# Cybercrime Law in Australia

**21 April 2017**

**Overview**

Emerging new technology involving internet usage, the rapid and broad expansion of devices connected to the internet or Internet of Things (IoT), mean the future scope for potential cybercrime activity is likely to be unparalleled.

What is Australia doing to combat the oncoming threat of cybercrime and what laws are in place to enable prosecution of cyber criminals?

What follows is an outline of cybercrime, types of cybercrime offences and the applicable legislation.

**What is Cybercrime?**

Cybercrime as a legal concept, may be regarded as being in an early developmental stage. Practical implementation of preventative measures are not always simple and legal solutions are sometimes difficult to implement.

The internet is still perceived by many as a frontier, where the players are anonymous, beyond certain jurisdiction and wrong-doers are hard to detect. Often the cyber criminals are located overseas.

**Highlights & Key Points**

- **What is cybercrime?**
- **Increase of the threat to cyber security**
- **Types of cybercrime offences**
- **Applicable laws**
- **Cybercrime Case Law**
- **Additional legislative power**

Without doubt, considerable resources, and the implementation of up to date sophisticated technology, needs to be channeled to increasing the level of cyber security. Effectiveness of policing, convicting and prosecution of offenders needs to be ensured.

**Increase of the threat to Cyber security**

The Australian Institute of Criminology (AIC), the Australian Government's national research and knowledge center on crime and justice, has recognized that the under-reporting of high tech crimes is a growing problem.

Some 10,000 cybercrimes were reported to the Australian Cybercrime Online Reporting Network in 2015-16. It is estimated there were around one million victims of identity theft online last year.

Almost 50% of the industrial organisations that use or plan to use the IoT have experienced security breaches in their industrial applications.

According to the worldwide leader in IT and networking Cisco, the overwhelming majority of business decision makers expect the IoT will cause increase in security threats both in quantity and in severity over the next 2-3 years.

The Australian Cybercrime Online Reporting Network (ACORN), is a national policing initiative that provides advice on how to recognise and avoid cybercrime. ACORN facilitates reporting of

cybercrimes that breach Australian law.

**Types of cybercrime offences**

The Australian Cyber Security Centre (ACSC) was established in 2014. In July 2015, the ACSC released its first public Cyber Security Threat Report, outlining the range of cyber adversaries targeting Australian networks, their motivations, the nature of the attacks and their impact.

Some of the types of offences by way of malicious and criminal cyber activity include the following:

- Internet Fraud, Online Fraud, Email Fraud, Identify theft, Credit Fraud, Computer hacking, Bootlegging and tripping;
- Malware that logs your keystrokes, giving your banking and credit card details to the cyber criminals;
- Phishing communication under disguise of a trustworthy entity in a deceptive electronic communication;
- Ransomware that encrypts your data files while they are still on your computer with the demand of payment of 'ransom' to a criminal to unlock them;
- Bitcoin and Cryptocurrency fraud and seizure;
- Spreading of viruses including Distributed Denial-of-Service attacks using botnets − emails sent with malicious links that unknowingly download viruses; and
- Unauthorised modification, damage and malicious destruction of data.

**Laws applicable to Cybercrime in Australia**

Australia's law enforcement and intelligence agencies are empowered to compel carriers to preserve the communication records of persons suspected of cyber-based crimes.

Australian cybercrime law also extends the geographic reach of the provisions to criminal activity which occurs wholly or partly in Australia, on board an Australian aircraft or ship, and in certain circumstances to the conduct of Australian nationals abroad.

The scope of Cybercrime has become international, and practically borderless. Exposure to penalties outside the jurisdiction where an individual or business is physically located is a real possibility.

In April 2016 the Australian Prime Minister, in his forward to the nation's Cyber Security Strategy, wrote: "…cyberspace cannot be allowed to become a lawless domain."

**National level**

In respect to high tech crime or cybercrime of national significance, the responsibility of investigation and response is with the Australian Federal Police (AFP). They also have jurisdiction over cybercrimes involving online fraud affecting a government department. In addition AFP jurisdiction extends to the investigation of crimes associated with online child sex exploitation, child protection and tourist child sex offenders.

The Director of Public Prosecutions prosecute offences relating to unauthorised access to data, impairment of electronic communication and using carriage service to harass or cause offence, within sections 478.1(1), 477.3(1) and 474.17 of the *Criminal Code (Cth)*. State or Territory offences are prosecuted by the corresponding state Director of Public Prosecutions.

**State law**

The NSW Police also have jurisdiction to investigate and prosecute online fraud including internet banking, mobile banking, phishing, mule recruitment, shopping and auction site fraud, scams, spam and identity theft, child sexual exploitation and cyber bullying offences.

The following particular provisions of *Crimes Act 1900* (NSW) are relevant to cybercrime at NSW state level*:*

- s91H: Production, dissemination or possession of child abuse material;
- s91K: Filming a person engaged in private act;
- s91L: Filming a person's private parts;
- s91M: Installing device to facilitate observation or filming;
- s192E: Fraud (including online fraud);
- s192J: Dealing with identification information;
- s192K: Possession of identification information;
- s308C: Unauthorised access, modification or impairment with intent to commit serious indictable offence;
- s308D: Unauthorised modification of data with intent to cause impairment;
- s308E: Unauthorised impairment of electronic communication;
- s308F: Possession of data with intent to commit serious computer offence;
- s308G: Producing, supplying or obtaining data with intent to commit serious computer offence;
- s308H: Unauthorised access to or modification of restricted data held in computer (summary offence); and
- s308I: Unauthorised impairment of data held in computer disk, credit card or other device (summary offence).

In addition, *Surveillance Devices Act 2007* (NSW) provision s7 provides a prohibition on

installation, use and maintenance of listening devices.

Cyber bullying has become prevalent in our society in recent times. The *Crimes (Domestic and Personal Violence) Act 2007* (NSW) relevant provision is s13: Stalking or intimidation with intent to cause fear of physical or mental harm (Bullying)

**Federal law**

In the Federal sphere the law is codified by *Criminal Code Act 1995* (Cth) which was amended in 2001 by the *Cybercrime Act 2001(Cth)*

The particular provisions of the Cybercrime Act criminalise activities such as computer hacking, denial of service attacks, spreading computer viruses and interfering with websites, regulate these offences and provide remedies to victims. Cyber related offences replacing those previously found in the Crimes Act are noted in the first Schedule to the Act:

(1) Unauthorised access to or modification of data stored in a computer with intent to commit a serious offence;

(2) Unauthorised impairment of electronic communication to or from a computer with intent to commit a serious offence;

(3) Unauthorised modification of data to cause impairment;

(4) Unauthorised impairment of an electronic communication;

(5) Unauthorised access to, or modification of restricted data (i.e., data protected by a password or other security feature), where the restricted data is either held for or on behalf of the Commonwealth or the access to or modification of it is caused by means of a telecommunications service;

(6) Unauthorised impairment of data held on a computer disk etc;

(7) Possession or control of data with intent to commit a computer offence;

(8) Producing, supplying or obtaining data with intent to commit a computer offence.

**Cybercrime Case Law**

A recent cybercrime case before the Supreme Court of ACT in respect to Australia's national security interests: Department of Defence graduate employee, 24-year-old Michael Scerba was convicted and sentenced to a maximum of 12 months imprisonment for disclosing secret organisation information online under section 70(1) of the ACT Crimes Act 1914.

Scerba downloaded a classified sensitive document from the Australian Defence Secret Network. He downloaded the secret 15-page document, burnt it to a disc, took it home, and posted two pages to an online forum.

Subsequently, the two pages were deleted. However several people had viewed and commented on the post but the total number who had accessed the sensitive information was undisclosed.

In handing down the sentence on 5 November 2015, the ACT Supreme Court accepted that Scerba had not intended to compromise national security, although he knew the disclosure could cause harm. The court further stated found Scerba had displayed a level of planning and detail, and attempted to avoid detection.

**Additional legislative power**

The *Cybercrime Act 2001* also introduced law enforcement powers relating to the search and seizure of electronically stored data. These powers allow officers to copy data, to access data that is not physically at the warrant premises, to uplift and move equipment if it is reasonably believed that the equipment contains or constitutes evidential material.

IT security industry service providers need to be aware of the abovementioned provisions so as not to get caught by a technical breach. For example IT security personnel may be in possession of technology and tools which can used for hacking activities, notwithstanding that they may be used for legitimate security purposes. IT security providers must be very careful in the allocation of such technology to staff and their usage should be controlled. It has been proposed that some of the above offences could be established regardless of whether any damage has been incurred; some offences are absolute liability offences, i.e. a mistake of fact cannot be made out as a defence.

Penetration testing activity and ethical attacks without adequate authority could also technically offend the provisions.

As persons can be compelled to assist in an investigation, this may include forcing them to allow third party access to their computer systems. This may also involve compelling them to reveal passwords and private or encrypted data. Consequently concerns have been raised that the breadth of the law enforcement provisions may result in the privacy of individuals being infringed.

As pointed out by countless authorities, Australian business, individuals and government are the targets for malicious and organised criminals. Cyberspace criminal activity will be used to attack innocent parties and legitimate interests. The unprecedented scale and reach of malicious cybercrime must be met with adequate security measures, and the law must adapt to meet these requirements.

## Pavuk Legal Services

Pavuk Legal can provide you with legal advice in respect of Cyber Security, Internet of Things and Cyber Crime matters, as well as provide advice in relation to privacy, data protection and cyber-related legal and commercial issues.

Many other essential hot topics for business owners is all found in the book Nobody Else's Business. Nobody Else's Business is about helping business owners live the life they want to live, now and in the future. It is the ultimate guidebook for succession planning of modern Australian businesses.

To purchase your own copy of Nobody Else's Business please follow the link:

http://www.nobodyelsesbusiness.com.au/

For the full range of Legal Services that Pavuk Legal offers please go to:

http://www.pavuklegal.com/services/

Please contact:

**Andrew Pavuk**:
Email: apavuk@pavuklegal.com
Phone: 02 9247 9013

**Mahsa Curci**
Email: mcurci@pavuklegal.com
Phone: 02 8069 8986

**Maryna Roganova**
Email: mroganova@pavuklegal.com
Phone: 02 8069 8981

**Jacob Roche**
Email: office@pavuklegal.com
Phone: 02 8069 8985

**Mark Shumsky**
Email: mark.shumsky@pavuklegal.com
Phone: 02 9251 3611

**Irene Omeros**
Email: iomeros@pavuklegal.com
Phone: 02 9251 3611

**Ann Matthias**
Email: ann.matthias@pavuklegal.com
Phone: 02 9251 3611