Will u friend me?
Legal Risks and Social Networking Sites

By

Dr Michael Henderson

Associate Professor Melissa de Zwart

Associate Professor David Lindsay

Mr Michael Phillips

MONASH University

funded by a grant from
Victoria Law Foundation
Grants
Publications
Education

This publication has been supported with a General Grant from the Victoria Law Foundation. Website: www.victorialawfoundation.org.au

Published by: Monash University

Faculty of Education
Building 6
Monash University
Victoria 3800
Australia

Phone: +61 3 99052868
Email: michael.henderson@monash.edu

First Published 2011

Disclaimer:

While the authors believe this publication will be of assistance to Victorian students, teachers and parents, they cannot guarantee that every single statement is without flaw of any kind. Therefore the authors disclaim all liability for any errors or for any loss or other consequences which may arise from any person relying on any information in these materials. This publication does not constitute legal advice.

Acknowledgement of sources:

‘Teen suspended over Morcombe site’, first published by ABC News Online, 26 February 2010, is reproduced by permission of the Australian Broadcasting Corporation and ABC Online. (c) 2010 ABC. All rights reserved.

The authors gratefully acknowledge Sarah Higginbotham for her superb illustration of the SNS privacy settings chart on Page 13.

Table of Contents

About the Victoria Law Foundation

Victoria Law Foundation helps Victorians understand the law and their legal systems. We are a not-for-profit organisation funded by the Legal Services Board Public Purpose Fund.

www.victorialawfoundation.org.au

About the authors

Dr Michael Henderson is a Senior Lecturer in the Faculty of Education, Monash University, Melbourne. In addition to the affordances and risks of social networking in education, his research and teaching interests lie in teachers' professional development, new learning technologies and online teaching and learning.

Associate Professor Melissa de Zwart lectures in the Adelaide Law School, The University of Adelaide. Her research interests are social networking, virtual worlds, copyright, the governance of online communities and the intersection between law and new communication technologies.

Associate Professor David Lindsay lectures in the Faculty of Law, Monash University, Melbourne. He is the author of International Domain Name Law (2007), and an expert in internet law, copyright and privacy law. His current research focuses on social networking sites, ISP liability and copyright policy.

Mr Michael Phillips is a doctoral candidate in the Faculty of Education, Monash University, Melbourne. His research focuses on the role of teacher identity, and the transformations of identity, in the planning and use of technologies across the curriculum.

Teacher Notes

About these Materials

This resource has been designed to aid teachers and parents in helping their students/children to critically consider the risks and legal implications of using social networking sites (SNS). This resource does not suggest that SNS should not be used. However, the research upon which this resource is based does strongly suggest that students do need to be actively engaged in meaningful discussions around their safety and the safety of the people in their networks.

This resource is a result of a large scale research project, funded by the Victoria Law Foundation, in which 1004 students, 204 teachers and 49 parents were surveyed from across Victoria. In addition, 58 students and 21 teachers were interviewed. The focus of the research was on students in years 7 to 10. However, this resource will be useful for any secondary school student. The purpose of the research was to better understand what and how SNS are being used by young people as well as the perception of risks held by all three groups of participants. This data was then considered in light of a comprehensive review of the legal risks related to the (mis)use of social networking sites, both within Australia and internationally.

What is Social Networking and what problems can it create?

Even if you haven't heard of the term "social networking sites" (SNS), it is likely you know and possibly even use some of them. One of the most common SNS is Facebook. However, not many people realise that there are many other sites such as YouTube which could also be considered a SNS.

SNS are websites that enable users to post information about themselves, their interests, likes and dislikes and to connect with other users, usually through the construction of a 'profile'. They may be open to the general public or only to subscribers. They may also have other elements such as live chat, messaging and interest groups. SNS have been defined in a variety of ways. For the purposes of this research, and founded on a broad synthesis of the research literature, SNS is defined as having three key characteristics:

- a website in which you can create a profile (eg. your own page) and you can post information about yourself, such as what you are doing, your interests, likes and dislikes; and
- on that profile other users are listed with whom you share a connection (eg. friends, followers); and
- that list can be seen by your 'friends' or others.

SNS have been the subject of rapid growth in Australia and overseas, particularly among young people. They have arguably become an essential part of life for

many Australian teenagers. Indeed, our study of 1004 students found that 95% of students in Years 7 – 10 use a SNS and that 93% of those students use Facebook (and often more than one SNS). For some students, social networking offers particularly valuable social benefits. For example, students who are in geographically remote locations or socially marginalised can network with like-minded peers. In addition, educational advantages to SNS are also increasingly being explored by teachers and researchers.

Most students and their teachers interviewed in this study understood the dangers associated with cyberbullying via the Internet; however, the majority of students appear to have a more limited understanding of other legal risks associated with SNS use, including:

- breaking the Terms of Service of which they have limited knowledge;
- copyright infringement;
- privacy, confidentiality and disclosure;
- defamation, and
- activity which constitutes criminal acts including harassment, identity theft and offensive material

Experts such as Jock Given (Professor of Media and Communications at the Institute for Social Research (ISR), Swinburne University) and Robyn Treyvaud (Cybersafety education consultant) agree that the legal risks posed to young people using SNS are significant. Their opinions, the surveys and interviews of students, parents and teachers, combined with a comprehensive review of research literature, SNS Terms of Service and international regulatory frameworks have been brought together to guide the development of this resource. This book aims to introduce you to key legal risks for young people and their teachers and suggests ways to protect your legal rights and uphold your legal responsibilities when using SNS in a personal or educational setting.

Curriculum Links

This book can be used as a general resource for engaging students in years 7 to 12 in a considered reflection of the implications of online activity in social networking sites. However, this book also has direct relevance for the Victorian Essential Learning Standards (VELS) and the Victorian Certificate of Education (VCE) Legal Studies.

VELS:

- **Interpersonal Development Domain**: The *Building social relationships* dimension requires that students learn about and practise the social conventions which underpin relationships and learn how to act in socially

responsible ways. Strategies for understanding, managing and resolving conflict are also an important focus.

- **Civics and Citizenship Domain:** The *Community engagement* dimension requires that students think critically about their own values, rights and responsibilities and those of organisations and groups across a range of settings, and explore the diversity in society.
- **Humanities Domain:** The *Humanities skills* dimension focuses on the development of basic inquiry skills including observation, the collection of various types of evidence, asking and answering questions about evidence and presenting information in a variety of ways.
- **Information and Communication Technology Domain:** The *ICT for creating* dimension requires students to examine the ethical and legal implications of using ICT in a range of settings such as the home, school and the workplace.

VCE Legal Studies

These curriculum links are drawn from the Legal Studies VCE Study Design (2011-2015).

- **Unit 1: Criminal law in action: Study Area 2**
  Through a consideration of contemporary cases and issues, students learn about different types of crimes and explore rights and responsibilities under criminal law.
- **Unit 2: Issues in civil law: Study Areas 1-4**
  Students examine the rights that are protected by civil law, as well as obligations that laws impose. They investigate types of civil laws and related cases and issues and develop an appreciation of the role of civil law in society and how it affects them as individuals.

Using these materials

The information and activities contained in this book have been designed to encourage students and their teachers and parents to critically discuss the benefits and challenges arising from the use of SNS. In particular it is hoped that this book will provide information that will stimulate a critical awareness of the potential legal risks faced by secondary school students when using SNS.

The nature of technologies and youth culture means that within a relatively short period of time SNS may no longer be functioning, relevant or popular in the forms which they take today. However, future technologies are likely to have many similar characteristics and consequently the legal risks are likely to be similar.

The book is divided into eight sections. Students should complete the first section since it includes several activities which will help students to understand some of the contextual details which are assumed in the subsequent sections.

Throughout the book there are opportunities for teachers to engage students in discussion and reflective activities. Many teachers may feel that they do not know enough about the field to effectively answer students' questions. However, the authors feel that any conversation is better than ignoring the issue. This book provides descriptions of risks, examples, and at the back of the book a list of very useful and informative websites designed specifically for students, parents and teachers.

Since the aim of this book is to stimulate critical thinking and further inquiry we suggest that teachers employ strategies which put the onus on students to research the issues, collaborate and negotiate in making decisions, and just as importantly articulate their thinking. Every teacher has their own favourite strategies. The authors would like to offer some of their own.

Think Pair Share

- The teacher sets a problem or asks for a response to the reading.
- The students think alone for a specified time.
- The students form pairs to discuss their ideas. (An extra step in the process is to then ask for several pairs to form into groups and share their best ideas.)
- The students then identify one idea which they share with the class or larger group. Rather than calling out their idea it may be useful to ask the pairs (or groups) to write their idea on the board, add it to a wiki, etc.
- A very important step in this process is the summary and synthesis of the students' ideas. The teacher or a student should somehow make sense of the ideas. For example, ideas can often be grouped, or seen as linked in some way. Once a summary is developed then a final concluding statement or group consensus can be sought.

Canvassing ideas

- Divide students into groups of 4. Give each group a piece of butcher's paper and ask them to either use a different coloured pen or to divide the paper into 4 sections.
- The 4 sections are for each student to write their thoughts about the topic. Students can either be asked to respond to the same question or you could ask them to each respond to one of four different questions or perspectives (eg. from a parent's perspective, from a students' perspective, etc.).

- After a set period of time each student gives their ideas verbally around the group. The role of the rest of the group is to affirm ideas which they support and to link ideas to their own. The presenting student can circle and annotate ideas which were received well from the group.
- Each group then reports the key ideas to the whole group, by posting their butcher's paper on the wall, writing the best ideas on the board or in some electronic format.

Plus, Minus, Interesting (PMI)

A PMI is used for talking about the positive, negative and interesting aspects of a lesson, concept or issue. Students are asked to write their ideas under three headings. This can be done in their books, on butcher's paper, as a class discussion with a scribe writing on the board, or on a wiki. The headings are:

- What I liked: Pluses (+)
- What I didn't like: Minuses (-)
- What I thought was interesting: Questions or thoughts

Interview

- Divide groups of four students into pairs.
- Each member of each pair takes turns interviewing the other.
- Each person then summarises the interviews (ie the ideas of his/her partner) with the rest of the group.

Active listening

Effective discussions are dependent on students' (and teachers') active listening. These strategies can be explained to students or placed around the walls of the classroom.

- Use effective nonverbal messages or body language. For example, do you maintain eye contact? Do you show that you are listening by nodding your head?
- Avoid early evaluations or reacting passionately. Let the speaker explain what they mean until you are able to paraphrase. Don't make judgements or get defensive. You can debate ideas later, active listening is all about making sure you understand their point.
- Practice paraphrasing. Paraphrasing is the art of accurately summarising (in your own words) what someone has said and then saying it back to them. This will clarify that his or her message was correctly understood and will encourage them to expand on their ideas.

- Ask questions. Active listeners ask questions to prompt speakers to clarify, expand and come to conclusions. Often speakers are still sorting out their ideas in their heads. A few good questions can help the speaker to sort out what it is that they are trying to say. Open-ended questions are the best. They require the speaker to convey more information.

Debate

This can be done in class or online in a discussion forum or other media. Choose a contentious issue (eg. a school or the government blocking Facebook). There could be more than two sides to the debate. Find out which way students vote and ask them to prepare arguments. They can then use the arguments in a turn-taking process to convey their arguments and rebut the points made by the opposing side(s). An online forum is excellent for this work since it is perfect for turn-taking, can be done outside of class time, can be watched and voted upon by a wider audience and since it is text based it allows students to carefully construct their argument. It also provides you with evidence for assessment.

Will u friend me?
Legal Risks and Social Networking Sites

1. Social networking and me

Using a social networking site can be lots of fun and it can be a great way to communicate with your friends and family. However it can sometimes get out of control and your actions can put yourself and your friends at risk. The risk is not just from strangers. This book describes many of the legal risks which you can find yourself in, even when you think you are just doing something for fun.

Read this ABC News article about an Australian student who thought his actions were just a joke but was suspended from school and even risked being charged with a crime.

> **Teen suspended over Morcombe site**
>
> *A teenage student responsible for a website offering to return missing Queensland boy Daniel Morcombe has been suspended from his school.*
>
> A Facebook webpage titled "If one million people join I will give back Daniel Morcombe" has attracted about 200 members and is listed as a group "just for fun".
>
> But the Morcombe family is not amused and wants the site taken off the internet.
>
> Police say the student could face charges of misuse of a telecommunications carriage service.
>
> Most of the posts on the group's wall condemn the page. "Grow up and show some respect - how can you possibly think that this is in any way funny?" one user wrote.
>
> Marist College Ashgrove principal Peter McLoughlin says the teenager responsible for creating the group has been suspended from the college with further disciplinary action possible.
>
> Daniel's mother Denise Morcombe says the group has been inundated with cruel remarks and swearing, and she is frustrated that it cannot be shut down. She says police and the school have been trying to get it shut down for almost a week.

> "I've been in contact with the principal of the school where the boy actually started it and he's been dealt with by the principal and police," she said.
>
> "But for some reason there's no administrator on [the group], and the boy can't shut it down, the school can't shut it down and the police can't shut it down.
>
> "So people are going on now to report it to Facebook, to try to get it shut down that way."
>
> *School apology*
>
> Mr McLoughlin says he has tried to contact Facebook to have the site removed but has not had a reply. He says the college has apologised to the Morcombe family and senior students have been given a lesson in human values and the dangers of the internet.
>
> Daniel was 13 when he was abducted from the Sunshine Coast in December 2003.
>
> His parents have sought a coronial inquest.
>
> More than 43,000 Facebook users are members of a legitimate group dedicated to finding Daniel.
>
> Reference: ABC News. (26 Feb, 2010). Teen suspended over Morcombe site. ABC News. Retreived 16/12/2010 from http://www.abc.net.au/news/stories/2010/02/25/2830443.htm.

Not only did this student do something which was potentially illegal, the problem was exacerbated by the way it got out of control. It is not uncommon for material which you place online to get out of your control.

Using the internet, a mobile phone or any other device brings with it a responsibility. A useful metaphor is driving a car. When you drive a car it is your responsibility to do everything you can to protect your own safety, the safety of your passengers and the safety of those people around you. It is the same when you are using SNS. Use this book to increase your understanding of the legal risks you face.

Task 1: *What websites are social networking sites?*

Do you have a profile on a social networking site (SNS)?

You might be surprised at what websites are classified as SNS. This activity asks you to look at a variety of websites that you may have seen or used. SNS usually have three characteristics:

- a website in which you can create a profile (eg. your own page) and you can post information about yourself, such as what you are doing, your interests, likes and dislikes; and
- on that profile is listed other users with whom you share a connection (eg. friends, followers); and
- that list can be seen by your 'friends' or others.

Another common feature of SNS is that your list of connections, and sometimes the world, can leave messages and other information on your page or in reply to your online activity (eg. uploading a video).

Question: Considering the above definition, which of the following websites do you consider to be SNS? Tick the answer that you think is correct.

Website	Yes	No	Maybe	Haven't heard of it
Facebook				
Tribe				
Myspace				
MSN				
YouTube				
Second Life				
Twitter				
Flikr				
Friendster				
Google				
Tumblr				

Are there any other websites that you know of that you think may be SNS? If so, please list them below:

_____

_____

Discussion: Compare your findings with others in your group or class and decide on which of the above are SNS.

Task 2: *How do YOU use SNS?*

As part of our research we asked Victorian students about the different ways they used SNS. You are now going to become a researcher and find out about the rest of your class (or family).

Use the table below to find out what your classmates do with SNS. Put your own answers in first and then ask your classmates. Once you have filled in the table you will then be able to compare the way your class uses SNS with year 7-10 students across Victoria.

What sort of things do your classmates put on their social networking sites?				
Category	**Tally**	**Frequency**	**Percent of class**	***Compare your findings to ours#***
This row gives you an example of how to use this table. In this example 6 students in a class of 20 students answered the question.	𝍸 |	6	$\frac{6}{20} \times 100 = 30\%$	
I post messages to a friend's page or wall				43.1%
I post photos / images to a friend's page or wall				15.3%
I send private messages to a friend within the social networking system				50%
I post pictures of myself on my own SNS				60.9%
I post pictures of friends on my SNS				52.6%
I upload music created by myself or other people (eg. singers/bands)				26.7%
I post other pictures (e.g of celebrities, general funny photos, etc.)				9.5%
I post video such as my own video clips, other movies, linking to youtube, etc.				38.5%

[#] 1004 students were surveyed but 47 students indicated they did not use SNS. This table is therefore based on the remaining 957 students from years 7 to 10 from across Victoria.

Discussion *(teachers may like to consider using one of the strategies outlined on pages 5-7)*

Can you see some possible risks in any of these activities? Don't just settle for the obvious ones. Consider the risks implied in this quote from a student who participated in our interviews.

> *I think with people using Facebook though, they share maybe a bit too much about themselves. They send pictures to people. I have a friend that sent a*

> *message to someone that said, "We're going away to Queensland in a week." And while they were gone to Queensland, that message must have gotten around, their house got robbed while they were gone. So, it's not always a good thing to tell everyone, and it might seem cool at the time, like, "Oh yeah, I'm going to Queensland and I'll tell you about it." But that can get around and turn out to be a negative thing.*

Make a list of all possible risks, especially legal risks, arising from the activities identified in the table as well as any others you can think of. Use the lists of other students to expand your own ideas until you have a complete list.

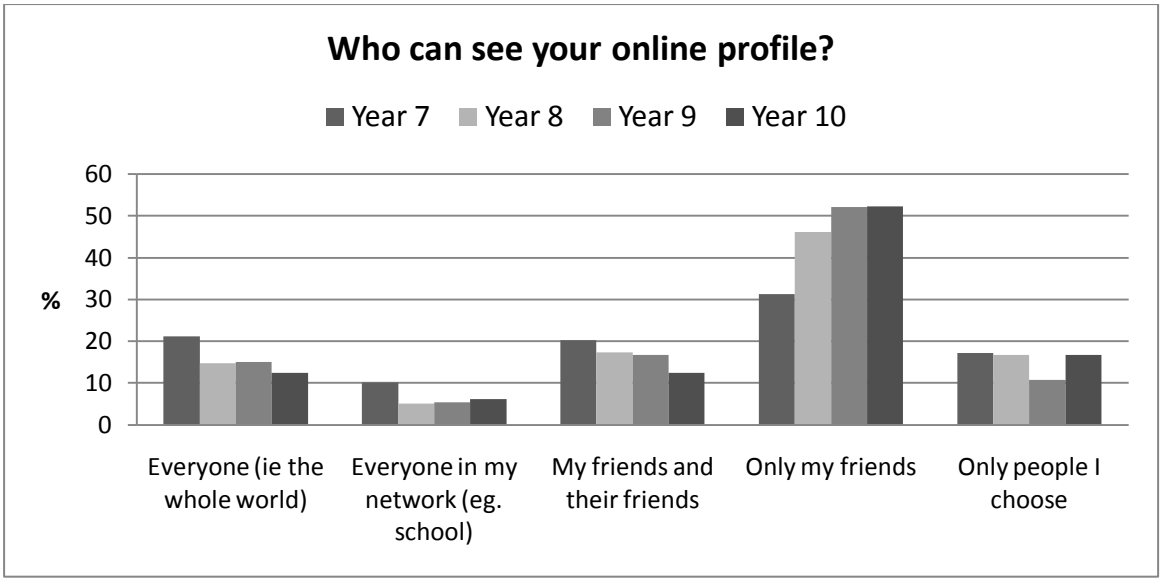
Task 3: *How private is your information?*

The popularity of SNS among school students gives rise to two different kinds of threats to privacy. The first set of concerns relates to the disclosure of personal information by yourself. The second set of concerns relates to the posting of information about you by other people.

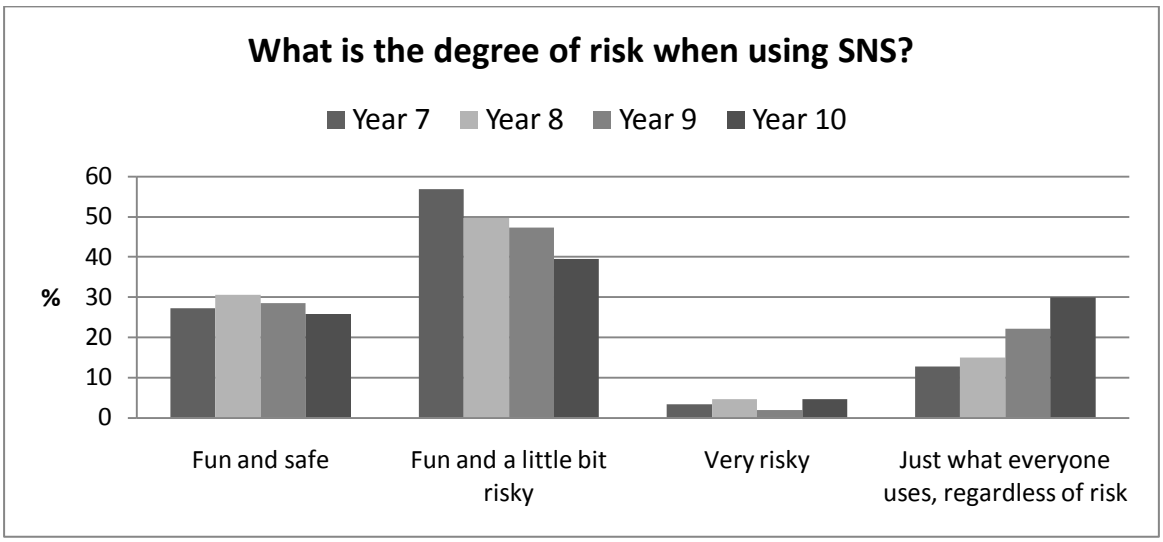
Many students believe that the in-built privacy settings of many SNS will protect them from any problems. While it is true that there are privacy settings that individuals can control, many people don't understand how these settings work and how they can be changed by the SNS (we will talk more about this in Section 2 of this book). Our research has also found that, despite awareness of privacy settings, many students don't protect their information on their sites.

Do you protect your information?

The students in our survey revealed a general trend, that students from years 7 to 10 are increasingly more selective in who can see their profile. Another way to say this is that the younger the student, the less selective they are. The graph below shows that over 50% of year 7 students have low privacy settings (for example their profiles can be seen by *everyone*, *everyone in my network* or *friends of friends*). However, even though year 7 students are less selective in who can see their profiles, almost 40% of year 10 students have similarly low privacy settings.



Choosing *everyone*, *everyone in my network* or *friends of friends* can lead to a number of risks, including legal risks. However, the students in our survey generally perceived their use of SNS to be safe or only a little bit risky. This graph below shows that over 20% of students felt that using SNS was safe. Over 40% of students felt that it was a little bit risky. Even more troubling was the increasing number of students between years 7 and 10 who simply used the SNS because it is "just what everyone uses, regardless of risk."



Questions:

- Do you use SNS simply because other people use it?
- Have you regularly check your privacy settings?
- Do you agree that year 7 students are at more risk than older year levels? Why?
- Do you agree that older year levels have a dangerous disregard for risk? Why?

How private is your information?

The most popular SNS (such as Facebook and MySpace) have a number of different privacy settings for your information. Usually each category of information such as photos, your contact information, your status updates, your list of friends and your age can have different privacy settings. The SNS will have a default privacy setting but you can usually change this setting to be more or less private.

Question: Based on your use of SNS (or that of your friends) what are the current privacy settings you have on your information? Shade in the sections of the chart below to indicate who can see what.

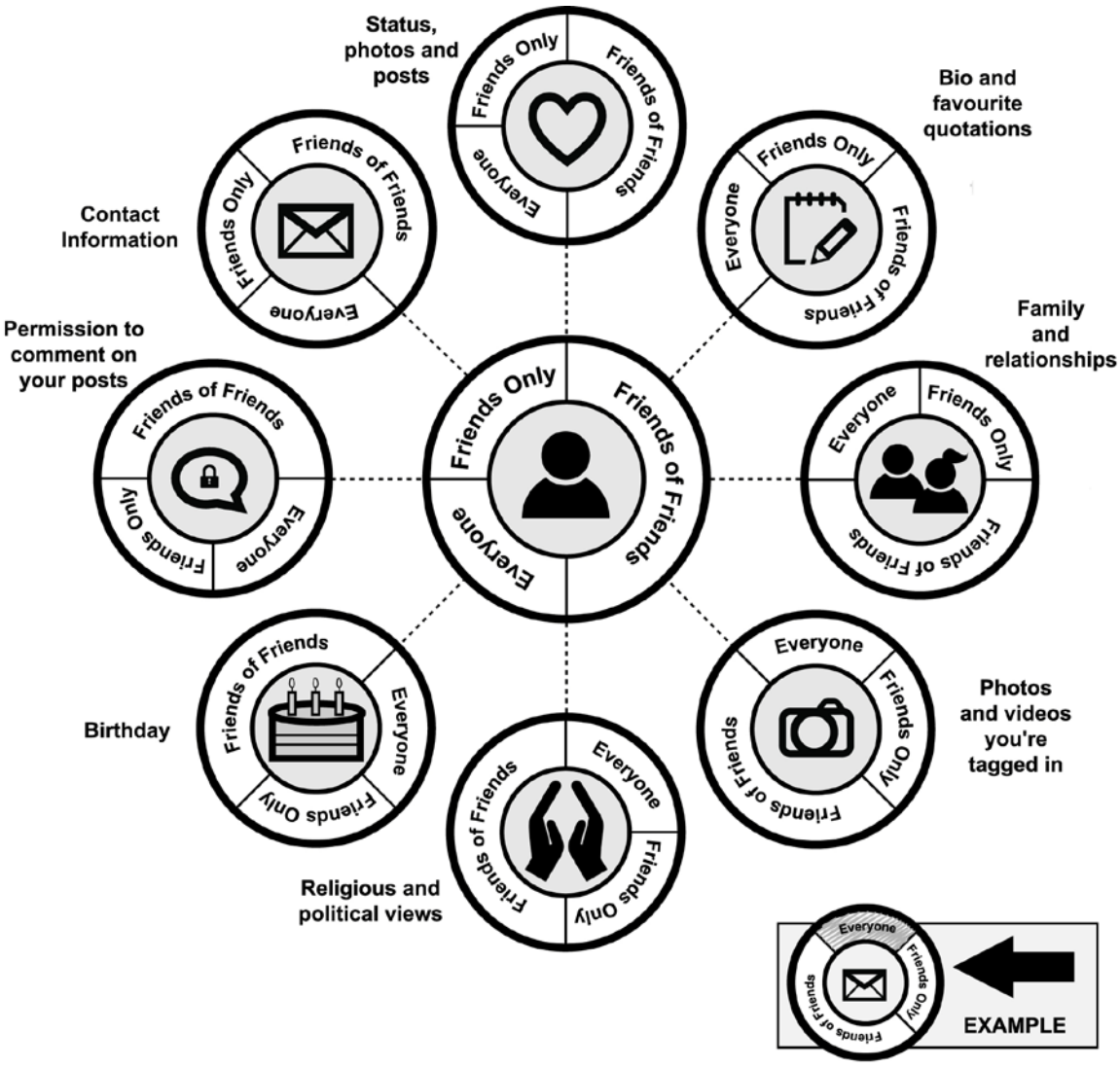


Illustration by Sarah Higginbotham

Question: Are you certain that the privacy settings you have indicated on this chart are actually correct? Check your privacy settings next time you access your SNS site. You might be surprised by what you find because the privacy settings don't always stay the same. We will talk about his more in the next section.

2. Terms of Service: What are you agreeing to?

Before you can start using a SNS you have to agree to be bound by the legal terms that apply to the use of that site. This means that you agree to be bound by the rules set by the operator of the SNS and any breach of those rules can lead to you being suspended or banned from that SNS (and as a consequence lose all of the content you have posted to that site).

All of these agreements are presented on a 'take it or leave it' basis. You are deemed to agree with these terms just by beginning, or continuing, to use the SNS. Most of these Terms of Service (ToS) are drafted in complex legal language and can be difficult to understand. But remember you do not have to have even read the ToS to be bound by them.

In addition, you should be aware that whilst you have a contract with the SNS provider, as does everyone else using the SNS, you do not have a contract with the other users. So, if they do something wrong to you, you have to ask the SNS provider to help you by enforcing the contract between the SNS provider and the other user. Thus disputes between users can be difficult to resolve, as SNS providers are reluctant to get involved in disputes between users.

You should be aware that some SNS are only suitable for people over a certain age, so many contain an age limit. If you lie about your age, your profile may be deleted. For example, if you are under 18 and represent yourself as being over 18, MySpace reserves the right to delete your profile. There are strict rules relating to the selection and registration of a user name; for example, you may not pretend to be another person.

The user is generally deemed to accept full legal responsibility for material that they post to the SNS, such as material that infringes copyright or is defamatory. Each provider has slightly different rules regarding removal of content, although each retains absolute discretion to do so. They also disclaim any obligation to monitor content. The ToS for Bebo, for example, say,

> We may, but shall have no obligation to remove or limit access to Materials originating from any Bebo user that we determine in our sole discretion are unlawful, fraudulent, threatening, libellous, defamatory, obscene or otherwise objectionable, or infringes or violates any party's intellectual property or other proprietary rights or these Terms of Service. Further, under no circumstances does Bebo have any obligation to check the accuracy or truthfulness of any Materials, nor to monitor any Member's use of the Bebo Service.

You should also be aware of the obligations that the providers accept with respect to removing material that you have posted and no longer want to appear, or accounts that you want to close. Most of the sites provide a warning that material may remain accessible post-removal or termination. For example, the ToS for Tumblr say,

> On termination of Subscriber's membership of the Site and use of the Services, Tumblr shall make all reasonable efforts to promptly remove from the Site and cease use of the Subscriber Content; however, Subscriber recognizes and agrees that caching of or references to the Subscriber Content may not be immediately removed.

One of the most important contractual obligations that you accept upon joining a SNS (and lots of other online services, such as online games) is that the user is obliged to keep their user name and password private and must not share the details with any other person for any reason. For example, the ToS for MySpace say,

> You are entirely responsible for maintaining the confidentiality of your password. You agree not to use the account, username, email address or password or another Member at any time or to disclose your password to any third party. You agree to notify MySpace immediately if you suspect any unauthorized use of your account or access to your password. You are solely responsible for any and all use of your account.

If you do share your password or user name with anyone, you may have your account suspended or terminated.

You should also be aware that each SNS includes a list of prohibited conduct which may result in banning or suspension, such as:

- Posting content which is offensive, incites or promotes racism, hate, bigotry or physical harm against any group or individual;
- Harassment or the encouragement of harassment of another person;
- Posting content which is sexually explicit, excessively violent or which exploits violence or sexual violence, contains nudity or links to an adult website or adult content;
- Posting content which promotes or facilitates illegal conduct or behaviour;
- Posting content which defames, abuses, stalks, threatens or otherwise violates the rights of other people;
- Posting false and misleading materials, including a false or misleading identity;

- Distributing viruses, Trojan horses, worms, or any other malicious code;
- Sending spam and other unauthorised advertising material, including pyramid schemes and chain letters;
- Posting or distributing material belonging to third parties;
- Using programs to harvest email addresses or solicit or collect personal information;
- Posting material disclosing the personal information of other people;
- Using any programs or content which may place an undue burden on the service.

All of the ToS include or link to a separate privacy policy, identifying what information is collected, how it is collected, what it may be used for, and how it will be stored and processed. The policies also identify who that information may be shared with, such as advertisers or apps providers. In some cases, if the user opts not to disclose some personal information, some aspects of the SNS may not be available to them.

Summary:

- In order to use any SNS you have to agree to the legal terms of service (ToS);
- You do not have to read those ToS to be bound by them;
- The ToS provide the rules you must abide by in using the SNS;
- These rules includes things like what you are allowed to post to the SNS (whether on your profile or someone else's) and how you must behave when using the SNS;
- You must keep your user name and password private and must not allow anyone else use your account;
- If you breach any of the ToS, you might be suspended or banned from using the SNS.

Activity: *The case against clicking "Next"*

The information below is taken from one of the interviews we did with groups of students from around Victoria. This is the actual text from the interview and indicates how young people could potentially be in legal difficulty simply by clicking 'next'.

Interviewer: Have you seen those updates that come through from Facebook every now and then saying "You've got to agree to these new terms of service"?
Student 2 – No.
Student 3 – No.
Interviewer: Are you, I certainly am, the sort of person that when you're installing new software or you're trying to download something you just go next, next, yes, yes, agree whatever?
[Students laughing]
Student 3 – Yep.
Student 2 – Yeah.
Interviewer: I'm exactly the same. So you don't even remember seeing those sort of things from Facebook come up?
Student 1 - No, I just click yes.
Interviewer: So it may have came up?
Student 1 - Yeah probably, but nobody reads them.
Interviewer: Would you be surprised to find out that when you click 'yes' you could be agreeing to many important changes. Without even knowing it, many people have agreed to new privacy settings, so that some of your data, which you thought was private was now on display to everyone?
Student 2 - Mm.
Student 3 – Mine's probably on display to everyone!
Interviewer: As he runs out to the computer.
[Students laughing]
Interviewer: Okay, do you think that sort of information would be helpful for people your age to know?
Student 1 – Yes.
Student 2 – Yep.
Student 3 – It might be a bit late for me!!
[Students laughing]

It is important to remember that SNS change their ToS. Sometimes this has significant implications for your privacy. Matt McKeon (see http://mattmckeon.com/facebook-privacy/) reports that in 2005 Facebook's default settings meant that your list of friends, wall posts and photos were available to only your network. However, after several changes to the ToS, in 2010 the default settings now allow all this information to be seen by all Facebook users but also by anyone in the world (eg. someone searching your name on Google could see your photos, lists of friends, wall posts, etc.).

Have you checked lately to see if your privacy settings are the same as what you remember?

Potential activities:

1. Design a brochure for students in your school that highlights the dangers associated with simply clicking 'next' when you are required to agree to SNS Terms of Service.
2. Create an instruction sheet for students in your school on how to maximise your privacy settings.

3. Copyright

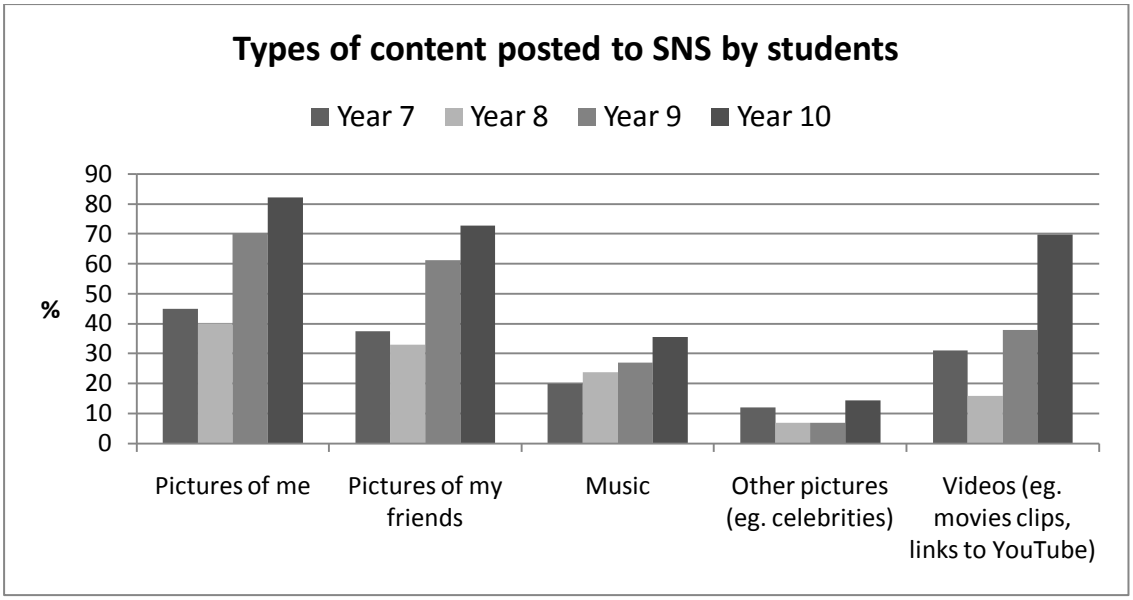
Most people who use SNS like to create profiles and other pages that represent their interests, hobbies, likes and dislikes and creative material such as photos of themselves, family and friends. The most common way to do this is through the display of images, movie and sound files. Most of this material, particularly that drawn from your favourite movies, TV shows, music and other popular culture is protected by intellectual property law, mostly copyright and trade mark. This means that if you cut and paste an image from your favourite film, or link to a music file from an unauthorised source, you can be liable for displaying that infringing material on your SNS profile.

Copyright protects all creative material, including books, films, music, poetry, drawings and broadcasts. It does not require registration or any other formalities and comes into existence at the time when the relevant creation is reduced to material form, i.e. when you write the story or draw the picture. Therefore most of the content that appears on web sites, including on SNS, is protected by copyright.

This means that if you want to make use of other people's creative material such as a photo or a music file, and unless you are permitted by one of the limited defences to copyright infringement, you need their permission or licence to do so. As there is no personal use exception to copyright infringement, you may need permission even if you are not making any money from the use.

If you do not have the relevant permission, licence or right to use the material, you will be infringing copyright. Infringement of copyright can carry with it both civil penalties, such as liability to pay damages, and criminal penalties, such as fines or even imprisonment. Criminal penalties are, however, unlikely unless someone is engaged in large-scale infringement.

Probably unsurprisingly, our research has shown that a number of secondary school students may be infringing copyright laws, as indicated by the types of materials they are posting to their profiles. The graph below indicates the percentages of students uploading different materials to their profiles. Pictures of themselves and of their friends would probably not infringe copyright (e.g. unless those photos were the creative work of someone else). However, the graph shows that students in years 7 to 10 generally increase in their posting of music and videos. If the student does not have the permission, license or the right to post those files they are then in breach of copyright and could be liable for civil penalties.



It is interesting to note that even if you embed a YouTube video clip in your Facebook page you need to ensure that you are allowed to do so. Just because Facebook and YouTube have a function that lets you embed videos on your page does not mean that you are allowed to do so.

In Australia, copyright is created and protected under the Copyright Act 1968 (Cth). Australia is a member of a number of international conventions and treaties which oblige Australia to grant copyright protection to materials created overseas. Therefore, even material which is downloaded from a US website may be protected under Australian law.

Copyright is infringed by doing one of the exclusive rights granted to the copyright owner. For example, with respect to a literary work, such as song lyrics, this includes the exclusive right to publish those lyrics on the internet, including on an SNS (Section 31(1) Copyright Act).

In order to infringe copyright you do not need to copy the whole thing. You need only take a 'substantial part' (section 14 Copyright Act) which is measured by quality, rather than quantity, i.e. how important that part is to the overall work. This means that you can infringe copyright even by using a relatively small piece of someone else's work, for example if you include a sound track, or clip from a movie or a computer game in a mashup video, which you then post to a SNS such as Facebook or YouTube.

You can also infringe copyright by 'authorising' someone else to do one of these acts. So that if you link to infringing material, and encourage other people to access that material, or download material such as a music or movie file, you may also be liable for copyright infringement.

For this reason, the ToS of all SNS prohibit displaying unauthorised material, or linking to it. Users are required to warrant that the material that they upload does not infringe the intellectual property rights of third parties

and service providers reserve the right to remove any material they believe is infringing. For example, YouTube frequently removes videos uploaded by users on the basis that it believes that they are infringing.

Further, several of the SNS provide for termination of the user's account in the event of multiple infringements of copyright. For example, the ToS for Bebo say,

> You may not post, modify, distribute, or reproduce in any way any copyright material, trademarks, or other proprietary information belonging to others without obtaining the prior written consent of the owner of such proprietary rights. Bebo respects the intellectual property rights of others and reserves the right to terminate any user's access to the Bebo Service according to these terms of use if Bebo is notified that such user's activities infringe the rights of third parties on more than one occasion.

So, you may find your account terminated if you repeatedly upload or link to infringing material.

In addition to copying material created by other people, SNS users also post a lot of content that they create to their profile and other pages, such as manga and other artwork, short stories, videos, and music. Creators of original content (popularly called 'user-generated content', or UGC) should also be aware of what they might be giving away when they post such content to the SNS. Many sites require you to give a full licence to the SNS provider, and sometimes other parties, to use such content without payment. It may also include the right to modify and commercialise such content.

The ToS for SNS include a range of licences relating to user-generated content. In general, the user grants a non-exclusive, worldwide, royalty free licence to use and distribute the content, and frequently a licence to modify, adapt and create derivative works using the content.

There are important differences in the sorts of licences users are required to give SNS providers. Some licences, for instance, only allow the service provider to use or copy the UGC in order to provide services to the user. For example, the ToS for Tumblr state that the:

> Subscriber shall own all Subscriber Content that the Subscriber contributes to the Site, but hereby grants and agrees to grant Tumblr a non-exclusive, worldwide, royalty-free, transferable right and license (with the right to sublicense), to use, copy, cache, publish, display, distribute, modify, create derivative works and store such Subscriber Content and to allow others to do so ("Content License") in order to provide the Services.

This should be compared to the even broader licence created in favour of Twitter, which allows rights of third party licensing and adaption, whilst the User retains all liability for any use of the content by Twitter or any third party. That is, whilst the ToS state that the User retains rights to content that they submit, the User grants Twitter,

> a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed).

The ToS then provide that the User is responsible for use of the Services, for Content they provide and,

> any consequences thereof, including the use of your Content by other users and our third party partners. You understand that your Content may be rebroadcasted (sic) by our partners and if you do not have the right to submit Content for such use, it may subject you to liability. Twitter will not be responsible or liable for any use of your Content by Twitter in accordance with these Terms. You represent and warrant that you have all the rights, power and authority necessary to grant the rights granted herein to any Content that you submit.

This licence is so broad that it may prevent you making any use of your own content in the future.

Summary:

- Copyright covers most creative works, such as pictures, music and video;
- Copyright protection is automatic and does not require registration;
- Generally, you can only copy or display copyright material with the permission (or licence) of the copyright owner, even if it is just for personal use;
- If you create copyright material and post it to a SNS you may have automatically granted permission to other people to use it;
- You can be banned from using a SNS if you infringe copyright.

Discussion 1: *SNS are designed to make us do certain things*

Have you filled in templates, answered questions, created lists, and posted other information just because the SNS had a space for it or asked you?

When you create an account on a SNS such as Facebook and MySpace you will be given a page with a variety of sections such as a place to put your photo, to post messages, link to videos, and show your lists of likes and dislikes. We call this a template.

Some people argue that the templates used by SNS encourage us to post certain types of information which can lead to risk, including copyright infringement. For instance, one researcher stated:

> The templates ask people to think of their identities in terms of popular culture references: with the requests for lists of favourite movies, television programs, books; with the capability to choose a song to play when the page opens; and with the capability to load images and video from other sources. We shouldn't be surprised that's how people respond to the template. (Williams, 2005, p.29)
>
> Williams, B. (2008) What South Park Character Are You?: Popular Culture, Literacy, and Online Performances of Identity. *Computers and Composition*, 25(1), 24-39.

The author of the above paragraph provides an argument why some people may put material on their profile page that infringes copyright.

In your own words explain the argument or defence the author is suggesting.

Do you think his argument is a valid? Do you think it would stand up in a court of law? Provide some reasons for your answer.

Discussion 2: *Do you know what you are giving away?*

This is a true story. Jason took a photo of his cousin Alison at a church fundraising day. He posted that photo of Alison to his Flickr page, without asking Alison. When he joined Flickr he accepted the standard user terms, which meant that he granted a Creative Commons licence to the world to make use of his photos without any permission or payment of a fee, provided that they attributed the photograph to him. Six months later, Alison's mum saw an advertisement for a mobile phone company with Alison's face on it. No one had sought Jason or Alison's permission and when Jason contacted the company they said they had copied it from Flickr and were using the image under a Creative Commons licence, which only required them to link to his Flickr site to acknowledge his authorship. *(more of the story can be read here http://www.out-law.com/page-8494)*

From a legal perspective who do you think is right in this example?

Discussion 3: *Be careful when being creative*

Oscar posted a video of himself to his Facebook page. The video, which he had filmed himself, showed him performing some martial arts moves and acrobatics, set to a 60 second sample of 'Disco Connection' by Isaac Hayes. Facebook has now contacted him and told him either to remove the video or get permission from the copyright owner to use the sound recording used as the audio track in the video.

Should he remove the video? Why or why not?

What else could Oscar do?

4. Privacy, confidentiality and disclosure

Privacy is recognised internationally as a fundamental human right. Despite this, it is not easy to explain what is meant by privacy. It can mean different things to different people. One of the best ways of explaining privacy, which has been accepted by the Australian Law Reform Commission (ALRC), is to divide it into the following four related concepts:

- *Information privacy,* which is about protecting your personal information, such as your medical records or credit history, when it is collected or used by government or business.
- *Bodily privacy,* which is about protecting your body against things like drug testing or physical searches, without your agreement.
- *Privacy of communications,* which concerns the security and privacy of telephone calls, email messages and other forms of communication.
- *Territorial privacy,* which is about setting limits on intrusions into your personal space, including video surveillance and ID checks.

Privacy is considered important because it can protect your freedom to make decisions for yourself. Privacy protection can also prevent other people from using your personal information without your agreement, in ways that might harm or embarrass you. For example, if someone uses a mobile phone to take a photo of you doing something potentially embarrassing, then posts it to Facebook, this may affect your reputation, and also how other people treat you.

Our research with Victorian secondary school students has shown us that although most students are aware of the issues of privacy, confidentiality and disclosure, many students still do not restrict access to their on-line SNS information (see Section 2 on ToS). In addition, many students do not check their privacy settings. For instance, a student who participated in our interviews reflected:

> *When I first belonged to Facebook, I just had everybody could see everything. I didn't have my number or anything. I had email and stuff. I didn't change it until a teacher sort of said, "Oh", like, we were doing something on privacy settings, one of them he saw it in class and I had to go and talk to him to get stuff or homework or something. I was watching it and I thought, 'well, I haven't even looked at that since I've made it'. This was a while ago now, a couple of years ago, but I haven't even looked at it since I've made it and then I looked at it and I had it, everybody could see everything, so then I changed it.*

While being unaware of your privacy settings can jeopardise your own privacy, it can also inadvertently result in unwelcome disclosure of information about your friends or other people. For instance one student in the interviews explained how students who do not have strict privacy settings can disclose information about their friends, such as through the tagging (naming) of people in photos:

> *Yeah, exactly. And so I have a friend, this really bugs me; I'm. like, get the picture off. She has all these pictures of her and her friends at school, and they're wearing their uniform and everything. And she has random people, and it could be anyone. And she has all these photos, and she tags other people, other friends, and they're, like, "Come on, can you please get that off?" And, like, they tag their friends.*

Not many students realised that their (mis)use of SNS can not only put themselves at risk but also put their friends at risk.

Australian law protects privacy, but it does so in ways that are complex and a bit haphazard. At present, you cannot take someone to court solely because they have invaded your privacy. Instead, you have to find some other reason for bringing an action. You can, for example, claim that someone has published or disclosed something about you that is confidential.

On this basis, the supermodel, Naomi Campbell, was able to sue a British newspaper for publishing photographs of her leaving a meeting of Narcotics Anonymous [*Campbell v MGN Ltd* [2004] 2 AC 457]. Similarly, in a Victorian case, a woman whose lover distributed copies of a video of them having sex was successful in claiming her confidentiality had been breached [*Giller v Procopets* [2008] VSCA 236 (10 December 2008)].

Someone whose privacy has been invaded might also be able to bring a case arguing that they have been defamed or that their property has been invaded by, for example, someone trespassing on their land. But the gaps remaining in the law have led to law reform bodies, such as the ALRC and the Victorian Law Reform Commission (VLRC), to recommend new laws to better protect privacy. These recommendations are controversial, and generally opposed by the media.

In addition to bringing an action in court, Australian law protects privacy in a variety of other ways. First, there are federal, state and territory laws that protect information privacy. These laws regulate the collection, handling and use of personal information, such as your name and mobile number, by government and business. There are, however, some important limitations on these laws. For example, they do not apply to small businesses or to individuals. There are also important differences between the various

federal, state and territory laws, which have led to the ALRC recommending major changes to harmonise the laws.

Secondly, there are laws that prevent people from intercepting private communications, such as phone calls and emails. Those laws permit the police to intercept or monitor private communications, but only if they have a warrant. Thirdly, there are state and territory laws that regulate the use of surveillance devices, such as a CCTV system or cameras in mobile phones, in public places.

There are differences between these laws in different parts of Australia. For example, in Victoria, devices like surveillance cameras can record any activity outside a building without consent, but consent must be obtained to record a private activity indoors. The VLRC has recommended some changes to the law to increase protection, such as prohibiting surveillance in toilets and change rooms, and preventing a person from recording an activity or conversation to which they are a party without the agreement of the other participants.

Privacy is also protected by the criminal law. For example, in Victoria it is a crime to engage in stalking or cyber-stalking [*Crimes Act 1958* (Vic) s 21A]. Cyber-stalking can occur when someone persistently contacts another person by phone or email, or persistently publishes material about that person on the Internet, with the intention of harming them, or causing them to fear for their safety.

Discussion 1: *Should we have the right to be forgotten?*

Think about this question and then discuss your ideas with another student or your teacher.
When you have made a decision, read the next paragraph and reflect on your reasons to see if any of them have changed.

> In November 2010, the European Commission suggested that there should be a legal 'right to be forgotten', that would give Internet users the right to ensure that embarrassing pictures, or other material, will be removed from Facebook or other social networking sites. The proposal came after the Commission received complaints that, under Facebook's privacy policy, when user profiles and photographs were deleted they were often not permanently removed. Viviane Reding, the European Commission Vice-President for Justice said, "Internet users must have effective control of what they put online and be able to correct, withdraw or delete it at will**.** In the recent public consultation on the review of the data protection rules, we were told that there should be "a right to be forgotten." We need

to look more closely at this idea. More control also means being able to move your data from one place to another, and to have it properly removed from the first location in the process. If I have my precious photos stored somewhere in the cloud, what happens if I want to change to another provider?"

References:
Viviane Reding, Speech to the American Chamber of Commerce to the EU, Brussels, 22 June 2010.
European Commission, 'A Comprehensive Approach on Personal Data Protection in the European Union', Brussels COM(2010) 609 final, 4 November 2010.

Discussion 2: *Should I share friends' details?*

This section has discussed some of the issues that involve privacy, confidentiality and disclosure. Most of us are aware that we shouldn't reveal personal details about ourselves whilst on-line, particularly to strangers. However, we should also ask ourselves:

1. *How much information should I share with people who are not complete strangers, for instance, friends of friends?*

In our research 20% of students did not like their photos being posted onto friends SNS. This raises two more questions you should try to answer:

2. *How can I find out if my friends give me permission to post information about them?*
3. *How much information about my friends should I include when I post status updates, photos or other information?*

Discussion 3: *Who do you trust to protect your information?*

Sometimes we need to also be cautious about not only what information we give to other people but also the kinds of information which we give to websites and services. Even when a service, such as Facebook, promises to protect our information, they can still make mistakes. Read the below article as an example of how your information can be shared without your knowledge or consent.

Facebook Caught Up in Privacy Scandal

18/10/2010

By Valerie Warrington

Facebook's top ranked applications have been transmitting information about users to advertising and Internet tracking companies, according to an investigation from the Wall Street Journal.

> Millions of Facebook app users will be affected in a scandal that involves transmitting people's names and sometimes their friends' names to outside companies, which goes against Facebook's rules. Even users who employ Facebook's strictest privacy settings are affected.
>
> Popular apps include games like FarmVille, Texas HoldEm Poker, FrontierVille, Café World, Mafia Wars, and Treasure Isle.
>
> Facebook developer Mike Vernal blogged on the subject and believed the sharing of personal information to be unintentional. "We take user privacy seriously," he wrote. "We are dedicated to protecting private user data. In most cases, developers did not intend to pass this information, but did so because of the technical details of how browsers work."
>
> It is not clear how long the privacy breach has been in place.
>
> On Sunday, a Facebook spokesman addressed the situation, saying that they are working on limiting the exposure to identifying information about users.
>
> "Our technical systems have always been complemented by strong policy enforcement, and we will continue to rely on both to keep people in control of their information," the Facebook official said.
>
> *Permission to reproduce this article has been granted by TheCelebrityCafe.com. The article was retrieved 16/10/2010 from: http://thecelebritycafe.com/feature/facebook-caught-privacy-scandal-10-18-2010*

Should companies be able to share your information with other companies?

Why are many people worried about companies sharing information about what you do online, who you communicate with, what you like, what you buy, when you go online, your age, gender, etc?

5. Defamation

Defamation is the area of law that protects your reputation against untrue statements about you. Your reputation is the way other people see you (this might be different from how you see yourself). As defamation protects reputation, it is not whether you are insulted or offended that is important, but whether some damage is done to the way other people think about you. Explaining the difference between insulting a person's character and damaging their reputation, Lord Denning famously said:

> A man's 'character', it is sometimes said, is *what he in fact is*, whereas his 'reputation' is *what other people think he is. (Plato Films Ltd v Speidel* [1961] AC 1090, 1138.)

In Australia, defamation is unlawful under State and Territory laws which, since 2006, are largely, but not completely, uniform. Most defamation cases are civil actions, involving a person who claims to have been defamed suing the person who has made or published allegedly defamatory statements. Although prosecutions are rare, defamation is also a criminal offence.

Defamation occurs when someone publishes something that is defamatory about another person. There is a lot of complex law on when something is defamatory, with it sometimes being said that it is anything that exposes a person to "hatred, ridicule or contempt" (*Parmiter v Coupland* (1840) 151 ER 340, 342 per Baron Parke), or that it is "anything which is likely to cause ordinary decent folk in the community, taken in general, to think less of" the person (*Gardiner v John Fairfax* (1942) 52 SR(NSW) 171, 172 per Jordan CJ.).

As the meaning of a statement can depend upon the context and the circumstances in which it is said, it is impossible to generalise about what might be defamatory. But the following are examples of some things that have been held to be defamatory:

- A magazine photograph of the rugby league player, Andrew Ettingshausen (or 'ET'), in a shower that included his partially obscured genitals;
- Suggestions made in a newspaper that a person had smelly feet or was constipated;
- Allegations that the flamboyant Sydney businessman, Rene Rivken, had a sexual relationship with his male chauffeur;
- Photographs of the actors who played Harold and Madge Bishop in *Neighbours*, which were published by an English magazine, and which consisted of the faces of the actors superimposed on the bodies of two people engaged in a 'bondage' session;

- An article untruthfully suggesting that the then captain of the West Indies cricket team, Clive Lloyd, had engaged in match fixing; and
- A current affairs television program alleging that a doctor was an 'abortionist'.

Defamation is committed whenever defamatory matter is communicated to someone other than the person being defamed, provided that the person being defamed is sufficiently identified. Australia's defamation laws define 'matter' broadly to include: articles, reports and advertisements in newspapers and magazines; anything communicated by means of television, radio or the Internet; letters, notes or any other writing; pictures or gestures; or anything at all that can be communicated to a person. Defamation can therefore be committed whenever someone reads a defamatory comment, or views a defamatory photograph or picture, on a SNS, such as Facebook.

Defamation does not prohibit all actions that may damage someone's reputation, as the protection of reputation must be balanced with protecting freedom of expression. Consequently, there are some very important defences to actions for defamation. For example, something is not defamatory if it can be shown that it is substantially true. Moreover, a defendant can argue that an apparently defamatory statement is really fair comment, or an honest opinion.

Although you might not think it is very likely that someone, like a Facebook friend, would take you to court for defaming them, people are actually very sensitive to defamatory material. For example, quite a lot of disputes have arisen from statements made in community magazines or newsletters produced by small clubs. You therefore need to be cautious whenever you write something about someone else, or post a photograph of someone else, to a SNS.

Case Study: *Defamation by Facebook*

Read this real life case study and then tackle one of the activities below.

> Christopher Cross, a 19 year old diesel mechanic from Yorketown in South Australia, set up a Facebook group called "Piss Off Mark Stuart". The Facebook page targeted one of Yorketown's two police officers, Senior Constable Mark Stuart, who had been active in charging Yorketown locals for driving offences, such as drink driving or driving defective cars. The page included photographs of the police officer, photographs of his children, the location of his house, and 43 posts from members of the Facebook group. Many of the posts about Constable Stuart were offensive or highly defamatory. After an investigation by the Commercial and Electronic Crime Branch of the

South Australian police, Cross was charged with criminal defamation. Given the overwhelming nature of the evidence, Cross pleaded guilty and was convicted, being placed on a two year $500 good behaviour bond. After his conviction, Cross said he "didn't realise you could get in trouble for things on the internet".

Reference: Nigel Hunt, 'Teen guilty of Facebook slur', *Sunday Mail (SA)*, 22 November 2009.

Using the case study either do one or the other of the below activities:

- Have students construct a mock court case with one group of students working as Christopher Cross' legal defence team with the other group of students acting on behalf of the Commercial and Electronic Crime Branch of the South Australian police. Depending on the time available, this could be done in an informal manner with students simply standing up in front of the class to present their 'case' with little preparation.
- Alternatively class time can be dedicated to allow each team to prepare their arguments from the case study and the defamation section of this book. In addition, students can examine the case study for other potential legal issues for example disclosure or copyright infringement.

6. Criminal Laws and Harassment

There are a number of criminal laws that can potentially apply to activities on SNS, which are usually described as cybercrime laws. There are three main categories of cybercrime laws, namely, laws outlawing identity theft, serious harassment or publishing offensive material.

Identity theft

Identity theft involves assuming someone else's identity, usually for the purpose of committing a criminal activity. The Australian states and territories have introduced new laws that make it an offence to assume or steal another person's identity. For example, in Victoria, it is a criminal offence to make, use or supply a false ID with the intention of committing on offence; to possess a false ID with the intention of committing an offence; or to possess equipment for making a false ID with the intention of committing an offence. Consequently, it is a crime to take another person's credit card details with the purpose of buying things without the permission of the credit card owner. There are other, more traditional, offences that can be committed by the use of a false ID, including theft, criminal fraud or forgery.

In a survey of 460 students in years 7 to 10, over 13% of students identified hacking and identify theft as serious risks of using SNS. Unfortunately, the other 87% of students were mistaken about how serious the risk of identity theft is. In an interview a teacher reported:

> "I have come across a student who showed me a site that was a mirror image of his own. And that person, whoever created it, tried to get his friends to add him on, pretending to be that person. So, yes, you do get imposters there."

Sometimes identity theft is committed for the purposes of bullying or other malicious purposes. Identity theft can also be motivated by people who want to use the identity for financial gain. SNS have now been identified as an easy way of collecting information about someone in preparation of identity theft. The ABC News reported that:

> "Officers say in the past criminals would have to go through a person's garbage to get their personal information. Now all they need to do is log onto a social networking site like Facebook. The Police Minister,

> Michael Daley, says social media and networking sites are now routinely searched to compile information on a targeted person... Identity fraud costs Australians nearly a billion dollars a year."
>
> *ABC News (2010) "Sophisticated identity theft warning." Retrieved 16/12/2010 from http://www.abc.net.au/news/stories/2010/07/27/2965646.htm*

Harassment

Federal criminal law includes a number of offences which involve the criminal misuse of telecommunications, including the Internet. The most important crimes are:

- Using a telecommunications network with the intention of committing a serious offence, such as criminal fraud or stalking;
- Using a telecommunications service to make a threat to kill or cause serious harm; and
- Using a telecommunications service to menace, harass or cause offence to a reasonable person.

Each of these offences may be committed by use of technologies such as mobile phones or via SNS. In addition to offences for using the Internet to threaten or harass someone, it is an offence to use telecommunications services, including the Internet, for promoting or inciting suicide. As a result, it is important to understand that rash statements posted to an SNS, which might involve threatening someone or encouraging them to commit suicide, can have potentially serious consequences.

Case study: *Agostino v Cleaves*

Read the summary of this real life court case and then answer the question.

> A 19 year old defendant 'Simon' became a Facebook friend of 'David's' through a mutual acquaintance . Simon had been in a relationship with a young woman that had ended some time before. David started a relationship with the same young woman, and shortly after began receiving threatening messages on his Facebook personal profile site from Simon. One message read, "You're a dead dog, … don't worry ill (sic) be taking you for a drive really soon don't forget I know where you live". David, who was concerned for his safety, ended the relationship with the young woman. Nevertheless, Simon continued to send threatening messages to David and his friends and relatives. Simon also posted digital photographs to his own Facebook site, one showing himself holding a replica silver pistol, and one

showing the silver gun on a table with five bullets. David contacted the police, who laid charges.

Simon was convicted of the criminal offence of using the Internet in a way that reasonable people would think was menacing under s 474.17(1) of the *Criminal Code 2005* (Cth). As he was over the age of 18 years, and had a criminal record, he was sentenced to six months imprisonment. An appeal against the sentence was dismissed. [*Agostino v Cleaves* [2010] ACTSC 19, 3 March 2010].

Reflection: Have you ever seen someone make a threatening comment online, even if you think they meant it as a joke? Imagine how a parent, the police or a judge might read that comment a month or even a year later. They may not see the joke, and just see the harsh words.

Question: Can you find at least two possible answers to the following question?

> *What makes social networking sites potentially more confronting, threatening or embarrassing than other online communication such as emails?*

Hint: the case study does not directly answer this question but may give you some ideas.

SNS are not necessarily more risky but they do have some peculiar features such as allowing the instant sharing of comments, photos, videos, and links across a network of 'friends' without the control of the victim. This means that the comments are semi-public, the people who see the comments are most likely important to you, that you do not always know exactly who sent the comment and, depending on your permission settings the comment could be made by a friend of a friend. Also they provide a semi-permanent record of the conduct, unlike, say, a practical joke at a party or made at school at lunchtime face to face.

Offensive material

Federal criminal law includes a number of offences that cover the use, access, distribution, production and supply of child pornography online. Child pornography is essentially material that is of a sexual and offensive nature that involves people under the age of 18 years. While accessing child pornography online is a federal crime, production and possession of child

pornography are crimes under the laws of the states and territories. The federal crimes extend to child abuse material, which is material that depicts cruelty or physical abuse to a person under the age of 18 years in a way that would be offensive to a reasonable person.

There are harsh penalties for child pornography offences. It is important to understand that posting material that might be classified as child pornography or child abuse, such as photos involving sexualised nudity or cruelty, can have very serious consequences. This is the case even if the person consented to their photo being taken, and if the photo was taken by a person who is themselves under 18.

In addition to child pornography offences, federal criminal law creates offences for people who are over the age of 18 years to use the Internet for luring or grooming people under the age of 16 years for sexual purposes. These crimes are aimed at preventing adults from taking advantage of young people online.

Discussion: *when things get out of hand*

Read the above section on Offensive Material and decide if anyone in the below scenario could be charged with a crime.

> James received a MMS message on his mobile phone which included a partially-nude photo of Janet. Janet had taken the photo but had sent it to John's mobile phone, her boyfriend, who had encouraged her to do so. He had said that he would leave her unless she'd do it. James didn't know Janet and didn't even know who sent it to him. In fact, John had sent it to him by mistake, he had thought he was sending it to a friend of his. Even though James did not know who had sent it to him he thought it would be pretty funny to post the photo onto his Facebook site for his friends to see. James hadn't changed any of his privacy settings from the default settings when he joined Facebook in August 2010. A couple of James' friends had downloaded the photo to their computers and phones.

Case Study: *victim or perpetrator?*

American law courts have seen a distressing increase in children being charged with disseminating offensive material. Dahlia Lithwick, for the Slate website, had reported in 2009 that:

> Last month, three girls (ages 14 or 15) in Greensburg, Pa., were charged with disseminating child pornography for sexting their boyfriends. The boys who received the

> images were charged with possession. A teenager in Indiana faces felony obscenity charges for sending a picture of his genitals to female classmates. A 15-year-old girl in Ohio and a 14-year-old girl in Michigan were charged with felonies for sending along nude images of themselves to classmates. Some of these teens have pleaded guilty to lesser charges; others have not. If convicted, these young people may have to register as sex offenders, in some cases for a decade or two.
>
> Reference: Lithwick, Dahlia. (14 Feb, 2009). What to do about teens and their dumb naked photos of themselves. *Slate.* Posted Saturday, Feb. 14, 2009. Retrieved 16/12/2010 from http://www.slate.com/id/2211169/

Young people have been charged whether they are senders, forwarders or recipients of such photos, or have simply saved the photos.

The same risks are also in Australia:

> Experts say few teens appear to grasp that they can be charged under tough laws created for paedophiles - or branded as registered child sex offenders - just for sending or even possessing naked images of themselves or other under-age teens. Only last week a Mackay teenager was spared prosecution for possessing a photo of a topless 15-year-old girl on his phone by a judge after he was charged with possessing child exploitation material.
>
> Reference: Hearn, Louisa. (28 Oct, 2010). Teens in trouble for sexting like the stars. *The Age.* Retrieved 16/12/2010 from http://www.theage.com.au/digital-life/mobiles/teens-in-trouble-for-sexting-like-the-stars-20101028-174sn.html

Question: Who are the victims in these two cases and who are the perpetrators?

7. Concluding comments: Are Xbox and Facebook different?

This book has described a number of ways in which students may be at risk when using SNS. These include:

- breaking the Terms of Service of which they have limited knowledge
- copyright infringement
- privacy, confidentiality and disclosure
- defamation, and
- activity which constitutes criminal acts including harassment, identity theft and offensive material

Understanding the risks is only a part of the story. You need to also build on your strategies to keep yourself and your friends safe. The next section includes a number of very useful sites which outline a number of warning signs, risks, and strategies for being safe online. We particularly recommend the Cybersmart website which has been created by the Australian Government and the Australian Communications and Media Authority.

In addition, these risks do not just apply to SNS. Blogs, emails, texting and even online gaming sites can all be places where copyright infringement, harassment, disclosure and other risks occur. Not many people realise that when you play World of Warcraft, Second Life, or other online games including those through Xbox live and other internet enabled console games that you could be exposed to some of the same risks as in Facebook.

It would be a useful exercise for you to list every single game (eg. World of Warcraft), website (eg Facebook) or device (eg. mobile phone) which lets you share information with other people and then consider if each of the risks outlined in this book are applicable.

8. Useful Internet Sites

Victoria Law Foundation
http://www.victorialawfoundation.org.au/
Victoria Law Foundation is a not-for-profit, independent statutory body that helps Victorians understand their legal system and the law.

Victorian Department of Education: Learning Online
http://www.education.vic.gov.au/management/lol/
The Department's Learning Online website provides policy advice, resources, classroom activities and professional learning actions to support the safe and responsible use of digital technologies.

ACMA – Cybersafety outreach
http://www.acma.gov.au/WEB/STANDARD/pc=PC_311102
The Australian Communications and Media Authority (ACMA) provides a program of cybersafety presentations in metropolitan and regional centres throughout Australia.

Cybersmart
http://www.cybersmart.gov.au/
Cybersmart provides activities, resources and practical advice to help young kids, kids, teens and parents safely enjoy the online world.Cybersmart also offers training and resources for schools and materials for library staff. Developed by the Australian Communications and Media Authority, Cybersmart is part of the Australian Government's cybersafety program.

CyberSavvy
http://www.stride.org.au/cyber-savvy.aspx
CyberS@vvy has been developed by Stride to tackle the growing issue of cyber-bullying in schools. The program, like Stride's other anti-bullying programs, looks at the problem in a holistic way, involving young people as part of the solution rather than demonising them or the technology they use

Think U Know
http://www.thinkuknow.org.au/site/index.asp
ThinkUKnow is an Internet safety program delivering interactive training to parents, carers and teachers through primary and secondary schools across Australia using a network of accredited trainers. Created by the UK Child Exploitation and Online Protection (CEOP) Centre, ThinkUKnow Australia has been developed by the Australian Federal Police (AFP) and Microsoft Australia.

iKeepSafe.org
http://www.ikeepsafe.org/
To give parents, educators, and policymakers the information and tools which empower them to teach children the safe and healthy use of technology and the Internet.

Cyber Safe Kids
http://www.cybersafekids.com.au/
Cyber Safe Kids is a resource for online safety and digital citizenship resources and is managed by its founder Robyn Treyvaud an educational leader and online safety educator working with schools and communities across Australia and the Asia Pacific region.

Privacy Victoria
http://www.privacy.vic.gov.au
Privacy Victoria regulates how Victorian government agencies and local councils handle personal information. Of particular interest to teachers, parents and young people is their website which contains useful resources and guidance regarding managing privacy, understanding the law, and using Social Networking Sites.