct constituting the alleged offence occurs wholly or partly in Australia, or wholly or partly on-board an Australian aircraft or an Australian ship; the conduct constituting the alleged offences occurs wholly outside Australia and a result of the conduct occurs wholly or partly in Australia, or wholly or partly on-board an Australian aircraft or an Australian ship; the conduct constituting the alleged offence occurs wholly outside Australia; at the time of the alleged offence, the person is an Australian citizen or at the time of the alleged offence, the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory; or all of the following conditions are satisfied (i) the alleged offence is an ancillary offence, (ii) the conduct constituting the alleged offence occurs wholly outside Australia, and (iii) the conduct constituting the primary offence to which the ancillary offence relates, or a result of that conduct, occurs or is intended by the person to occur, wholly or partly in Australia or wholly or partly on-board an Australian aircraft or an Australian ship.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Section 16A of the *Crimes Act 1914* (Cth) sets out matters for the Court to consider when sentencing for Federal offences, including offences against the Criminal Code. Matters that will generally mitigate a penalty include the timing of any guilty plea, the offender's character, the offender's prior record, assistance

provided by the offender to the authorities and the offender's prospect of rehabilitation and likelihood of reoffending. In some circumstances, the absence of intent to cause damage or make a financial gain could be taken into account by a sentencing court as a factor of mitigation, if this is not a necessary element of the offence.

A number of the offences particularised above require intent to be proven to establish the charge. For example, a necessary element of section 478.2 of the Criminal Code is that the defendant 'intended to cause the impairment' to the data. It is feasible that a factual scenario could exist where impairment to the data is caused without the necessary intent to cause that impairment or damage. This means the offence would not be established.

Furthermore, a number of the offences particularised above cannot be 'attempted'; they must actually be committed. For example, a person cannot attempt to commit the offence of 'Unauthorised access, modification or impairment with intent to commit a serious offence'.

2 Cybersecurity Laws

2.1 *Applicable Laws*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, trade secret protection laws, data breach notification laws, confidentiality laws, and information security laws, among others.

There are both Federal and state/territory laws relevant or applicable to cybersecurity. Federally, these include the following laws: the *Privacy Act 1988* (Cth) ('**Privacy Act**'); the *Crimes Act 1914* (Cth); the *Security of Critical Infrastructure Act 2018* (Cth) ('**SOCI Act**'); the Criminal Code; the *Telecommunications (Interception and Access) Act 1979* (Cth); the *Corporations Act 2001* (Cth) ('**Corporations Act**'); and the *Freedom of Information Act* 1982. There are also state/territory laws that may be applicable to cybersecurity, including criminal laws (e.g. *Crimes Act 1900* (NSW), section 308H) and privacy legislation relating to accessing and handling certain information (e.g. health records).

As a common law jurisdiction, the Australian legal system also gives significant weight to court decisions distinct from legislation, and there is a relevant equitable doctrine against the misuse of confidential information (see, e.g. *ABC v Lenah Game Meats* (2001) 208 CLR 199).

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The SOCI Act, which commenced on 11 July 2018, seeks to manage national security risks of sabotage, espionage and coercion posed by foreign entities. The Act was implemented in response to technological changes that increased cyber connectivity to critical infrastructure. An object of the Act, set out at section 3(d), includes 'imposing enhanced cybersecurity obligations on relevant entities for systems of national significance in order to improve their preparedness for, and ability to respond to, cybersecurity incidents'.

The Australian Government considers 'the responsibility for ensuring the continuity of operations and the provision of essential services to the Australian economy and community' as being shared 'between owners and operators of critical infrastructure, state and territory governments and the Australian Government'.

In April 2022, the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (Cth) came into effect. This Act expanded the application of the 2018 Act from electricity, gas, water and ports, to also include defence, space, transport, food and groceries, higher education and research, healthcare and medical services, energy, financial services and markets, data storage or processing, water and sewerage, and communication sectors as critical infrastructure sectors.

Under section 30BC of the SOCI Act, if an entity responsible for a critical infrastructure asset becomes aware that a cybersecurity incident has occurred or is occurring, and the incident has had, or is having, a significant impact on the availability of the asset, the entity must report it to the relevant Commonwealth body as soon as practicable, and in any event within 12 hours after the entity becomes aware.

Under section 30BD of the SOCI Act, if an entity responsible for a critical infrastructure asset becomes aware that a cybersecurity incident has occurred, is occurring or is imminent, and the incident has had, is having, or is likely to have, a relevant impact on the asset, the entity must report it to the relevant Commonwealth body as soon as practicable, and in any event within 72 hours after the entity becomes aware.

The relevant Commonwealth body is the Australian Cyber Security Centre ('**ACSC**').

Under section 30CD of the SOCI Act, an entity responsible for a system of national significance must adopt and maintain an incident response plan for cybersecurity incidents.

Under section 30CM of the SOCI Act, an entity responsible for a system of national significance may be required to undertake a cybersecurity exercise, to test the entity's ability and preparedness to appropriately respond to and mitigate the impact of cybersecurity incidents.

Under section 30CU of the SOCI Act, an entity responsible for a system of national significance may be required to undertake a vulnerability assessment in relation to all types of cybersecurity incidents.

At the time of writing, the Australian Government was considering reforming the SOCI Act and related laws in the wake of the high-profile data breaches last year, including expanding the sectors covered to customer data and customer systems. The Australian Government has released two key papers in this respect: the Privacy Act Review Report (16 February 2023); and the 2023–2030 Australian Cyber Security Strategy Discussion Paper (27 February 2023).

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Organisations have both general and specific obligations relating to the risk management of data protection and security under the Applicable Laws. For example, the *Privacy Act* requires the relevant entities to take reasonable steps to protect the security of certain information and to destroy/ensure the de-identification of personal information if no longer needed. There are additional cybersecurity requirements for other types of information (e.g. tax file numbers) and certain sectors (e.g. financial services), such as per the SOCI Act, the Corporations Act and the Prudential Standard CPS 234.

Three key regulators provide guidance on what the general (and specific) obligations entail, being:

- The ACSC is part of the Australian Signals Directorate ('**ASD**') of the Australian Government. The ACSC provides advice and guidance to individuals and families, small and medium business, organisation and critical infrastructure, and government on how to respond to and report cybersecurity incidents.
- The Australian Securities and Investments Commission ('**ASIC**'). The ASIC provides guidance to Australia's integrated corporate markets, financial services and consumer regulator, and organisations through its 'cyber reliance good practices'. The good practices recommend, *inter alia*, periodic reviews of cyber strategy by a board of directors, using cyber resilience as a management tool, for corporate governance to be responsive (i.e. keeping cybersecurity policies and procedures up to date), collaboration and information sharing, third-party risk management and implementing continuous monitoring systems.
- The Office of the Australian Information Commissioner ('**OAIC**'). The OAIC recommends that entities have a data breach response plan that includes a strategy for containing, assessing and managing data breaches and strategies for containing and remediating data breaches.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Two main areas where the Application Laws require actual or potential Incident reporting are under the SOCI Act and the Privacy Act. There are other reporting obligations, as per the Prudential Standard CPS 234.

First, entities responsible for critical infrastructure assets have legislated obligations to report cybersecurity incidents under the SOCI Act. The circumstances in which reporting is triggered are set out above at question 2.2. The entities are required to report the cybersecurity incident to the ACSC within, in some instances, 12 hours. In the report, the entity is to provide the date and time of the incident, identify whether the incident is ongoing, identify what systems are being impacted and identify the type of incident (such as denial of service, unauthorised access to network or device, data exposure, malicious code, ransomware, phishing or scanning).

Second, since February 2018, the *Privacy Act* has required Australian Privacy Principles ('**APP**') entities to, as soon as practicable, provide notice to the OAIC and affected individuals of an 'eligible data breach', where there are reasonable grounds to believe that an 'eligible data breach' has occurred. This process is called the Notifiable Data Breaches Scheme ('**NDB Scheme**').

Eligible data breaches arise when: there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds; this unauthorised disclosure of personal information, or loss of personal information, is likely to result in serious harm to one or more individuals; and the entity has not been able to prevent the likely risk of serious harm with remedial action. Indicators such as malware signatures, observable network vulnerabilities and other 'red-flag' technical characteristics may represent reasonable grounds for an APP entity to form a belief that an eligible data breach has occurred.

The OAIC expects APP entities to conduct a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm.

The notification to the OAIC must include the identity and contact details of the organisation, a description of the data breach, the kinds of information concerned and recommendations about the steps that individuals should take in response to the data breach.

Under the Privacy Act, an APP entity is defined as an 'agency' or 'organisation'. 'Agency' includes a Minister, a department, and most government bodies, whilst 'organisation' means an individual, a body corporate, a partnership, any other unincorporated association or a trust that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

In relation to data breaches, the affected individual must also be notified of an 'eligible data breach', as defined above. The notification must include the identity and contact details of the organisation, a description of the data breach, the kinds of information concerned and recommendations about the steps that individuals should take in response to the data breach.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Certain relevant authorities are introduced in question 2.3 above. Two key regulators are the ACSC and the OAIC.

As discussed above, entities responsible for critical infrastructure assets are required to report to the ACSC, which is part of the ASD of the Australian Government. The ACSC's objective is to improve Australia's cybersecurity by monitoring cyber threats. The ACSC provides advice to individuals, businesses and critical infrastructure operators in relation to cybersecurity.

Entities required to report data breaches report to the OAIC. The OAIC is an independent statutory agency within the Attorney-General's Department. The OAIC has three functions; namely, privacy functions conferred by the *Privacy Act*, freedom of information functions, such as reviewing the decisions made by agencies and Ministers pursuant to the *Freedom of Information Act 1982* (Cth), and government information policy functions conferred by the *Australian Information Commissioner Act 2010* (Cth).

In relation to its privacy functions, the OAIC has the power to commence investigations, conduct privacy performance assessments, request an entity to develop an enforceable code, direct an agency to give the OAIC a privacy impact assessment about a proposed activity or function and recognise external dispute resolution schemes to handle privacy-related complaints.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

A failure to comply with notification obligations can result in the imposition of civil penalties. For example, if an entity responsible for a system of national significance fails to have an incident response plan for cybersecurity incidents, contrary to section 30CD of the SOCI Act, the maximum civil penalty is 200 penalty units (AUD 62,600). A body corporate is subject to a maximum penalty five times the amount listed, therefore making the maximum civil penalty 1,000 penalty units. This is currently a fine of AUD 313,000.

Similarly, a serious or repeated interference with privacy attracts a fine of 2,000 penalty units, currently AUD 626,000. The maximum penalty that a court can order for a body corporate is five times the amount listed in the civil penalty provision, currently a maximum of AUD 3.13 million.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The *Privacy Act* confers a number of additional enforcement powers on the OAIC, including accepting an enforceable undertaking, bringing proceedings to enforce an enforceable undertaking, making a determination, making orders that the APP entity must redress any loss or damage suffered by the complainant and that the complainant is entitled to payment of compensation for such loss or damage, bringing proceedings to enforce a determination, delivering a report to the responsible Minister and seeking an injunction.

From 2014 until the time of writing, the OAIC Commissioner had accepted 11 enforceable undertakings and made 55 determinations of a privacy breach. Most recently, the Commissioner accepted an enforceable undertaking from Marriott International requiring it to, amongst other things, increase its monitoring and assessment protocols relating to its privacy and security risk management. Specific examples of proceedings brought by the OAIC Commissioner under the Privacy Act are those related to Facebook, concerning its alleged role in the Cambridge Analytica breach, which commenced in 2020 (and is therefore subject to an earlier regime and penalties). These are still ongoing.

There has not been any enforcement action reported in relation to the SOCI Act.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems): (i) beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content); (ii) honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data); or (iii) sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)?

Beacons

There are presently no specific laws in Australia that prohibit the use of beacons or near-field communication technology.

Honeypots

There are presently no specific laws in Australia that prohibit the use of honeypot technology or similar autonomous deception measures.

Sinkholes

There are presently no specific laws in Australia that prohibit the use of Sinkhole technology. The malicious use of Sinkhole methods to steer legitimate traffic away from its intended recipient may, however, constitute an offence under section 477.3 of the *Criminal Code*.

Sinkholes can be lawfully used as a defensive practice for research and in reaction to cyber-attacks. In this capacity, Sinkholes are a tool used by both public and private agencies.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber attacks?

There are presently no laws in Australia that prohibit organisations from monitoring or intercepting electronic communications on their networks.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber attacks?

Yes. Under the *Defence Trade Controls Act 2012* (Cth) or *Customs (Prohibited Exports) Regulations 1958* (Cth), if a technology can be used for military purposes or dual-use purpose (military and civilian), then export controls may prevent the technology's exportation from Australia. These export controls intend to prevent the exporting of technology that can be used for developing or producing weapons or goods that are used against Australia's military and security interests.

The technology regulated by the legislation are listed on the Defence and Strategic Goods List ('**DSGL**'). The list generally defines 'Technology' to mean specific information necessary for the 'development', 'production' or 'use' of a product. This information takes the form of 'technical data' or 'technical assistance'. Examples include certain forms of source code, encryption, cryptography and electronic hardware.

4 Specific Sectors

4.1 Do legal requirements and/or market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Cybersecurity laws and market practice vary across different business sectors in Australia. While certain legislation captures various industries, there is no uniform cybersecurity law that applies to all business sectors.

For example, the NDB scheme only requires Australian Government agencies, private sector companies and not-for-profit organisations with an annual turnover of more than AUD 3 million to report data breaches.

4.2 Excluding the requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services, health care, or telecommunications)?

The *Privacy Act*, at part IIIA, specifically regulates the handling of personal information about individuals' activities in relation to consumer credit, including the types of personal information that credit providers can disclose. All credit reporting bodies (defined in sections 6 and 6P as a business that involves collecting, holding, using or disclosing personal information about individuals for the purposes of providing an entity with information about the creditworthiness of an individual) are subject to Part III.

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**').

The *Telecommunications Act 1997* (Cth), at part 13, regulates carriers and carriage service providers in their use and disclosure of personal information. Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (Cth) requires providers of telecommunications services in Australia to collect and retain specific types of data for a minimum period of two years and must comply with the *Privacy Act* in relation to that data.

Further, the SOCI Act was amended in December 2021 to require telecommunication carriers and carriage service providers to report cybersecurity incidents to the ACSC.

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

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

A failure by a company to prevent, mitigate, manage or respond to an Incident may result in breaches of provisions of the Corporations Act. The Corporations Act imposes duties on directors to exercise powers and duties with the care and diligence that a reasonable person would. A director who ignores the real possibility of an Incident may be liable for failing to exercise their duties with care and diligence. This is heavily suggested by such cases as *Australian Securities and Investments Commission v RI Advice Group Pty Limited [2022] FCA 496*, which emphasised that effective cyber risk management is essential to adequate risk management systems.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Presently, the Applicable Laws do not require companies to designate a chief information security officer ('**CISO**'), establish a written Incident response plan or policy, conduct periodic cyber risk assessments or perform penetration tests or vulnerability assessments.

However, as set out above, entities responsible for critical infrastructure assets may be required to have a critical infrastructure risk management programme, report cybersecurity incidents, have an incident response plan, undertake cybersecurity exercises, undertake vulnerability assessments, and so on.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Other than those mentioned in section 2 above, no further specific disclosure is required in relation to cybersecurity risks or Incidents.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Australian common law does not recognise a general right of privacy. The equitable cause of action for breach of confidence may provide a remedy for invasions of privacy. Traditionally, the elements are that information must be confidential, information must have been imparted in circumstances importing an obligation of confidence and there must be an unauthorised use of that information. The current doctrine of breach of confidence does not currently entertain cases of wrongful intrusion, as opposed to cases of wrongful disclosure of confidential information.

The *Privacy Act* regulates the way Commonwealth agencies handle personal information. A person may obtain an injunction in the Federal Circuit Court against a Commonwealth agency that engages in, or proposes to engage in, conduct that is in breach of the *Privacy Act*. An action cannot be brought against an individual acting in their own capacity. A person may apply to the Court for an order that an entity pay compensation for loss or damage suffered by the person if a civil penalty has been made against the entity, or the entity is found guilty of an offence under the *Privacy Act*.

There may be other avenues to bring civil or other private actions in relation to an Incident, such as contractual, a duty of care under common law, equity or statute and as a claim under the Australian Consumer Law.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

Limited relevant civil proceedings or other private actions have been brought by individuals in relation to an Incident under legislative instruments.

Investigations conducted by the OAIC most commonly result in out-of-court outcomes. For example, a joint investigation conducted by the Australian Privacy Commissioner and the Privacy Commissioner of Canada into a highly publicised hacking breach of confidential data held by online adult dating service Ashley Madison resulted in an enforceable undertaking being entered into by the company pursuant to section 33E of the *Privacy Act*.

However, in the wake of the significant data breaches, there has been a spike in civil proceedings, many of which are still on foot. Multiple class action lawsuits have recently commenced on various grounds. For example, one has been filed against Optus for breaches of the Privacy Act, of the Australian Consumer Law, of a duty of care to its customers, and of the customer contracts. A further four class actions have been filed against Medibank (in relation to a different data breach), two of which are consumer class actions, with the other two being shareholder class actions alleging, amongst other things, that Medibank failed to disclose market information relating to alleged deficiencies in its cyber security systems. On an individual-basis, one former customer of Latitude Financial Services Australia recently commenced an action against the firm in June 2023 for AUD 1 million in damages resulting from a data breach, which the OAIC and AFP are still investigating.

In respect of the equitable doctrine of breach of confidence, given its evolution, it is likely such cases may also be forthcoming.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

The High Court in *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 sanctioned the recognition of a tort of invasion of privacy. Judge Hampel in the case of *Doe v ABC* (2007) VCC 281 imposed liability in tort for the invasion of the plaintiff's privacy. Such reasoning may apply to an action in relation to a failure to prevent an Incident.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. Organisations are permitted to take out insurance against Incidents in Australia. This includes breaches of the *Privacy Act*.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations specifically targeted at losses associated with Incidents.

Numerous entities offer insurance for data breaches, business interruptions, email forgery, ransomware attacks, costs of rebuilding an IT system, theft of crypto-currencies and legal fees associated with the investigation of Incidents. Coverage is governed generally by the *Insurance Act 1973* (Cth), the *Insurance Contracts Act 1984* (Cth), the Corporations Act and the common law.

7.3 Are organisations allowed to use insurance to pay ransoms?

There are no specific laws prohibiting organisations from using insurance to pay ransoms.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. anti-terrorism laws) that may be relied upon to investigate an Incident.

Several well-established legal investigatory powers are deployed by law enforcement authorities when investigating an Incident. These powers include the use of search warrants, the seizure of IT equipment for forensic analysis, decryption (whether at encrypted or decrypted data points) and the compulsory examination of suspects in certain circumstances.

Under the *Telecommunications Act 1997* (Cth), the Secretary of the Department of Home Affairs has the power to obtain information and documents from carriers, carriage service providers and carriage service intermediaries – to monitor and investigate their compliance with the security obligation – while, under the *Privacy Act*, the Privacy Commissioner can also initiate an investigation into an Incident on its own initiative or as a result of receiving a complaint.

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

The ASD is responsible for defending Australia from global threats and advancing its national interests by providing foreign signals intelligence, cybersecurity and offensive cyber operations as directed by the Australian Government. One of the express strategic objectives of the ASD is to provide advice and assistance to law enforcement. To this end, the ASD collaborates with the Federal, State and Territory police forces regarding matters of national interest, including emerging areas such as cyberterrorism.

See the answer to question 8.2 below for statutory notices that can be issued by law enforcement agencies to access data held by designated communications providers.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth), law enforcement and intelligence agencies can compel communications providers to provide covert access to data for the purposes of disrupting and investigating criminal activity. The Act also establishes a framework to facilitate lawful assistance from communications providers.

The legislation allows various Australian law enforcement and intelligence agencies to make a Technical Assistance Notice ('TAN'), ordering designated communications providers to provide data or assistance in relation to criminal investigations or matters of security. This may include access to encryption keys or provision of decrypted data. Similarly, a Technical Capability Notice ('TCN') can be issued, mandating that a designated communications provider establish new capability to intercept and decrypt communications that would otherwise be encrypted or inaccessible.

The above notices may be issued in a broad variety of circumstances, including the enforcement of criminal laws and laws imposing pecuniary penalties, either in Australia or in a

foreign country, or if it is in the interests of Australia's national security, Australia's foreign relations, or Australia's national economic wellbeing.

A designated communications provider, including an individual employed or acting on behalf of such providers, who has been compelled to provide data or assistance under a computer access warrant and fails to do so, may face up to 10 years' imprisonment, a fine of up to 600 penalty units (currently AUD 187,800) or both.

Section 3LA of the *Crimes Act 1914* (Cth) also provides law enforcement authorities a mechanism by which a person must provide information or assistance that is reasonable and necessary to allow a constable to:

- access data held in, or accessible from, a computer or data storage device that is on warrant premises or that has been moved to a place for examination under subsection 3K(2) of the *Crimes Act 1914* (Cth);
- copy data held in, or accessible from, a computer or storage device; and
- convert into documentary form, or another form intelligible to a constable, data held in, or accessible from, a computer or data storage device, or data held in a data storage device to which the data was copied, or data held in a data storage device removed from warrant premises under subsection 3L(1A) of the *Crimes Act 1914* (Cth).

Acknowledgments

The authors would like to thank Arman Salehirad and Jack Dennis for their contributions to this chapter.

Dennis Miralis is a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional regulatory investigations and prosecutions. His areas of expertise include cybercrime, global investigations, proceeds of crime, bribery and corruption, anti-money laundering, worldwide freezing orders, national security law, Interpol Red Notices, extradition and mutual legal assistance law. Dennis advises individuals and companies under investigation for economic crimes both locally and internationally. He has extensive experience in dealing with all major Australian and international investigative agencies. Full biography: https://ngm.com.au/our-team/dennis-miralis-partner-defence-lawyer/

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: dm@ngm.com.au
URL: www.ngm.com.au

Jasmina Ceic is 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. She has represented and advised persons and companies being investigated for white-collar and corporate crime, complex international fraud and transnational money laundering. Full biography: https://ngm.com.au/our-team/jasmina-ceic-senior-associate/.

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: jc@ngm.com.au
URL: www.ngm.com.au

Mohamed Naleemudeen is an international criminal lawyer whose practice focuses on domestic and international white-collar crime investigations, sanctions and extraditions. He holds a Master's Degree in Public and International Law from the University of Melbourne. Mohamed previously worked for the United Nations Assistance to the Khmer Rouge Trials in Cambodia.

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: mn@ngm.com.au
URL: www.ngm.com.au

Nyman Gibson Miralis is an international award-winning criminal defence law firm based in Sydney, Australia. For over 50 years it has been leading the market in all aspects of general, complex and international crime, and is widely recognised for its involvement in some of Australia's most significant criminal cases.

Our international law practice focuses on cybercrime, white-collar and corporate crime, transnational financial crime, bribery and corruption, international money laundering, international asset freezing or forfeiture, extradition and mutual legal assistance law.

Nyman Gibson Miralis strategically advises and appears in matters where transnational cross-border investigations and prosecutions are being conducted in parallel jurisdictions, involving some of the largest law enforcement agencies and financial regulators worldwide.

Working with international partners, we have advised and acted in investigations involving the USA, Canada, the UK, the EU, China, Hong Kong, Singapore, Taiwan, Macao, Vietnam, Cambodia, Russia, Mexico, South Korea, the British Virgin Islands, New Zealand and South Africa.

www.ngm.com.au

NYMAN GIBSON MIRALIS
Criminal Defence Lawyers and Advisors est. 1966

International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Cybersecurity 2024 features two expert analysis chapters and 21 Q&A jurisdiction chapters covering key issues, including:

- Cybercrime
- Cybersecurity Laws
- Preventing Attacks
- Specific Sectors
- Corporate Governance
- Litigation
- Insurance
- Investigatory and Police Powers

The International Comparative Legal Guides are published by: glg Global Legal Group