The Shopfront
YOUTH LEGAL CENTRE

Cybercrime
(sexting, stalking, hacking, phishing and other online offences)

1 What is cybercrime?

We often use the word “cybercrime” to include a range of criminal activities involving computers or other 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.

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 you could be breaking the law, for example:

- Producing or distributing images that amount to “child abuse material” or child pornography (see part 4 below).
- Taking photos of someone’s private parts or sexual activity without their consent, or distributing these sorts of images without their consent (revenge porn) (see part 5 below).
- Filming a person without their consent for your own sexual gratification (C*rimes Act* 1900 (NSW) sections 91K -91M).
- Recording private conversations without consent (*Surveillance Devices Act* 2007 (NSW) section 7).
- Spying on people in private places (e.g. trespassing on private property to take photos, planting a hidden camera in someone’s room).
- Filming someone in a way that amounts to stalking, harassment or assault.
- Hindering police or other officers in the course of their duty. It is perfectly legal to film police officers, but it may be hindering if you are getting in their way and making it more difficult to do their job.

- Recording musical performances etc. (especially if you forward the video or post it online), or unauthorised copying or distribution of photographs or footage taken by someone else. In this case you could be breaching copyright, which is not always a criminal offence but still has legal consequences (see part 9 below).

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 conduct such as trolling (intentionally causing distress by posting inflammatory comments on blogs, social media sites and public forums) or doxing (publishing someone's personal information online).

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 5 years' imprisonment and/or a fine of $5,500. [NSW Parliament passed a new cyber-bullying law (known as 'Dolly's Law') which commenced on 1 December 2018. This makes it clear that intimidation and stalking offences can be committed using the internet or any other technologically assisted means.]
- 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 5 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 reasonable persons would find offensive (section 91FB *Crimes Act*).

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*). 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).

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. However, there have been some amendments to the law which make it less likely that young people will be criminalised for sexting.

Amendments to the *Crimes Act* in 2018

The *Criminal Legislation Amendment (Child Sexual Abuse) Act* 2018 has recently introduced several amendments to the *Crimes Act.*

These amendments came into force on 1 December 2018 and will help young people who are involved in sexting and similar behaviour.

Firstly, a person will not be guilty of possession of child abuse material under section 91H if the person was under 18 when in possession of the material *and* a reasonable person would consider possession reasonable having regard to:

- the nature and content of the material;
- the circumstances under which it was produced and came into the accused's possession;
- the age, intellectual ability, vulnerability and other circumstances of the child depicted in the material and the accused (both at the time of possession and arrest); and
- the relationship between the parties.

Secondly, new defences to offences against section 91H have been introduced:

- It is a defence to possession of child abuse material under section 91H if the only person depicted in the material is the accused (section 91HA(9)).
- It is a defence to the production and dissemination of material if the accused was under 18 at the time and is the only person depicted in the material (section 91HA(10)).

Finally, the approval of the director of Public Prosecutions (DPP) is required before charging a person under 18 with an offence under section 91G or 91H (sections 91G(6) and 91H(3)).

Child abuse 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 abuse material".

These extend to possession of child abuse material received via a carriage service, or possession with the intention of sending it online. There are also similar offences relating to sending child abuse material by post.

The definition of "child abuse material" under Commonwealth law is somewhat similar to the definition in the NSW Crimes Act, but it includes material that depicts a person who is or appears to be *under the age of 18* (*not 16, as in NSW law*).

Most of these offences carry maximum penalties of 15 years' imprisonment (e.g. Commonwealth *Criminal Code*, section 474.22).

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. 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").

Child protection register

One of the important consequences for a NSW person found guilty of distributing child abuse material is being placed on the child protection register (under the *Child Protection (Offenders Registration) Act* 2000 (NSW)).

Not all people found guilty of these offences are placed on the register, but most adults (and some juvenile offenders) will end up on the register for these types of offences.

A person who is on the register must report a large amount of personal information to the police each year. These reporting obligations can continue for up to 15 years (or 7½ years for a person who was a child at the time of the offence).

People on the register face restrictions on having contact with children, travel, and other activities.

Even when your reporting obligations are over, you are on the register for life.

For more information, see our fact sheet on *The Child Protection Register*.

5 Revenge porn

In 2017, NSW Parliament passed new laws to deal with the increasing problem of "revenge porn". Although revenge porn could have led to charges under existing laws (e.g. "use carriage service to menace, harass or offend"), the new laws are clearer and may include conduct not covered by other laws.

Under the *Crimes Act* 1900 (NSW) it is a crime to record, distribute or threaten to record or distribute intimate images of another person without consent.

"*Intimate image*" means an image of a person's private parts, or of a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy. It also includes an image that has been altered to appear to show a person's private parts, or a person engaged in a private act (for example, if someone's head has been Photo shopped onto a nude photo of another person).

The offences are:

- Recording an intimate image of another person without their consent. "*Record*" means to record, take or capture an image, by any means (*Crimes Act* section 91P).
- Distributing an intimate image of another person without their consent. "*Distribute*" includes to send, supply, exhibit, transmit or communicate to another person or make available for viewing or access by another person. It doesn't matter if the image was originally recorded with the person's consent (*Crimes Act* section 91Q).
- Threatening to record or distribute an intimate image of another person without their consent (*Crimes Act* section 91R).

All three offences carry a maximum penalty of 3 years' imprisonment or 100 penalty units (a fine of $11,000), or both.

The approval of the Director of Public Prosecutions (DPP) is required before charging a child under 16 with one of these offences.

Under section 91T, there are defences to offences under sections 91P and 91Q if:

- the conduct alleged to constitute the offence was done for a genuine medical or scientific purpose, or
- the conduct alleged to constitute the offence was done by a law enforcement officer for a genuine law enforcement purpose, or
- the conduct alleged to constitute the offence was required by a court or otherwise reasonably necessary to be done for the purpose of legal proceedings, or
- a reasonable person would consider the conduct of the accused person acceptable, having regard to each of the following:
    - the nature and content of the image,
    - the circumstances in which the image was recorded or distributed,
    - the age, intellectual capacity, vulnerability or other relevant circumstances of the person depicted in the image,
    - the degree to which the accused person's actions affect the privacy of the person depicted in the image,
    - the relationship between the accused person and the person depicted in the image.

6 Online grooming or procuring

"*Grooming*" means 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.

"*Procuring*" means trying to get a child to engage in sexual activity with you or someone else.

Grooming or procuring children for sexual activity are serious offences under NSW and Commonwealth law (see section 66EB *Crimes Act* 1900 (NSW); Division 474 Commonwealth *Criminal Code*).

From 1 December 2018, it is also an offence in NSW to groom parents or carers to gain easier access to children (section 66EC).

Under NSW and Commonwealth law, children cannot generally be found guilty of online grooming or procuring offences (although strangely there is a separate offence under the Commonwealth Criminal Code of grooming children outside Australia, apparently aimed at sex tourism, which is not restricted to adults).

Sometimes, 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 child protection register which requires her to report to police annually for seven and a half years. She also has to advise police of changes to her personal situation (e.g. her address), and to request permission if she wants to travel.

Note: amendments to the law that came into force on 1 December 2018 mean that the Children's Court has discretion to exempt people like Gina from the child protection register in the future.

7 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 ideas of fraud.

Example: "Phishing"

"Phishing" is a common method of obtaining information which may then be used to commit fraud.

"Phishing" usually refers to 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).

8 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 by revenge after he was refused a job at the plant.

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

***Soyke v R* [2016] NSWCCA 112**

In 2014, Justin Soyke was arrested in a police raid and charged with several counts of unauthorised access and modification to computer data after attempting to hack government and private company servers.

Soyke pleaded guilty to one count of "cause unauthorised modification of computer data" under section 477.2(1) of the Commonwealth *Criminal Code*, one count of "attempt to cause unauthorised modification of computer data" under section 477.2(1) of the Commonwealth *Criminal Code* and two counts of "unauthorised access to data with intent to commit serious indictable offence" under section 477.1(1)(a)(i) of the Commonwealth *Criminal Code.* He was sentenced to 3 years' imprisonment.

9 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 sometimes a criminal offence. Even if it's not a criminal offence, 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 (e.g. novels, lyrics, reports, newspaper articles and letters); artistic works (e.g. drawings, paintings, graphic art, photographs); musical works (e.g., sheet music); computer programs; cinematographic films (e.g. feature films, TV programs and music videos); and sound recordings (e.g. 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 work (for example, a piece of music) 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).

When is copyright infringement a criminal offence?

In some cases, infringing copyright may also be a criminal offence which can lead to a large fine or up to 5 years' imprisonment or both (see, for example, *Copyright Act* section 132AC(2)).

Generally, only infringements of copyright that involve commercial dealings or are on a commercial scale are criminal offences (*Copyright Act* Division 5). For example, you may be committing a criminal offence if you are selling pirated movies or music.

When is it OK to share or download material?

Owners 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 (peer to peer) 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 posting 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 licence to use and display that content. In many cases this would also include allowing your Facebook friends to share the content. This licence ends when the copyrighted content is deleted. However, in situations where the content owner has shared their content with another Facebook user (e.g. a photo) and that user has not deleted it, it will continue to appear on Facebook. For more information, see Facebook 'Terms'.

Instagram: When a person shares, posts or uploads content they grant Instagram a non-exclusive, royalty-free, transferable, worldwide licence to host, use, distribute, modify, run, publicly perform or display, translate and create derivative works of that person's content. This licence is cancelled upon deletion of the person's content or account.

Snapchat: When a person creates, uploads, posts, sends or receives content they retain whatever ownership rights in that content they had to begin with. However, that person grants Snapchat a licence to host, use, store, display, reproduce, modify, adapt, edit, publish and distribute their content.

Tinder: By creating a Tinder account a person grants Tinder a licence to use, host, store, copy, display, reproduce, adapt, edit, publish, modify and distribute information that the person makes available on their account. This licence ends upon termination of a person's Tinder account.

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. See https://www.smh.com.au/technology/pirated-simpsons-video-filmed-on-mobile-20070817-gdqvwl.html.

Even recording a school concert or play could land you in trouble. Recording any performance that happens to include copyrighted music or any other copyrighted creation is called reproduction and requires a licence from APRA AMCOS (the Australasian Performing Right Association and the Australasian Mechanical Copyright Owners Society).

10 Further information and resources

Legal information

The Law Handbook (currently in its 15th edition) is a practical guide to the law in NSW. It has chapters on copyright and Internet Law. The chapters can be accessed online at https://legalanswers.sl.nsw.gov.au/law-handbook-your-practical-guide-law-nsw.

Youth Law Australia (formerly called the National Children's and Youth Law Centre) has legal fact sheets and links for young people on a range of cyber-safety topics: https://yla.org.au/nsw/topics/internet-phones-and-technology/cyber-safety/

The Australian Institute of Criminology website contains reports on topics including sexting, identity theft and other types of online crime. Go to https://aic.gov.au/publications and search or browse under the topic of "cybercrime".

The NSW Police website has a page about child abuse material, procuring and grooming: https://www.police.nsw.gov.au/crime/sex_crimes/child_abuse/child_abuse_categories/faqs

Cyber-bullying and staying safe online

The Office of the Children's eSafety Commissioner has resources and practical advice for kids, teens and parents on how to safely use the internet: https://esafety.gov.au/

"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/

"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: http://www.bullyingnoway.gov.au/

ReachOut Australia has a webpage with strategies on how to deal with cyber-bullying. It also has links to agencies that can help someone experiencing cyberbullying: https://au.reachout.com/everyday-issues/cyberbullying

Bravehearts' website has tips on internet safety for young people, parents and carers; it also has details of internet safety contacts, links and resources: https://bravehearts.org.au/what-we-do/education-and-training/for-parents/keeping-safe-online/

The Alannah and Madeleine Foundation has developed eSmart, an educational program designed to improve cyber-safety and reduce cyber-bullying https://www.amf.org.au/what-we-do/esmart/

Privacy, scams, fraud, hacking, identity theft

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

Scamwatch, operated by the Australian Competition and Consumer Commission, provides news updates and alerts on recently discovered online scams. It also lets you know when companies have experienced data breaches: http://www.scamwatch.gov.au/

The Australian Cybercrime Online Reporting Network (ACORN) is a national policing initiative of the Commonwealth, State and Territory governments. It is a national online system that allows the public to securely report instances of cybercrime such as fraud and hacking. It will also provide advice to help people recognise and avoid common types of cybercrime: https://www.acorn.gov.au/about-acorn

Copyright

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

The Shopfront Youth Legal Centre
Updated March 2022

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

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 March 2022 and to the best of our knowledge is an accurate summary of the law in New South Wales at that time.