The Shopfront
YOUTH LEGAL CENTRE

Cybercrime (or how technology can get you into trouble)

1 What is cybercrime?

We often use the word "cybercrime" to include a range of criminal activities involving computers or other electronic devices such as mobile phones and cameras. This can include cyber-bullying, offensive phone calls or messages, accessing or distributing child pornography, online grooming of children for sexual activity, hacking, illegal file sharing and various forms of fraud.

Although the law uses a narrower meaning of "cybercrime" (in the Commonwealth *Cybercrime Act 2001,* "cybercrime" applies only to offences against computer data and systems), this document uses broader meaning of "cybercrime".

There are a number of different laws covering technology and crime in Australia. In NSW, many of these offences are covered by the *Crimes Act* 1900 (NSW). There are also laws (such as the Commonwealth *Criminal Code*) which apply all over Australia (and in some cases outside Australia as well).

This document discusses some of the laws that are most likely to affect young people.

2 Photography and filming

In most cases it is perfectly legal to photograph or film a person, and to publish or distribute the photo or footage, even if that person does not consent. However, in some situations this sort of conduct can be an offence, for example:

- Producing or distributing images that amount to "child abuse material" or child pornography (see the section below on "Sexting and child pornography").
- Filming a person without their consent for your own sexual gratification (*Crimes Act* 1900 (NSW) sections 91K -91M).
- Using a mobile phone or the internet to distribute images which could be regarded as offensive (see the section above on "Cyber-bullying").
- Recording private conversations without consent (*Surveillance Devices Act* 2007 (NSW) section 7).
- Unauthorised copying or distribution of photographs or footage taken by someone else (in this case you could be breaching that person's copyright, which is not always a criminal offence but still has legal consequences).

3 Cyber-bullying

"Cyber-bullying" is not a legal term. It is commonly used to refer to online activities such as posting videos and images or typing harmful words with the intention to humiliate, annoy or harass the victim. This can include "trolling", which is intentionally causing distress by posting inflammatory comments on blogs, social media sites and public forums.

People who participate in cyber-bullying could be charged with a range of offences including:

- Stalking or intimidation with intent to cause fear of physical or mental harm (section 13 *Crimes (Domestic and Personal Violence) Act* 2007 (NSW)). The maximum penalty for this offence is five years' imprisonment and/or a fine of $5,500.
- Using a carriage service to threaten to kill, to threaten serious harm or to menace, harass or offend (sections 474.15 to 474.17, Commonwealth *Criminal Code*). A "carriage service" includes any kind of telecommunications service. Maximum penalties for these offences range from 3 to 10 years' imprisonment.

Case study – Troy

Troy, aged 16, was arrested for a minor offence and was badly treated by one of the police officers. A few weeks later he found the police officer on Facebook and sent a message saying "Die, you bitch. I know where you live".

Troy was charged with using a carriage service to menace /harass/offend and intimidating a police officer in the execution of her duty.

The Children's Court regarded these as very serious offences and gave Troy a suspended sentence.

4 Sexting, child pornography and child abuse material

Young people who distribute sexually explicit photos or videos of themselves or each other (e.g. by "sexting", internet chat or even Facebook posts) could unwittingly be guilty of producing and distributing child pornography.

"Sexting" can be a crime, depending on the age of the people sexting and whether the pictures would be considered offensive.

In NSW it is unlawful to access, possess or distribute "child abuse material". Under Commonwealth law, it is an offence to access, possess or distribute "child pornography material".

Child abuse material – NSW *Crimes Act*

The definition of "child abuse material" in the *Crimes Act* 1900 (NSW) is very broad. It covers any material that "depicts or describes" a person who is, appears to be, or is implied to be a child under 16:

- in a sexual pose or engaged in sexual activity;
- in the presence of a person (or persons) in a sexual pose or engaged in sexual activity;
- the private parts of a child; or
- as a victim of torture, cruelty or physical abuse,

in a way that a reasonable person would find offensive (section 91FB *Crimes Act*).

Family photos of little kids playing naked on the beach, tasteful artistic photography, or legitimate news stories about violence against children, would not amount to "child abuse material".

However, filming a schoolyard fight on a mobile phone, and then uploading that video on YouTube, could possibly amount to distribution of "child abuse material".

Sexting may also amount to distribution of "child abuse material", even if a young person is simply sending their own picture in a private SMS or email.

Penalties for offences involving child abuse material can be severe. The maximum penalty for producing, possessing or disseminating child abuse material is 10 years' imprisonment (section 91H *Crimes Act*); for using a child for the production of child abuse material also attracts a maximum penalty of 10 years' imprisonment; this increases to 14 years' imprisonment if the child is under 14 (section 91G).

Child pornography material – Commonwealth *Criminal Code*

Under the Commonwealth *Criminal Code*, there are a number of offences which relate to the use of a "carriage service" (a very broad term that includes the internet or a mobile phone network) for the transmission of "child pornography material".

Importantly, under Commonwealth law "child pornography material" is material that depicts a person who is or appears to be under the age of 18 (*not 16, as in NSW law*):

- in a sexual pose or engaged in sexual activity; or
- in the presence of a person in a sexual pose or engaged in sexual activity,

in a way that is offensive.

Penalties of up to 15 years' imprisonment apply for the transmission of such material (Commonwealth *Criminal Code*, section 474.19).

Other offences involving sexting

Even if the people depicted do *not* appear to be under 16 (in NSW) or under 18 (under Commonwealth law), violent or sexually explicit images could be regarded as offensive, and a person who distributes them could be charged with other types of offences, including "using a carriage service to menace, harass or offend" (see the section above on "cyber-bullying").

Sex offender register

One of the important consequences for a NSW person found guilty of distributing child abuse material is registration as a sex offender (known as a "registrable person" under the *Child Protection (Offenders Registration) Act* 2000 (NSW)).

A person who is registered in this way must report their relevant personal information (including their name, address, children residing in the household and affiliation with any clubs which have child participants) to the police each year. These obligations can continue for up to 15 years (or 7½ years for a person who was a child at the time of the offence).

Failure to comply with reporting obligations without reasonable excuse, or reporting false or misleading information, is an offence punishable by a fine of up to $5,500 or imprisonment for 5 years, or both.

5 Online grooming

"Grooming" refers to actions taken by a person to gain a child's trust, making it easier to engage in sexual activity with the child. Grooming is often done online, with offenders creating false identities and striking up "friendships" with children.

Grooming a child for sexual activity is a serious offence under NSW and Commonwealth law (see section 66EB *Crimes Act* 1900 (NSW); Division 474 Commonwealth *Criminal Code)*.

Under NSW and Commonwealth law, children cannot generally be found guilty of online grooming offences (although strangely there is a separate offence under the Criminal Code of grooming children outside Australia, apparently aimed at sex-tourism, which is not restricted to adults). However, victims of online grooming can unwittingly end up being charged with criminal offences, as the following case study shows.

Case study – Gina

Gina, aged 13, was groomed online by a man in his twenties posing as a teenage boy. After several months he persuaded Gina to strip and to perform sexually explicit acts in front of a webcam. He eventually persuaded her to get her younger sister involved.

It turned out that the perpetrator was an overseas resident who was being investigated by police in several countries for online grooming of young people. Police discovered images of Gina and her sister on his computer, and traced them back to Gina.

Gina was charged with several counts of indecently assaulting a child under 16. Faced with the photographic evidence, Gina pleaded guilty and was sentenced to probation. Gina is now on the "sex offender register" which requires her to report to police annually, and advise them every time she changes address for seven and a half years.

Gina is now making an application for Victims Compensation for the psychological harm caused to her by the online grooming.

6 Online fraud and identity offences

Fraud, whether committed online or not, is a serious offence under Part 4AA of the NSW *Crimes Act* and Part 7.3 of the Commonwealth *Criminal Code*.

The amount of financial data online, and the relative ease with which data can be accessed and used to obtain a financial advantage, make online fraud relatively common.

The law has also adapted to more sophisticated forms of cybercrime based around the possession and use of information (such as financial information) which do not fit well with traditional notions of fraud.

Example: "Phishing"

The practice of "phishing" is a common method of obtaining information which may then be used to commit fraud. "Phishing" usually refers to the attempts to acquire sensitive information (such as usernames, passwords, account numbers or credit card details) by masquerading as a trustworthy entity in an electronic communication.

A "phishing" attempt will usually take the form of an email that purports to come from a bank or financial institution to one of the bank's existing customers. The email will ask the customer to click a link that directs them to a website that mirrors the bank's own online login page, but which is created solely for the purpose of capturing customer account details. If the customer enters their username, password, or other relevant data, the "phisher" can then use that data to (fraudulently) obtain access to an account.

"Phishing" by itself, however, is not fraud - unless and until the "phisher" actually uses that information to obtain a financial advantage, no fraud has taken place.

Part 4AB of the *Crimes Act* 1900 (NSW) and Part 9.5 of the Commonwealth *Criminal Code* both set out a range of "identity offences" which capture modern practices such as "phishing" and identity theft, and are based on the use of "identification information".

"Identification information" is defined in almost exactly the same way at State and Commonwealth law, and includes things such as name or address, date of birth, a driving licence, passport, credit card, biometric data (e.g. fingerprints) or an ABN.

It is an offence under State and Commonwealth law to:

- make, use or supply identification information with the intention of committing, or facilitating the commission of an indictable offence (maximum 10 years' imprisonment under *Crimes Act* 1900 (NSW) section 192J; maximum 5 years' imprisonment under Commonwealth *Criminal Code* section 372.1); and
- possess identification information with the intention of committing, or facilitating the commission of an indictable offence (maximum 7 years' imprisonment under NSW *Crimes Act* section 192K; maximum 3 years' imprisonment under Commonwealth *Criminal Code* section 372.2).

7 Hacking and unauthorised access

Hacking is not a legal term. Generally speaking, "hacking" means the use of software or hardware to "break into" computer systems, usually with the intention of altering or modifying existing data, settings or code. Sometimes malicious in nature, these break-ins may cause damage or disruption to computer systems or networks.

Under the *Crimes Act* 1900 (NSW), the main offences around hacking are:

- unauthorised modification of data (with intent to impair access to, or to impair the reliability, security or operation of, any data held in a computer) (section 308D); and
- unauthorised impairment of electronic communication to or from a computer (section 308E) .

Both of these offences carry maximum terms of 10 years' imprisonment. Hacking may also result in a charge of destroying or damaging property under section 195 of the *Crimes Act*.

Sections 476-478 of the Commonwealth *Criminal Code* set out similar offences.

R v Boden [2002] QCA 164

In 2001, Votek Boden, a 49-year-old hacker, was accused of causing millions of litres of raw sewage to spill out into local rivers and parks killing marine life and causing offensive smells. He was motivated to revenge after he was refused a job at the plant.

Votek Boden was sentenced to two years' imprisonment after being found guilty of hacking into the Maroochy Shire's computerised waste management system.

8 Downloading and file sharing

Downloading and file-sharing may or may not be legal, depending on whether the file is protected by copyright. Breaching copyright is not always a criminal offence but there may still be legal consequences.

What is copyright?

Copyright is the exclusive right to do or authorise others to do something in relation to original literary, dramatic, musical or artistic work.

For example, copyright protects literary works (eg. novels, lyrics, reports, newspaper articles and letters); artistic works (eg. drawings, paintings, graphic art, photographs); musical works (eg, sheet music); computer programs; cinematographic films (eg. feature films, TV programs and music videos); and sound recordings (eg. music or voice recording).

Copyright does not protect ideas, information, styles or techniques, names, titles or slogans (although some of these things may be protected by trade marks).

Australian copyright law is set out mainly in the Commonwealth *Copyright Act* 1968.

Copyright applies automatically when material is created, and there is no system of registration in Australia. As soon as an original musical work, for example, is recorded in some way it is protected by copyright.

What rights do copyright owners have?

Copyright owners have a number of exclusive rights, including the right to control the reproduction of their material and the communication of that material to the public.

The right to control "communication" means that making material available online and transmitting over the internet is within the exclusive scope of a copyright owner's legal rights.

Copyright is infringed if someone, without the permission of the copyright owner, acts in a way that compromises the copyright.

Infringement of copyright may lead to a court granting an injunction, which is an order to stop using the copyrighted material; you may also be sued in court for compensation or to repay any profits you have made from infringing copyright (*Copyright Act* section 115).

In some circumstances, infringing copyright may also be a criminal offence. Generally, only infringements of copyright that involve commercial dealings or are on a commercial scale are criminal offences (*Copyright Act* Division 5). If you infringe a copyright which is a criminal offence you may be subject to a large fine or up to 5 years' imprisonment or both (see for example *Copyright Act* section 132AC(2)).

When is it OK to share or download material?

Owner of copyright may give "express" or "implied" permission to reproduce material. The owner may expressly give permission to download material and this may be written on the website itself, or the owner may give permission in reply to a specific request.

Implied permission is permission that can be inferred from all the circumstances and this is rare. An example may be websites which clearly contain "printer friendly version" or "email to a friend" buttons.

Just because material is available on a website, or contained in an email, does not automatically mean it can be freely downloaded. Internet users should check the website for permission, or terms and conditions that may apply to downloading material.

Similarly, just because a file can be found on a file-sharing network through P2P software does not automatically mean it can be freely copied, even for personal use. Permission from the owner of the copyright is needed before it is legal to copy he material. In Australia, there are at least three people who have ended up with criminal records as a result of illegal file sharing of music files.

Generally, the author of a work does not lose ownership of copyright by uploading the work, such as photos or text, to a website. People who wish to make copyright use of material later, for example uploading it to another site or copying the material, must ask the author of the work for permission. Certain websites may contain terms and conditions about ownership and use of copyright material. For example, the terms may entitle the website owner to allow certain uses of the uploaded material by visitors to the site.

Common examples:

BitTorrent: People who download copies of movies using BitTorrent are infringing copyright if they do not have permission from the copyright owner, *Roadshow Films v iiNet* [2011] FCAFC 23

YouTube: People using YouTube videos will generally need to ask permission first. This may be from the person who made the video, or from the music publishers and record companies where the video was originally made.

Facebook: People own all the content covered by copyright, such as photos and videos, that they post on Facebook. By uploading the information, however, the owner grants Facebook a license to use and display that content. This licence ends when the copyrighted content is deleted, unless it has been shared by others and they have not deleted it. For more information, see Facebook 'Terms'.

P2P: It is legal to download a file through P2P software if a copyright owner has given permission. Many of the major record companies offer music downloads through their sites or those of their partners such as iTunes. Uploading or downloading songs, software and movies without permission, or sharing pirated songs, software and movies is illegal.

Recording performances or movies: In venues such as theatres and concert premises, entry to performances is often subject to restrictions on filming. A man received a criminal conviction after he recorded The Simpsons Movie in an Australian cinema on his mobile phone and placed a copy on a US-based website before the US release date.

9 Further information and resources

Legal information

"Lawstuff" is the website of the National Children's and Youth Law Centre. It contains useful legal information for young people on a range of topics including camera phones, mobile phones, cyber-safety, internet downloading, pornography www.lawstuff.org.au

"Hot Topics: Cyberlaw" (2009 Hot Topics 70) is published by the Legal information Access Centre at the NSW State Library: http://www.legalanswers.sl.nsw.gov.au/hot_topics/pdf/cyberlaw_70.pdf

The Australian Institute of Criminology website contains extensive reports and papers, including literature reviews on cyber-stalking, grooming, sexual solicitation and cyber-bullying: http://www.aic.gov.au/crime_types/cybercrime/onlinevictimisation/children.aspx

The Australian Institute of Criminology has also published a paper on "Online child grooming laws" (July 2008): http://www.aic.gov.au/publications/current%20series/htcb/1-20/htcb017.aspx

The Australian Copyright Council is an independent, non-profit organisation that contains helpful Information Sheets and FAQs for copyright creators and users: http://www.copyright.org.au/

Staying safe online

"Bullying. No Way!" is a website developed and managed by Australian Education Authorities for use by Australian Government, Catholic and Independent School Communities. The website aims to provide nationwide resources to minimise bullying, harassment and violence at schools: www.bullyingnoway.com.au

The Australian Government's cyber security website provides information for Australian internet users on the simple steps they can take to protect their personal and financial information online: www.staysmartonline.gov.au

"Cybersmart", developed by the Australian Communications and Media Authority, is part of the Australian Government's cybersafety program. It provides activities, resources and practical advice to help kids, teens and parents on how to safely use the internet: www.cybersmart.gov.au

"NetSmartz Workshop" is an interactive, educational program that uses videos, games, activity cars and presentations designed to teach children aged 5-17 on how to be safer online:www.netsmartz.org

"ThinkUKnow Australia" is a website developed by the Australian Federal Police and Microsoft Australia. It contains useful information for young people on how to secure their social networking profiles, email and IM accounts. It also contains information for parents and teachers on how to stay in control of young people's online activities: www.thinkuknow.org.au/

"Smart online Safe online" is a website designed to educate young children to be smart online. It's campaigns target online threats such as predation, grooming, cyber bullying and identity theft: www.soso.org.au/

The NSW Public Schools Website contains articles for parents on how to deal with children who are victims of cyber-bullying: http://www.schools.nsw.edu.au/news/technology/cybersafety/index.php

Shopfront Youth Legal Centre
February 2013

Shopfront Youth Legal Centre
356 Victoria Street
Darlinghurst NSW 2010
Tel: 02 9322 4808
Fax: 02 9331 3287
www.theshopfront.org
shopfront@freehills.com

The Shopfront Youth Legal Centre is a service provided by Herbert Smith Freehills, in association with Mission Australia and the Salvation Army.

This document was last updated in February 2013 and to the best of our knowledge is an accurate summary of the law in New South Wales at that time.