PRELIMINARY

LEGAL STUDIES

A brand-new format that makes even better use of your study time

Robert Barlow

PASCAL PRESS

2014

GLEBE NSW
2.3 Contemporary issue: The individual and technology

Technological change is not new—it has existed as long as humans have walked the planet. However, the advances made with developing and improving technology in recent times have meant that technological advances are occurring faster than the law can 'keep up'. This makes it difficult to ensure that all parties that access technology have adequate legal protection along with access to legal remedies if individual rights are violated.

2.3.1 Impacts of technology on the individual

The main driver of technological change has been the Internet and the use of computers and telephone systems to access it. Along with the Internet has come the concept of 'cyberspace', a term coined by the science-fiction author, William Gibson. Today the term is taken to refer to the global network of interdependent information technology infrastructures, telecommunications networks and computer-processing systems. The idea of cyberspace places it outside of the jurisdiction of any judicial body or nation state, creating a problem when it becomes necessary to try to find legal remedies where individual rights have been violated.

Accessing the Internet can provide a social experience where individuals can interact, exchange ideas, share information, provide social support, conduct business, direct actions, create artistic media, play games and engage in political discussion. The benefits that individuals can gain by accessing the Internet include:

- the inexpensive access to a multitude of information on an incredible amount of topics
- the ability to associate with literally millions of people through social networks such as Facebook and Twitter as well as a multitude of online forums
- associating with a wide variety of people from different nations and cultures
- the ability to work from a remote location and communicate electronically with workmates and supervisors
- the ability to conduct commerce online via the online transfer of funds.

On the other hand, there are a number of disadvantages that exist from accessing the Internet, including:

- the difficulty that geographical jurisdictions face in terms of developing laws to ensure the orderly use of technology
- problems that exist with enforcing laws
- the development of cybercrime and crimes associated with identity theft and fraud
- problems where individuals have a lack of access to the Internet and online commerce.

While the social experiences of online interaction with other individuals and businesses can be beneficial for individuals there are aspects of this interaction and use of technology that can cause breaches of both civil and criminal law.
Other ways in which the development of technology has impacted on individuals in contemporary society include:

- the use of technology in medicine
- surveillance, including the use of closed circuit television
- entertainment
- new methods of food production, including techniques which can increase yields and improve resistance to disease along with speeding up the growth of plants and livestock
- the area of criminal law
- online supermarket shopping which can assist 'time poor' individuals.

2.3.2 Legal implications

A major legal implication of the use of technology for individuals is that with the use of computer technology individuals are able to remain anonymous. Individuals can subscribe to a number of forums and have login names that are not their own. These are known as pseudonyms. By doing this, individuals are able to conceal their identities while making online comments. This allows individuals to make comments that may be defamatory or may vilify others with a small chance of being caught. To some extent, this has led to cyber-bullying.

Another legal implication is security with regard to online financial transactions. Many individuals conduct online financial transactions including:

- banking and the transfer of money
- purchases of goods and services
- purchase and sale of shares
- payment of debts
- management of superannuation accounts.

Online financial transactions have led to the computer crime of hacking. Hacking refers to unauthorised access to data and information and using this information to defraud people or businesses of money. Hacking changes the owner's original intent.

The idea of hacking leads to a third legal implication: the concept of cybercrime. Cybercrime is defined as:

an offence that is committed against individuals with a criminal motive to intentionally harm the reputation of the victim or cause economic or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (chat rooms, e-mails, notice boards and groups) and mobile phones.

In Section 2.2, the role of the Australian Federal Police (AFP) in fighting cybercrime was examined (page 107). The AFP website notes that:

The AFP sees the increasing use and dependence on technology as one of the major influences on the domestic and international law enforcement operating environment.

Information and Communications Technology (ICT) impacts on law enforcement because of the way in which it can facilitate both lawful and unlawful activities. Crimes such as fraud, scams and harassment can be facilitated by using technology which brings unique challenges to old crimes.

A fourth legal implication of the use of technology for individuals deals with issues associated with Internet fraud. Internet fraud is defined as 'using the Internet to misrepresent information or conceal information or to mislead or deceive individuals'.

There are a number of ways that cyber criminals can commit Internet fraud as outlined below.

'Phishing' is an attempt to acquire usernames and passwords as well as details of credit cards. This is done through sending an e-mail disguised as being from a reputable source. There is also the possibility that a phishing e-mail will contain links to sites that contain 'malware' (malicious software) which may be able to relay password or username information.

'Spam' is unsolicited e-mail and spamming is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. It also covers instant messaging, SMS and other mobile phone messaging. At best, spam clogs up individual and business e-mails.

Spam also has the potential to violate individual privacy. There are many programs available today with spam filters and in 2003 the Australian Parliament passed the Spam Act 2003 (Cth) in response to the growing volume of unsolicited commercial electronic messages.

Pyramid selling is a scheme that involves promising participants' payment in exchange for enrolling other people into the scheme, rather than supplying any real investment or sale of products or services to the public. Pyramid selling has been around for a long time and existed long before the widespread use of electronic communication. A variant that many people are familiar with is chain letters.

Many Australians have become victims of what are known as 'Nigerian scams', so-called because they originated in Nigeria. With these scams, individuals are contacted by e-mail and promised huge rewards if they help someone transfer money out of their country by paying fees or giving them their bank account details.

The crime of identity theft is associated with the previous four methods of Internet fraud and is one of the fastest growing crimes in Australia. Identity theft is when an imposter obtains key pieces of personal information which can be used to obtain credit, merchandise and services in the name of the victim, or to provide the thief with false credentials.

Apart from individuals who have their identity stolen, the main victims of this crime include consumers, lending institutions and retail establishments. It has the potential to generate a loss of confidence in our commercial system and leads to other criminal activity, such as theft, fraud and terrorism. It also causes business losses that are never recovered and generates emotional distress for the victims.

Although there are conventional, low-technology techniques of stealing identity, there are a number of ways in which new technology is used to steal identities, usually with the victim being unaware until bills start appearing. Most theft of identity is used to purchase goods or services or to obtain credit or a loan.

2.3.3 Difficulties with enforcing rights

Before explaining the difficulties with enforcing rights it is important to identify the rights that are at risk of being infringed by technological applications. Listed on page 102 are a number of rights enumerated in the UN Universal Declaration of Human Rights 1948. Technology has the potential to infringe on these rights as follows.
Recognition as a person can be denied through identity theft.
There is the right to own and not be arbitrarily deprived of property,
which happens more easily through computer scams and identity theft.
There is some overlap between the right to privacy and the right to
freedom of expression and there is a tension between this last right
and the potential to use technology for acts of cyber-bullying and
vilification.
The difficulties with enforcing rights stem from two problems outlined
below.

- Technology is developing more rapidly than the laws that regulate the
  use of that technology are developing.

- The nature of the use of technology raises the problem of geographical
  jurisdiction, which may put the user beyond the jurisdiction of the
  country of the victim and its law enforcement agencies. Another
  problem is that the perpetrator may often be able to hide behind
  anonymity by using concocted usernames or untraceable social media
  or e-mail accounts.

In the Commonwealth jurisdiction, the decision to enforce rights rests
with the Commonwealth Director of Public Prosecutions (CDPP). The
CDPP prosecutes offences against some 70 Acts and Regulations.

One major area of responsibility relates to national infrastructure. This
includes money laundering, offences relating to postal services,
telecommunications offences, including in relation to use of a carriage
service involving child abuse, child pornography material and suicide-
related material, and offences relating to financial information.

In NSW, rights are enforced through the provisions of the Crimes Act
1900 (NSW). This Act has been amended many times since enactment
and it contains 582 different sections. Section 308 defines the area of
computer crimes and the jurisdiction of NSW law enforcement.

**CRIMES ACT 1900 (NSW)— Sect 308**

**General definitions**

In this Part:

- 'data' includes:
  - (a) information in any form, or
  - (b) any program (or part of a program).

- 'data held in a computer' includes:
  - (a) data entered or copied into the computer, or
  - (b) data held in any removable data storage device for the time being in the computer, or
  - (c) data held in a data storage device on a computer network of which the computer forms part.

- 'serious computer offence' means:
  - (a) an offence against section 308C, 308D or 308E, or
  - (b) conduct in another jurisdiction that is an offence in that jurisdiction and that would constitute
    an offence against section 308C, 308D or 308E if the conduct occurred in this jurisdiction.

The NSW Crimes Act (Subsections 308C and 308D) provides that:

- a person who intentionally and without authority or lawful excuse destroys, erases or alters data
  stored, or inserts data into a computer, or interferes with, or interrupts or obstructs the lawful
  use of a computer is liable to imprisonment for a maximum of 10 years or a fine, or both.

It is difficult for the pace of legislation to keep up with the development of technology. The same is true of international law, which relies on the establishment of treaties. There is a need to develop regional and global responses to computer crimes in order to enforce rights that have been violated. This is just one way that control and regulation of technology could be improved. The following contemporary media report raises several privacy and property issues as well as extortion via hacking.

**Russian hackers hold Gold Coast doctors to ransom**

by Sara Hicks, ABC News Radio

Russian hackers are holding a Gold Coast medical centre to ransom after encrypting thousands of patient health records.

The hackers are demanding a ransom of $4000 to decrypt the sensitive information held on a server at the Miami Family Medical Centre.

IT security expert Nigel Phair says this latest attack is a ‘wake-up call’ with businesses around Australia hacked five to ten times a week.

‘Cyber criminals based mainly throughout Eastern Europe look for rich targets, places with identifying information to extort,’ said Mr Phair, the director of the Centre for Internet Safety and a former investigator with the Australian High-Tech Crime Centre.

Mr Phair says health professions that store valuable information are the biggest target with small-to-medium hacking operations that collect credit card details.

David Wood, co-owner of the Miami Family Medical Centre, says they thought they had a good system in place.

‘We’ve got all the antivirus stuff in place—there’s no sign of a virus. They literally got in, hijacked the server and then ran their encryption software,’ he said.

‘It’s people who know how to break in past firewalls and hack passwords to get onto the server.’

He has reassured patients that the data has not been stolen.

‘It’s secure in the sense that no-one’s taken any of it,’ he said.

‘We’re trying to work out how to pay the hackers or find someone to decrypt the information.’

The server with encrypted information is being held offline and an IT contractor is working with the practice to restore a backup of patient records.

Mr Phair says the information may be lost permanently.

‘At this point, most probably, their only option is to pay,’ he said.

‘Though that’s not the best option because as we know from extortion once you pay they’ll follow that up.’

‘They might follow it up saying they want another payment or partially decrypt some of the information.’

Mr Phair says the hackers are not easy to trace and international police investigations are difficult, reducing the chance of retrieving information without paying a ransom.

‘It’s not impossible, just time intensive,’ Mr Phair said.

‘The hackers will hide their traces and their steps really well—they could be based anywhere in the European continent. In a lot of those places law enforcement isn’t that strong and so it’s difficult to get cooperation with [local] police.’

The seemingly low ransom price is a strategy of the hackers to increase their chances of collecting.

‘It’s similar to traditional fraud in that you keep the value low and the volume high, so you can get $4000,’ Mr Phair said.

Mr Wood warns other businesses to ‘check your IT security and don’t leave backups connected to servers’.

Source: ABC News Radio, 10 December 2012
Issues raised in this article include:

- The relative ease of committing computer crime through hacking.
- The problems that businesses (and individuals) have in storing information.
- The violation of individual rights, including privacy and ownership of property.
- Problems of securing the cooperation of law enforcement authorities in other nations.
- The difficulty of tracing hackers.

These issues highlight the difficulties with enforcing rights.

2.3.4 Future directions—the role of law reform

A major area where law reform is needed to protect individuals and businesses is in the area of international law. At present there are very few international treaties that deal with the problems associated with the misuse of technology.

The main international treaties that deal with technology surround the World Intellectual Property Organization (WIPO). WIPO is the United Nation's agency dedicated to the use of intellectual property (patents, copyright, trademarks, designs) as a means of stimulating innovation and creativity. The main way in which WIPO protects intellectual property is through development of the international legal intellectual property framework. The two major treaties to enforce this are:

- The WIPO Copyright Treaty (WCT) (adopted in Geneva on 20 December 1996).

With the WCT, 90 member nations of the 157 members of the parent body, the World Trade Organization (WTO), have signed the treaty while 91 member nations have signed the WPPT. Australia has signed both treaties. With less than half the world's nations as signatories to both treaties, this makes enforcement more difficult because intellectual property pirates can establish themselves in a non-signatory nation.

Another international area where important safeguards and sanctions exist is the Council of Europe's Convention on Cybercrime 2001. This was the first international treaty seeking to address crimes committed via the Internet, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures, such as the search of computer networks and interception. This has had the impact of improving investigative techniques and increasing cooperation among nations.

In presenting the Convention for signing, the Committee of Ministers of the Council of Europe concluded:

The criminal law must therefore keep abreast of these technological developments which offer highly sophisticated opportunities for misusing facilities of the cyber-space and causing damage to legitimate interests. Given the cross-border nature of information networks, a concerted international effort is needed to deal with such misuse. Only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena.

The above extract indicates the future directions that the Committee of Ministers of the Council of Europe sees as essential to containing cybercrime.

In 2006 the Additional Protocol to the Convention on Cybercrime came into force. The purpose of this is two-fold and aims to:

- make it easier for nations that have agreed to the Convention to adopt similar laws in the fight against racism and promoting dislike and hatred of other people on the Internet
- improve international cooperation in this area.

The Convention on Cybercrime and the Additional Protocol to the Convention on Cybercrime indicate that there is a pressing need for governments to create legal frameworks where the rule of law will prevail and, in enforcing the law, provide a deterrent to individuals and organisations that break laws regarding cybercrime.

In Australia, the Commonwealth has attempted to address the problems of tightening the laws that deal with cybercrime. Much of the legislation that existed in the federal jurisdiction had not kept pace with technological developments so a numbers of Acts were amended in the Cybercrime Legislation Amendment Bill 2011 (Cth) which became law in September 2012. The following contemporary media report explains the reasons behind the law reforms that the bill contained and indicates future directions in terms of legal controls on technological development and cybercrime.

"New laws in the fight against cybercrime"

New legislation has today passed the Senate today that will make it easier for police to track down cyber criminals around the world.

Attorney-General Nicola Roxon said the passage of the legislation will also allow Australia to accede to the Council of Europe Convention on Cybercrime.

"Cybercrime is a growing threat that touches all aspects of modern life. It poses complex policy and law enforcement challenges, partly due to the transnational nature of the Internet," Attorney-General Nicola Roxon said.

By acceding to the Convention, Australia joins 34 other nations that have become a party to the Convention, including the United States and Germany. Over 100 nations are also using the Convention as the basis to strengthen their legislation to combat the threat of cybercrime.

"This is good news for fighting crime and will help make it easier for police to track down cyber criminals around the world.

"In particular, this will help combat criminal offences relating to forgery, fraud, child pornography, and infringement of copyright and intellectual property.

"The Convention promotes a coordinated approach to cybercrime by requiring countries to criminalise these computer-related offences. The Convention also establishes procedures to make investigations more efficient to improve international cooperation."

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with computer-related fraud, child pornography and violations of network security.


The government amended the Bill in the Senate to address some of the recommendations made by the Joint Select Committee on Cyber-Safety, including privacy protections and aspects of the provision of assistance to foreign agencies. The government has agreed in principle with 12 of the Committee’s 13 recommendations.

The Bill will ensure that Australian legislation is consistent with international best-practice and enable domestic agencies to access and share information to facilitate international investigations.

Example of contemporary issue: The individual and technology—cyber-bullying

Bullying involves the use of information and communication technologies, such as computers, the Internet and mobile phones, to perpetrate deliberate, repeated and hostile behaviour towards a targeted individual. It is harassing, threatening and intimidating to the victim.

Bullying may involve:

- Posting embarrassing photos of people on the Internet or social networking sites
- Sending unwanted messages or belittling or insulting other people online
- Making threats or sending cruel or hurtful messages
- Creating phony profiles or posting fraudulent or misleading material about others.

Impacts of technology on the individual with regard to cyber-bullying

The following contemporary media report illustrates how serious the issue of cyber bullying is.

‘Charlotte Dawson: How the cyber trolls beat me’

Trolling victim Charlotte Dawson has told of how a hate campaign on Twitter got the better of her and landed her in hospital.

Speaking for the first time about the torrent of abuse she received on Twitter last Wednesday night, the 46-year-old TV presenter told 60 Minutes last night ‘I’ve never had death threats of this ferocity. I’ve never had a campaign of this ferocity.’

Dawson was admitted to hospital after she was targeted by a stream of abusive death threats on Twitter, including taunts to ‘stick your head in a toaster’ and ‘kill yourself’.

After spending hours fending off the insults, Dawson signed off with the disturbing message ‘you win x’ along with a picture of a hand holding pills at 2.07 am. Just after 3 am, an ambulance arrived at her home and took her to Sydney’s St Vincent’s Hospital. Dawson said it was the relentless and vicious messages that finally broke her.

‘It just triggered that feeling of helplessness when the trolls got to me,’ Dawson said. ‘They got the better of me and they won.’

Dawson said as a celebrity she expected to cop a certain amount of abuse.

‘You do have to have a thick skin and you do understand that no matter what you do, even if you’re Mother Teresa, people are still going to hate you just because they think you’re ugly or they don’t like the sound of your voice,’ she said.

‘If people are wanting you to kill yourself and you are somebody who has previously tried to end your life it’s very, very easy to feel like that’s exactly what you want to do.’

Source: Staff writers, News Limited Network, 3 September 2012
Cyber-bullying basically applies to young people under the age of 18. When the concept applies to adults, there may be the possibility of a crime being committed, such as cyber-harassment or cyber-stalking. The ‘cyber’ prefix simply means that the harassment or stalking is conducted through the use of information and communication technologies, such as computers, the Internet and mobile phones. The rise of social network sites has also facilitated the growth of cyber-bullying.

A 2008 poll of Australian youth aged 15–20 found that 64% of respondents had a social network site such as MySpace or Facebook. The poll also found that 22% of these young people had been bullied online.

Cyber-bullying can take the form of harassment or stalking. There is not much distinction between the two but harassment can be defined as systematic and continued unwanted and annoying actions of one party or a group, including making threats and demands on the target. Stalking refers to unwanted or obsessive attention by an individual or group toward another person. Stalking behaviours are related to harassment and may include following the victim in person or monitoring them.

Advancements in technology have allowed the opportunity for cyber-bullying of children to expand for the reasons outlined below.

It is easy for the cyber-bully to hide his or her identity.

It is easy to enlist the support of others to cyber-bully individuals or groups.

There has been a substantial growth in the use of online social networking, which may be used as a tool for cyber-bullying.

Cyber-bullying can continue day and night, unlike the more traditional forms of physical bullying that took place at school.

**Legal implications with regard to cyber-bullying**

Because the use of mobile and online communications has grown so rapidly and the cyber-bullying is relatively new, many jurisdictions are deliberating over cyber-bullying laws. However, the crime is covered by existing laws against personal threats and harassment. It is always important to report abuse of the telecommunications system to the Australian Federal Police who have a responsibility in this area as well as programs to assist young victims. Individuals should not retaliate because such behaviour can lead to heightened attacks.

Caslon Analytics, an organisation that develops online information about aspects of law, digital technology, business and society, notes that state and territory legislation in Australia regarding stalking defines stalking as ‘acts that occur repeatedly and these acts intend to cause fear to the individual’.


The online article goes on to note that the ‘federal Criminal Code, updated through the Crimes Legislation Amendment (Telecommunications Offences & Other Measures) Act (No. 2) 2004 (Cth), features offences of using a ‘postal or similar service’ or a carriage service ‘to menace, harass or cause offence’. This means that it is an offence to use a postal or similar service (such as the telephone system) in a way that reasonable persons would regard as menacing, harassing or offensive.
CASE STUDY 2.11: Gerada in Melbourne Magistrates Court 2 April 2009

A 17-year-old Allem Halkic had once been friends with Shane Phillip Gerada, a 21-year-old. In early 2009, Gerada sent a number of threatening text messages. On 5 February 2009 Halkic jumped from Melbourne’s West Gate Bridge.

What crime had Gerada committed?

Prosecution

Gerada was charged with stalking via cyber-bullying. He pleaded guilty to this charge. In court he impressed the magistrate with the remorse that he showed. Magistrate Peter Reardon made the following remarks:

It just demonstrates SMS messages or Internet communication may have severe consequences on intended victims whether it was meant to or not. People really should think about what they are doing instead of just hammering some message of hate or aggression.

Gerada received an 18-month community-based order as a sentence. Gerada was the first person in Australia to face prosecution for stalking via cyber-bullying.


Difficulties with enforcing rights with regard to cyber-bullying

One major problem with enforcing an individual’s rights with regard to cyber-bullying is being able to prove that a person’s rights have been violated. Section 2.3.3 (page 133) identified the main rights that cybercrime can violate.

Another problem stems from trying to fit cyber-bullying into a legal context. For many years, bullying has been part and parcel of the school environment though this does not make bullying right, nor does it excuse it. In recent years, with the notification of suicides of young people as a result of cyber- and other forms of bullying, there has developed a growing public awareness of this problem. Unfortunately, finding successful solutions has not been as easy as recognition of the problem.

Within the school context, teachers are guided by system policies in terms of dealing with instances of bullying. The problem with cyberbullying is that it often does not come to the attention of teachers and parents until the problem has grown out of proportion or until it is too late. However, there are a number of steps that teachers and parents can take to assist young people to protect their rights with regard to cyberbullying once the problem has been identified. These are outlined below.

- Notifying the school—the school can only act if it is aware that there is a problem. Children need to be encouraged to share the problem with parents and the school.
- It is possible to block the sender’s messages by installing a spam filter, which will ‘jail’ messages from designated e-mail addresses.
- It is important to discuss the use of technology with children and place limits on that use.
- Instances of cyber-bullying should be reported to the police and Internet service providers while telephone bullying should be reported to the appropriate telephone service provider.
- The Internet can be used to search for information about cyberbullying.

Explain the difficulties with enforcing rights with regard to cyber-bullying.
If instances of cyber-bullying are recognised in their early stages there may be ways to solve the problem without resorting to legal processes. If a legal solution is sought, it can become difficult to find appropriate legislation where action can be taken.

The question of jurisdiction may also be an issue as with many instances of cyber-bullying it can be difficult to determine whether it is a state or federal matter. Recently, as part of the process of law reform, laws enacted in both state and federal jurisdictions can be used to address the specific problem of cyber-bullying.

**Future directions—the role of law reform with regard to cyber-bullying**

Current state and federal legislation offers substantial protection though it is important to note that it is difficult to prevent cyber-bullying. However, there are avenues of legal relief that can be obtained if there are substantiated instances of cyber-bullying. People who have had their rights infringed by cyber-bullying can seek redress through the actions below.

- By taking out an apprehended violence order (AVO) where the victim can apply to the police or the courts for an order for the perpetrator to cease the action.
- In NSW it is a criminal offence to harass or intimidate a school student while the student is at school.
- Commonwealth legislation can be used in the federal jurisdiction to prosecute offenders who have used the telephone system or technology to harass, stalk or threaten victims.

Law reform commissions and parliaments need to consider the issue of regulating social networking sites such as Facebook and Twitter. The media report dealing with the cyber-harassment and bullying of Charlotte Dawson indicates the need for some external control (rather than self-regulation) of social networking sites. In this instance it was the policy of Twitter not to mediate content even if it was potentially offensive. This area of law reform could involve a separate regulatory authority to control social network sites in a similar way that the Australian Communications and Media Authority (ACMA) regulates radio and television broadcasting. The ACMA does have regulatory power over online content through codes of practice. Its role in regulating online content is as follows:

- The ACMA administers a ‘co-regulatory’ scheme for online content, including Internet and mobile phone content. The scheme aims to address community concerns about offensive and illegal material online and, in particular, to protect children from exposure to material that is unsuitable for them.

Source: www.acma.gov.au/WEB/STANDARD/pc=PC_90154

At present, the Internet Industry Association has developed codes of practice which are applicable to its members and are self-regulating. New standards need to be developed to ensure that people have some protection from online and mobile bullying, while ensuring that rights such as freedom of speech are protected.

Another cyber issue relates to ‘sexting’, a form of texting that involves taking and sending nude or provocative photos of oneself or another person. These photos are then sent to a person or several peers and can cause extreme embarrassment by being posted on a social network.
Areas for reform of the law that need addressing include determining the point where this practice becomes a police matter and out of the control of the school. There is the possibility of the recipient being prosecuted for possessing child pornography or being sued for sexual harassment.

The federal government has announced its intentions to reform laws to address the problems raised by sexting. It has proposed amendments to the sex discrimination legislation so that cases involving cyber-bullying and sexting become part of this law. Amendments would mean that there would be protection for persons under the age of 16 who are the victims of sexting and cyber-bullying and other forms of sexual harassment.

2.4 Themes and challenges

2.4.1 Theme 1: Relationship between justice, law and society

In Chapter 1 (Section 1.6.1, page 71) the relationship between law and society was explained. Societies are regulated by laws that govern the behaviour of their members and provide a framework for all activities of a community. The community accepts the legitimacy of the lawmaker bodies to make laws that will govern the affairs of the community. Because of this acceptance the laws are binding on all the members and organisations of that community.

Also in Chapter 1, the concept of justice was defined as a set of principles of moral rightness, based on ethics, values, law, natural law, religion and equity. It is the quality of being fair and reasonable. The ideas of equality, fairness and access underpin the nature of justice. (Section 1.1.5, page 6)

For society to accept the legitimacy of lawmaker bodies there must be a recognition that justice prevails. In order for this to occur, the rule of law must be the paramount principle that underpins the operation of all functions of government—legislative, executive and judicial.

The rule of law holds that all people and authorities within a nation, whether public or private, are bound by the laws of the nation. This means that no person or institution is more important than the law.

The operation of the rule of law is essential in a democratic society because it protects citizens against the abuse of power by the government. When it seems that the government is abusing its considerable powers, citizens seek the protection of their legal, citizenship and constitutional rights (Section 2.1.1, page 100). In order for citizens to enjoy the exercise of these rights, the rule of law must apply in a society.

The application of the rule of law and the relationship between justice, law and society becomes evident when individuals attempt to resolve disputes with other individuals and between an individual and the state. In order for effective resolution there must be an effective executive branch of government that will investigate disputes in terms of the law. There must also be an effective range of judicial options for individuals and the state to access if the dispute escalates beyond the range of non-legal methods and alternative dispute mechanisms.
2.4.2 Theme 2: Relationship between rights and responsibilities

To be able to enjoy and exercise rights, individuals need to ensure that they are giving consideration to the rights of others. This means that in order to exercise a right a person has a responsibility to ensure that the rights of others are not infringed. Rights are a part of communities of people living together.

The relationship between the rights and responsibilities of an individual refers to the fact that to exercise every right also involves a responsibility. This means that if a person wishes to enjoy the right of freedom of speech, that person has a responsibility to ensure that others are able to exercise the same right.

A number of areas that need to be considered when examining the relationship between rights and responsibilities were outlined in Section 2.1.2 (page 104).

2.4.3 Theme 3: Balancing the rights of individuals with the needs of the state

Although individual rights (human rights) are inalienable (cannot be given up), many nations are able to restrict them because of the notion of sovereignty. Sovereignty was discussed in Section 1.2.16, page 46.

However, the notion of sovereignty can help people exercise their rights where sovereignty is firmly in the hands of people. In this situation, people can exercise their democratic right to change the government at an election if they are dissatisfied with its performance. If, however, the state has a non-democratic, totalitarian government there may be little protection of human rights.

In Section 2.1.2 (page 106) the relationship between the individual and the state in terms of guarantee of rights and support of the state was explained. It is the role of the state to identify, protect and enforce the natural rights of the individual and to protect individual rights through the application of the law.

This protection and enforcement of individual rights by the state places obligations on individual citizens. Citizens have an obligation to support the state in return for this protection (see Section 2.1.2, page 104). Individual support of the state includes paying appropriate taxes, respecting the rights, beliefs and opinions of others, and participating as a responsible citizen in the local community.

In our contemporary era, the ‘war on terror’ that has taken place since the attacks on the USA on 11 September 2001 have seen the needs of the state placed on a higher priority than the rights of individuals in certain areas. In Australia, two laws passed by federal parliament have placed some restrictions on the complete exercise of rights by individuals. These Acts are the:

Security Legislation Amendment (Terrorism) Act 2002 (Cth)

Anti-Terrorism Act (No.2) 2005 (Cth).

The restrictions on rights include the establishment of Preventative Detention Orders (PDOs) and control orders when an individual is suspected of belonging to a terrorist organisation or being involved in the planning and committing of a terrorist act. These orders represent a fundamental departure from the long-held principle that a person should not be detained without trial.
2.4.4 Theme 4: Role of the law in regulating technology

As technological developments progress there are a number of impacts on our society, including:

- greater access to online forums, which can enhance freedom of speech
- an increase in employment opportunities
- when and where work is conducted
- greater access to sources of information and knowledge
- the ability to conduct commerce online through the online transfer of funds.

While each of these impacts is beneficial, there is the potential for abuse of technology which can lead to criminal acts.

The law has several roles in regulating technology. Firstly, the law must be able to regulate and approve of certain types of technology. Many contemporary technological devices use the telephone system and the law already has a role in how that system may be used. Where there are breaches of the law there is the potential for the appropriate authorities to prosecute offenders.

There is a substantial body of both state and federal criminal law that can be applied to crimes where technology is used, though some laws may not apply directly to the offence committed. There is also the problem of jurisdiction: if a hacker in Perth hacks into a Sydney resident’s bank account has the crime been committed in Sydney or Perth? Which state police force has jurisdiction? Is federal jurisdiction involved because the telephone system has been used? This becomes even more complicated when the cyber-criminal is located in another country.

These are some of the reasons why governments in Australia and the rest of the world are developing legislation and treaties that deal with specific instances of cybercrime. This law reform can be seen in Section 2.3.4, page 137.

There is also the serious matter of cyber-bullying that was examined in Section 2.3.5, page 139. Current thinking is that existing laws are sufficient in dealing with this area although there are proposed reforms to criminalise the cyber-bullying of young people under the age of 16.

There is still a substantial time lag between emerging technology and the legal response to its manipulation by people intent on committing criminal acts. Both Commonwealth and state law reform commissions need to be proactive in proposing law reform to regulate technology.

2.4.5 Theme 5: Effectiveness of legal mechanisms for achieving justice for individuals and society

The effectiveness of legal mechanisms in achieving justice for individuals are discussed throughout this chapter, primarily in Sections 2.2.2 (page 111), 2.2.3 (page 116) and 2.2.5 (page 130). There are also concise summaries of the effectiveness of these mechanisms in tables 2.3 (page 130) and 2.4 (page 131).

As a general rule, the more prepared that the parties to a dispute are to negotiate a settlement and the more informal the dispute resolution mechanism, the greater the chance of success in resolving the matter and the more effective the process. Of course there are exceptions to this and parties to a dispute may wish for the certainties that go with the impartial decision making of the more formal processes of dispute resolution.
Do you know all the key definitions and concepts for this chapter? Go through each term in the list and check that you know them all. Place a bookmark underneath each definition to cover up the one below and slide it down. This way you can focus on each definition by itself.

**Administrative review** is a review of a decision made by a government minister or agency that is conducted by an independent government tribunal such as the NSW Administrative Decisions Tribunal or the federal government’s Administrative Appeals Tribunal.

**Alternative dispute resolution (ADR)** refers to a variety of different processes where a disinterested or impartial negotiator assists people in resolving their disputes without the need to go to court.

**Arbitration** is a formal and structured process. As part of this process the parties present arguments and evidence to an independent third party, the arbitrator, who makes a determination. This decision will be binding on the parties involved.

**Claim rights** are those that an individual can exercise, but these rights imply that others have a duty to the person who exercises a claim right.

**Conciliation** is an ADR process where an independent third party assists people in dispute in an effort to try to resolve that dispute. Unlike mediation, this process is chaired by an independent person who has expertise in the area of the dispute and will provide advice about the issues and options for resolution.

**Council of Europe** is not part of the European Union but an international organisation in its own right, based in Strasbourg. Its main role is to strengthen democracy, human rights and the rule of law throughout its member states. The 28 member states of the EU are all members of the Council of Europe, whereas the Council of Europe, with its 47 member states, has a much wider membership.

**Customary rights** are those to which an individual may feel entitled because of custom or social practice.

**Cyber-bullying** is the use of information and communication technologies, such as computers, the Internet and mobile phones, to support deliberate, repeated and hostile behaviour. It is harassing, threatening and intimidating to the victim.

**Cybercrime** is an offence committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim/s or cause economic or mental harm to them, directly or indirectly, by using modern telecommunication networks (chat rooms, e-mails, notice boards and groups, mobile phones, etc).

**Cyberspace** is the global network of interdependent information technology infrastructures, telecommunications networks and computer-processing systems.

**Direct negotiation** involves the key players in a dispute talking and trying to come to an agreement that works for everyone.

**Dispute** is a continuing disagreement between two or more parties.

**Domestic rights** are those that people have within their own nation.

**Donkey vote** is where an apathetic voter numbers the squares on a ballot paper in sequence from top to bottom.

**External review** is the review of a complaint against a government agency by a body or tribunal that is separate from the agency being complained about. An example of an external review agency would be the NSW Administrative Decisions Tribunal.

**Hacking** refers to unauthorised access to data and information and using this to defraud people or businesses of money. Hacking changes the owner’s original intent.

**Harassment** is the systematic and continued unwanted and annoying actions of one party or group. It can include making threats and demands on the target.

**Human rights** are the inalienable fundamental rights to which a person is inherently entitled simply because that person is a human being.

**Identity theft** is a crime in which an impostor obtains key pieces of personal information, such as driver’s licence numbers, credit card details, or other documents which verify identity, in order to impersonate someone else.

**Individual rights** outline what is owed to a person or the freedoms that a person can exercise through a legal system, custom or morality or ethics.

**Interest groups** are not-for-profit and usually voluntary organisations whose members have a common cause for which they seek to influence public policy, without seeking political control.

**Internal review** is an investigation that is conducted by the government agency against which a complaint has been made.

**International rights** are those that are deemed to apply to all people regardless of their nationality or the type of political system or government that exists within their own nation. These rights include human rights.

**Internet fraud** is using the Internet to misrepresent or conceal information or to mislead or deceive individuals.

**Judicial review** is when a court considers whether a decision made by a government minister, department or authority has been made correctly.
Legal responsibility is defined as something that an individual is expected or required to do by legal force.

Legal rights are an entitlement that is given to a person and enforced or protected by the law.

Liberty rights give the person claiming the right the freedom to be able to do something without there being an obligation on anyone else to do or not do something.

Mediation is an ADR process where an independent third party assists people in dispute to try to resolve the issue.

Moral or ethical rights are those where a person feels that he or she has an entitlement to something because of a moral or ethical principle.

Ombudsman is an intermediary between the state and the population. An Ombudsman is appointed by the government to investigate complaints of individuals and attempt to resolve them, usually through recommendations or mediation.

Phishing is an attempt to acquire information, such as usernames and passwords, as well as details of credit cards via an email that appears to be from a reputable source.

Pyramid selling is a scheme that involves promising participants payment in exchange for enrolling other people into the scheme, rather than supplying any real investment or sale of products or services to the public.

Sexting is a form of texting that involves taking photos of oneself or another person, while posing in a provocative manner or exposing a body part, and sending or posting these images via a mobile phone or social network.

Spam is unsolicited email, frequently containing commercial content and sent in large quantities to an indiscriminate set of recipients.

Stalking refers to unwanted or obsessive attention by an individual or group toward another person. Stalking behaviors are related to harassment and intimidation and may include following the victim in person or monitoring them.

Standing (or locus standi) refers to the right to take action in court or to be heard or represented in a case.

Statutory body is an organisation that has been created by parliament through legislation for a public purpose.

Trade union is an organisation of workers who have banded together to achieve common goals, such as protecting the jobs of its members, achieving higher pay or better working conditions.

Tribunal is a judicial body established mainly to deal with specific area of law such as the NSW Consumer, Trader and Tenancy Tribunal. Tribunals are designed to be fair, informal, efficient, quick and inexpensive.

Vilification is an act that makes vicious and defamatory statements which debase another person or group of people.
<table>
<thead>
<tr>
<th>Page No.</th>
<th>For a complete understanding of this topic:</th>
</tr>
</thead>
<tbody>
<tr>
<td>115</td>
<td>Can I examine courts as a method of resolving disputes between individuals?</td>
</tr>
<tr>
<td>116</td>
<td>Can I compare and contrast disputes between individuals and between individuals and the state?</td>
</tr>
<tr>
<td>117</td>
<td>Can I assess the effectiveness of the media as a method of resolving disputes between individuals and the state?</td>
</tr>
<tr>
<td>118</td>
<td>Can I assess the effectiveness of members of parliament as a method of resolving disputes between individuals and the state?</td>
</tr>
<tr>
<td>118</td>
<td>Can I assess the effectiveness of trade unions as a method of resolving disputes between individuals and the state?</td>
</tr>
<tr>
<td>118</td>
<td>Can I assess the effectiveness of interest groups, including non-government organisations, as a method of resolving disputes between individuals and the state?</td>
</tr>
<tr>
<td>120</td>
<td>Can I assess the effectiveness of internal review as a method of resolving disputes between individuals and the state?</td>
</tr>
<tr>
<td>121</td>
<td>Can I assess the effectiveness of external review as a method of resolving disputes between individuals and the state?</td>
</tr>
<tr>
<td>121</td>
<td>Can I assess the effectiveness of administrative review as a method of resolving disputes between individuals and the state?</td>
</tr>
<tr>
<td>122</td>
<td>Can I assess the effectiveness of judicial review as a method of resolving disputes between individuals and the state?</td>
</tr>
<tr>
<td>124</td>
<td>Can I assess the effectiveness of the Ombudsman as a method of resolving disputes between individuals and the state?</td>
</tr>
<tr>
<td>125</td>
<td>Can I assess the effectiveness of statutory bodies including Australian Human Rights Commission, Independent Commission Against Corruption (ICAC), Royal Commissions as methods of resolving disputes between individuals and the state?</td>
</tr>
<tr>
<td>129</td>
<td>Can I distinguish between non-legal and legal methods of enforcing rights and resolving disputes?</td>
</tr>
<tr>
<td>130</td>
<td>Can I assess the effectiveness of dispute resolution processes in achieving justice for and between individuals?</td>
</tr>
<tr>
<td>132</td>
<td>Can I discuss the impacts of technology on the individual?</td>
</tr>
<tr>
<td>133</td>
<td>Can I discuss the legal implications of the use of technology and its impact on the individual?</td>
</tr>
<tr>
<td>134</td>
<td>Can I explain the difficulties with enforcing rights?</td>
</tr>
<tr>
<td>137</td>
<td>Can I assess the role of law reform in addressing emerging technological issues and enforcing rights?</td>
</tr>
<tr>
<td>139</td>
<td>Can I discuss the impact of technology on the individual with regard to cyberbullying?</td>
</tr>
<tr>
<td>140</td>
<td>Can I discuss the legal implications of the use of technology and its impact on the individual with regard to cyberbullying?</td>
</tr>
<tr>
<td>141</td>
<td>Can I explain the difficulties with enforcing rights with regard to cyberbullying?</td>
</tr>
<tr>
<td>142</td>
<td>Can I assess the role of law reform in addressing emerging technological issues and enforcing rights with regard to cyberbullying?</td>
</tr>
<tr>
<td>143</td>
<td>Can I explain the relationship between justice, law and society?</td>
</tr>
<tr>
<td>144</td>
<td>Can I explain the relationship between rights and responsibilities?</td>
</tr>
<tr>
<td>144</td>
<td>Can I explain balancing the rights of individuals with the needs of the state?</td>
</tr>
<tr>
<td>145</td>
<td>Can I explain the role of the law in regulating technology?</td>
</tr>
<tr>
<td>145</td>
<td>Can I examine the effectiveness of legal mechanisms for achieving justice for individuals and society?</td>
</tr>
</tbody>
</table>

Acts

Australian Citizenship Act 2007 (Cth) (see Section 2.1.1, page 103)
Anti-Discrimination Act 1977 (NSW) (Section 2.1.2, page 105)
Australian Securities and Investments Commission Act 2001 (Cth) (Section 2.2.1, page 110)
National Consumer Credit Protection Act 2009 (Cth) (Section 2.2.1, page 110)
Criminal Code Act 1995 (Cth) (Section 2.2.1, page 107) (Section 2.3.4, page 138)
Crimes Act 1914 (Cth) (Section 2.2.1, page 107)
Crimes Act 1900 (NSW) (Section 2.2.1, page 108)
Independent Commission Against Corruption Act 1988 NSW (Section 2.2.1, page 111)
Community Justice Centres Act 1983 (NSW) (Section 2.2.2, page 112)
Consumer, Trader and Tenancy Tribunal Act 2001 (NSW) (Section 2.2.2, page 114)
Disputes Between Neighbours Act 2006 (NSW) (Section 2.2.2, page 115)
Fair Work Act 2009 (Cth) (Section 2.2.3, page 119)
Privacy and Personal Information Protection Act 1998 (NSW) (Section 2.2.3, page 120)
Administrative Decisions (Judicial Review) Act 1977 (Cth) (Section 2.2.3, page 123)
Australian Human Rights Commission Act 1986 (Cth) (Section 2.2.3, page 126)
Disability Discrimination Act 1992 (Cth) (Section 2.2.3, page 126)
Racial Discrimination Act 1975 (Cth) (Section 2.2.3, page 127)
Spaa Act 2003 (Cth) (Section 2.3.2, page 134)
Cybercrime Legislation Amendment Act 2012 (Cth) (Section 2.3.4, page 138)
Genius Legislation Amendment (Telecommunications Offences & Other Measures) Act (No. 2) 2004 (Cth) (Section 2.3.5, page 140)
Security Legislation Amendment (Terrorism) Act 2002 (Cth) (Section 2.4.3, page 144)
Anti-Terrorism Act (No. 2) 2005 (Cth) (Section 2.4.3, page 144)

Treaties, conventions and other international instruments
Universal Declaration of Human Rights (UDHR) 1948 (Section 2.1.1, page 102)
International Covenant on Civil and Political Rights (ICCPR) 1966 (Section 2.1.1, page 103)
UN Convention on the Elimination of All Forms of Racial Discrimination (CERD) 1965 (Section 2.1.2, page 104)
UN Convention against Transnational Organized Crime 2003 (Section 2.2.1, page 108)
WIPO Copyright Treaty (WCT) 1996 (Section 2.3.4, page 137)
WIPO Performances and Phonograms Treaty (WPPT) 1996 (Section 2.3.4, page 137)
Convention on Cybercrime 2001, Council of Europe (Section 2.3.4, page 137)
Additional Protocol to the Convention on Cybercrime 2006 (Section 2.3.4, page 138)

Case studies
Racialisation in New South Wales (Case Study 2.1, Section 2.1.2, page 105)
Australian Securities and Investments Commission (Case Study 2.2, Section 2.2.1, page 110)
Independent Commission Against Corruption (Case Study 2.3, Section 2.2.1, page 111)
Mediation at Community Justice Centres in NSW (Case Study 2.4, Section 2.2.2, page 112)
Consumer, Trader and Tenancy Tribunal (NSW) (Case Study 2.5, Section 2.2.2, page 114)
McDonnell v Harrison (2012) NSWLEC 1291 (Case Study 2.6, Section 2.2.2, page 115)
'Speed camera disgrace' (Case Study 2.7, Section 2.2.3, page 117)
The 'Your Rights at Work' campaign (Case Study 2.8, Section 2.2.3, page 119)
Denton v State of Victoria (2011) FCA 854 (Case Study 2.9, Section 2.2.3, page 126)
Gerada in Melbourne Magistrates' Court 8 April 2010 (Case Study 2.11, Section 2.3.5, page 141)

Other cases
Barker v Kyrklides (2007) NSWLEC 292 (Section 2.2.2, page 116)
Yang v Scarr (2007) NSWLEC 592 (Section 2.2.2, page 116)

Other documents
'Former Queensland director jailed', ASIC media release, 5 September 2012 (Section 2.2.1, page 109)
'Graffiti artist loses freedom of expression appeal', Sarah Farnsworth, ABC News, 11 September 2012 (Section 2.1.2, page 106)
'Russian hackers hold Gold Coast doctors to ransom', Sara Hicks, ABC News Radio 10.12.2012 (Section 2.3.3, page 136)
www.abc.net.au/news/2012-12-10/hackers-target-gold-coast-medical-centre/4418576
'New laws in the fight against cybercrime', Attorney-General's Department, 22 August 2012 (Section 2.3.4, page 138)
'Charlotte Dawson: How the cyber trolls beat me', News Limited, 3 September 2012 (Section 2.3.5, page 139)
Australian citizenship: www.citizenship.gov.au/should_become/
Australian Government Department of Immigration and Citizenship:
Anti-Discrimination Act 1977 (NSW):
Australian Federal Police:
NSW Independent Commission Against Corruption:
NSW Government Courts and Tribunals Service—ADR:
National Alternative Dispute Resolution Advisory Council (NADRAC):
NSW Community Justice Centres:
Consumer, Trader and Tenancy Tribunal:
Hot Topics 71, Courts, 2009:
McDonnell v Harrison (2012) NSWLEC 1291:
Aussie Speeding Fines:
www.aussiespeedingfines.com/
The ‘Your Rights at Work’ campaign:
Internal Reviews NSW (Office of the Privacy Commissioner NSW):
www.privacy.nsw.gov.au/Lawlink/privacynsw/il_nsw.nsf/pages/privacy_internalreviews#1
Administrative Decisions (Judicial Review) Act 1977 (Cth)—Sect 5:
Commonwealth Ombudsman:
NSW Ombudsman:
Australian Human Rights Commission:
humanrights.gov.au/
Hot Topics 70, Cyberlaw, 2009:
Commonwealth Director of Public Prosecutions:
World Intellectual Property Organization (WIPO):
www.wipo.int/portal/index.html.en
Council of Europe Convention on Cybercrime 2001:
conventions.coe.int/Treaty/en/Summaries/Html/185.htm
Council of Europe Additional Protocol to the Convention on Cybercrime:
conventions.coe.int/Treaty/En/Reports/Html/189.htm
Caslon Analytics (cyber-stalking):
Australian Communications and Media Authority (ACMA):
Gerada cyber-bullying case:
End of chapter questions

Key Concept questions

These questions test whether you have grasped the key ideas in each subsection. They are not difficult questions, but will test your recall of knowledge of the material you have read. If you are unsure what a question is asking you to do, refer to page viii to check the meaning of the Board of Studies key words. If you can answer all these questions, you will know you have a sound knowledge of content.

Refer to pp. 238-41 for

2.1 Your rights and responsibilities

2.1.1 The nature of individual rights
1. Distinguish between claim rights and liberty rights.
2. Distinguish between moral rights and legal rights.
3. Define 'international rights'.

2.1.2 Relationship between rights and responsibilities
4. Identify four responsibilities of Australian citizens.
5. Explain the relationship between rights and responsibilities.

2.2 Resolving disputes

2.2.1 Roles of the federal and state police and other law enforcement agencies
6. Outline the role of the federal police.
7. Identify the roles of the NSW Police Force.
8. Outline the roles of three other law enforcement agencies.

2.2.2 Resolving disputes between individuals
9. Identify methods of resolving disputes between individuals.
10. Examine negotiation as a method of resolving disputes between individuals.
11. Distinguish between tribunals and courts.

2.2.3 Resolving disputes with the state
12. Define and identify non-legal methods of resolving disputes between individuals and the state.
13. Assess the effectiveness of members of parliament as a method of resolving disputes between individuals and the state.
14. Define and identify legal methods of resolving disputes between individuals and the state.

2.2.4 The distinction between non-legal and legal methods of dispute resolution
17. Distinguish between non-legal and legal methods of enforcing rights and resolving disputes.

2.2.5 Effectiveness of dispute resolution processes
18. Assess the effectiveness of the media as a dispute resolution process in achieving justice for individuals.

2.3 Contemporary issue: The individual and technology

2.3.1 Impacts of technology on the individual
19. Outline the disadvantages that exist for individuals accessing technology through the Internet.

2.3.2 Legal implications
20. Identify four legal implications of the use of technology and discuss their impact on the individual.

2.3.3 Difficulties with enforcing rights
21. Identify some of the rights that are at risk of being infringed by technological applications.
22. Explain why there are difficulties with enforcing rights in the area of technology.

2.3.4 Future directions—the role of law reform
23. Outline the extent of one international law reform to enforce rights in the area of technology.
24. Describe an Australian Government reform which assists in enforcing rights in the area of technology.

2.3.5 Example of contemporary issue: The individual and technology—cyber-bullying
25. Define 'cyber-bullying'.