ICLG

The International Comparative Legal Guide to:

Cybersecurity 2019

2nd Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Angara Abello Concepcion Regala & Cruz Law Offices
Bagus Enrico & Partners
Boga & Associates
BTG Legal
Christopher & Lee Ong
Cliffe Dekker Hofmeyr Inc
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Ferchiou & Associés
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.
JIPYONG LLC
King & Wood Mallesons
Latham & Watkins LLP
Lee, Tsai & Partners Attorneys-at-Law
LT42 – The Legal Tech Company
Maples and Calder
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Simmons & Simmons LLP
Siqueira Castro Advogados
Stehlin & Associes
Synch
Templars
USCOV | Attorneys at Law

glg
global legal group

glg
global legal group

Contributing Editors
Nigel Parker & Alexandra Rendell, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Sam Friend

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
October 2018

ISBN 978-1-912509-38-6
ISSN 2515-4206

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Australia

Phillip Gibson

Nyman Gibson Miralis

Dennis Miralis

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? 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 New South Wales, Australia, unauthorised access to computer systems is criminalised by both state and federal legislation, namely, the *Crimes Act 1900* (NSW) ("the Crimes Act") and the Commonwealth Criminal Code ("the Code"). Most commonly, persons suspected of engaging in cybercrime are charged pursuant to the Code, given its universal application in all states and territories in Australia.

Persons suspected of unauthorised access to computer systems are charged pursuant to s. 478.1 of the Code, which provides for the offence of "Unauthorised access to, or modification of, restricted data". The offence is comprised of three elements of proof. The offence is committed if a person causes any unauthorised access to, or modification of, restricted data, the person intends to cause the access or modification and the person knows that the access or modification is unauthorised. The maximum penalty for a contravention of s. 478.1 of the Code is two years' imprisonment.

Denial-of-service attacks

Denial-of-service attacks ("DoS attacks") or Distributed Denial of Service attacks ("DDoS attacks") are criminalised by s. 477.3 of the Code, which provides for the offence of "Unauthorised impairment of electronic communication". The offence is comprised of two elements. The offence is committed if a person causes any unauthorised impairment of electronic communication to or from a computer and the person knows that the impairment is unauthorised. The maximum penalty for a contravention of s. 477.3 of the Code is 10 years' imprisonment.

Phishing

Phishing, being a form of online fraud, is criminalised by both the Crimes Act and the Code. However, enforcement of online fraud is generally left to the law enforcement agency of the state in which the victim of the fraud resides. In New South Wales, fraud is criminalised by s. 192E of the Crimes Act. The offence is comprised of three elements. The offence is committed if a person who, by any deception, dishonestly obtains property belonging to another or obtains any financial disadvantage or causes any financial disadvantage. The maximum penalty 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 s. 478.2 of the Code, which provides for the offence of "Unauthorised impairment of data held on a computer disk etc.". The offence is comprised of three elements. The offence is committed if a person causes any unauthorised impairment of the reliability, security or operation of data held on a computer disk, a credit card, another device used to store data by electronic means, the person intends to cause the impairment and the person knows that the impairment is unauthorised. The maximum penalty is two years' imprisonment.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Possession or use of hardware, software or other tools used to commit cybercrime is criminalised by s. 478.3 of the Code, which provides for the offence of Possession or control of data with intent to commit a computer offence. The offence is comprised of two elements. The offence is committed if a person has possession or control of data and 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 Code or facilitating the commission of such an offence. The maximum penalty for a contravention of s. 478.3 of the Code is three years' imprisonment.

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

Identity crime, and in particular identity fraud offences, are criminalised by Division 372 of the Code. Particular 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. It is criminalised by 372.1A of the Code and is comprised of four elements. The offence is committed if a person deals in identification information, the person does so using a carriage service, 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, and 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 s. 478.1 of the Code. As the offence is committed if a person modifies restricted data, and

modification is defined in the Code as the alteration or removal of the data held in a computer, or an addition of the data held in a computer, the unauthorised copying of data from a computer would contravene the offence provision.

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 Code creates offences related to telecommunication services. They include offences relating to dishonesty with respect to carriage services and interference with telecommunications.

Failure by an organisation to implement cybersecurity measures

See the discussion below in relation to corporate governance.

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

Extended geographical jurisdiction applies to offences under Part 10.7 of the 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; or 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; or the conduct constituting the alleged offence occurs wholly outside Australia and 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: the alleged offence is an ancillary offence; the conduct constituting the alleged offence occurs wholly outside Australia; and 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 actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

In New South Wales, the penalties for criminal offences are prescribed by the *Crimes Sentencing Procedure Act 1999* (NSW). The *Crimes Act 1914* (Cth) prescribes the penalties applicable to breaches of federal legislation, such as the Code. Matters that generally will 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. Notification would be a matter that could be taken into account by a sentencing court as a factor of mitigation.

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".

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

A number of criminal offences may arise in relation to cybersecurity or the occurrence of an Incident, although they are best understood as tangential or ancillary to cybersecurity or the occurrence of an Incident. For example, there have been prosecutions for offences such as blackmail where an offender has used material obtained as a result of a breach of confidence to blackmail the owner by threatening to release that material online.

2 Applicable Laws

2.1 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, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

The following laws in New South Wales relate to cybersecurity: the *Privacy Act* (Cth) ("Privacy Act"); the *Crimes Act 1914* (Cth); the *Security of Critical Infrastructure Act 2018* (Cth); the *Criminal Code 1995* (Cth); and the *Telecommunications (Interception and Access) Act 1979* (Cth).

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The *Security of Critical Infrastructure Act 2018* (Cth), 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 as a response to technological changes that have increased cyber connectivity to critical infrastructure. 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". The Act applies to approximately 165 specific assets in the electricity, gas, water and ports sectors.

The Act establishes a Register of Critical Infrastructure Assets, empowers the Secretary of the Department of Home Affairs with an information-gathering power (whereby certain information can be requested of direct interest holders, responsible entities and operators of critical infrastructure assets) and a Minister directs power that allows the Minister to issue a direction to an owner or operator of critical infrastructure assets to mitigate national security risks.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

See generally the answer to question 4.3 below in respect of the NDB Scheme.

The Australian Securities and Investments Commission ("ASIC") provides guidance to Australia's integrated corporate markets, financial services and consumer regulator, and provides guidance to organisations through its "cyber reliance good practices". The good

practices recommend, *inter alia*, periodic review 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.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

See the answer to question 4.3 below.

2.5 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 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 (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

See the answer to question 4.3 below.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Subject to the restrictions in the Applicable Laws (such as the Privacy Act), organisations are permitted to voluntarily share information related to an Incident or potential Incidents with a regulatory or other authority and other private sector or trade associations.

2.7 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.

See the answer to question 4.3 below.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

See the answer to question 4.3 below.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Office of the Australian Information Commissioner ("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.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

See the answer to question 4.3 below.

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

To date, there have been no published examples of enforcement action taken in cases of non-compliance with the Notifiable Data Breaches ("NDB") Scheme.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practice varies across different business sectors in New South Wales. The NDB Scheme, for example, only requires not-for-profit businesses with an annual turnover of more than AUD $3 million to report data breaches.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Part IIIA of the Privacy Act 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 ss 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.

Part 13 of the Telecommunications Act 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.

See generally the answer to question 4.3 below for more information. The NDB Scheme in Part IIIC of the Privacy Act requires telecommunications and financial services sectors to take steps to secure personal information. These sectors must notify individuals whose personal information is involved in a data breach that is likely to result in serious harm and must also notify the OAIC.

4 Corporate Governance

4.1 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' 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 2001* (Cth). The *Corporations Act 2001* (Cth) 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 duties with care and diligence.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (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 CISO, establish a written Incident response plan or policy, conduct periodic cyber risk assessments and perform penetration tests or vulnerability assessments.

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

In February 2018 the Privacy Amendment (Notifiable Data Breaches) Act 2017 amended the Privacy Act to require 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.

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.

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 and to the affected individual 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 individuals should take in response to the data breach.

A failure to comply with the notification obligations can result in the imposition of substantial civil penalties. A serious or repeated interference with privacy attracts a fine of 2,000 penalty units, currently AUD $420,000.00. 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 $2.1 million.

The Privacy Act also 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, bringing proceedings to enforce a determination, a report to the responsible Minister and seeking an injunction.

Under the Privacy Act, an APP entity is defined as an "agency" or "organisation". "Agency" includes a Minister, a Department, and most government bodies; and an "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.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

The Australian Privacy Principles contained in schedule 1 of the Privacy Act provide for the manner in which APP entities must handle and use personal information. There are 13 privacy principles, covering: open and transparent management of personal information; anonymity and pseudonymity; collection of solicited personal information; dealing with unsolicited personal information; notification of the collection of personal information; the use or disclosure of personal information; direct marketing; cross-border disclosure of personal information; adoption, use or disclosure of government-related identifiers; quality of personal information; security of personal information; access to personal information; and the correction of personal information. The APPs are not prescriptive, and an APP entity must consider how the principles apply to its own situation.

5 Litigation

5.1 Please provide details of any civil 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.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

No relevant civil proceedings have been brought in relation to an Incident. Given the evolution of the doctrine of breach of confidence, it is likely such cases will be forthcoming.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

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 an Incident.

6 Insurance

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

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

6.2 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 limits specifically targeted at losses associated with Incidents. Numerous entities offer insurance for data breach, business interruption, 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 2001* (Cth) and the common law.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

The *Workplace Surveillance Act 2005* (NSW) restricts the use of both overt and covert forms of surveillance of an employee. Surveillance can include computer surveillance. Significant penalties are imposed for breaches of the Act, including imprisonment.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

Whistle-blowers are recognised and protected by the *Corporations Act 2001* (Cth). There are five criteria that must be met when a whistle-blower makes a disclosure in order to be protected by the Act. Firstly, the whistle-blower must be a current office, a current employee or a current contractor (or the employee of a contractor). Secondly, the disclosure must be made to the company's auditor or a member of the company's audit team, a director, secretary or senior manager of the company, a person authorised by the company to receive whistle-blower disclosure or ASIC. Thirdly, the whistle-blower must provide their name to the person or authority to whom the disclosure is made. Fourthly, the whistle-blower must have reasonable grounds to suspect that the information being disclosed on the company or company officer may have breached the *Corporations Act 2001* (Cth) or the *Australian Securities and Investments Commission Act 2001* (Cth). Fifthly, the disclosure must be made in good faith, in that the disclosure must be honest and genuine, and motivated by wanting to disclose misconduct.

The information disclosed by whistle-blowers is protected by ASIC, the whistle-blower is protected by the *Corporations Act 2001* (Cth) from civil or criminal litigation, and the Act also makes it a criminal offence to victimise a whistle-blower.

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. antiterrorism laws) that may be relied upon to investigate an Incident.

A number of well-established legal investigatory powers are deployed by law enforcement authorities when investigating an Incident. These powers can include the issuing 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.

The *Assistance and Access Bill 2018* (Cth), presently up for parliamentary debate, is seeking to expand the investigative powers of law enforcement. For example, the Bill seeks to modernise and strengthen search warrants to "account for the growing complexity of communications devices and the evidential value of data".

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?

Presently, there are no requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities. The Australian government has expressed that it remains "committed to the security of communications services and devices and the privacy of Australians".

Section 3LA of the *Crimes Act 1914* (Cth) 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).

Phillip Gibson
Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney
New South Wales
Australia

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

Phillip Gibson is one of Australia's leading criminal defence lawyers with more than 30 years of experience in all areas of criminal law. Phillip manages and advises on the most complex criminal cases.

Phillip has vast experience in transnational cases across multiple jurisdictions often involving: assets forfeiture; money laundering and proceeds of crime; cybercrime; extradition; mutual assistance; white-collar crime; royal commissions; bribery and corruption; Interpol notices; international and national security law; and matters related to the Independent Commission Against Corruption and the Crime Commission.

Dennis Miralis
Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney
New South Wales
Australia

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

Dennis Miralis is a leading Australian defence lawyer who acts and advises in complex domestic and international criminal law matters in the following areas: white-collar and corporate crime; money laundering; serious fraud; cybercrime; international asset forfeiture; international proceeds of crime law; bribery and corruption law; transnational crime law; extradition law; mutual assistance in criminal law matters; anti-terrorism law; national security law; criminal intelligence law; and encryption law.

He appears in all courts throughout Australia and regularly travels outside Australia for complex international and transnational criminal law matters.

NYMAN GIBSON MIRALIS
Criminal Defence Lawyers and Advisors est. 1966

Nyman Gibson Miralis 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. By its very nature, cybercrime is borderless, and therefore the exposure to penalties outside the jurisdiction where an individual or business is physically located is often a real possibility.

Our criminal lawyers have expertise in dealing with complex national and international cybercrime investigations and advising individuals and businesses of defence strategies that take into account the global nature of cybercrime.

Our 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.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com