Section 2 Privacy

Contents

Overview

This guide seeks to help staff understand the issues and the relevant legislation and students appreciate their legal obligations, their legal rights and the potential dangers ignoring privacy concerns can bring. The textual material is intended to provide teachers with the foundation expertise to guide student discussion and answer questions.

What is privacy?

The word 'privacy' means different things to different people. Your idea of privacy is likely to be different from the ideas of your family and friends. Privacy of information recorded by large organisations and government agencies about individuals is protected to some extent by federal and state laws. Privacy, in the sense of, an individual’s right to be free of unlawful public attack on their reputation is protected by Victorian Law under the *Charter of Human Rights and. Responsibilities Act 2006*.

There are less obvious forms of privacy, ones that can have real world consequences. Collecting information about an individual from sources online is increasingly easy. This type of information we leave behind is called a *Digital Footprint* and while the information individuals give to directly to organisation is to some extent protected by law, the information we leave behind unintentionally or otherwise is not. Individual internet users are identified and tracked every day, often without their knowledge by thousands of commercial organisations.

An individual's digital footprint may be harvested by other internet users to track individuals down in the physical world. While such behaviour may contravene Cyberstalking laws in most states, if an internet user has malicious intent, the probability of detection prior to the potential for harm being realised is extremely low.

All internet users, but in particular young people, should be particularly vigilant about their own privacy and the right of privacy of others.

Privacy Legislation

Types of privacy

The type of privacy covered by the Privacy Act and our Office is the protection of people's personal information, this can include privacy issues associated with *information* about your location, your health and body and your communications with others. Other types of privacy can include territorial privacy and physical or bodily privacy and privacy of your communications. Most privacy laws are more correctly described as data protection laws, as they are limited to regulating the handling of personal information by organisations.

What is personal information?

Personal information is information that identifies you or could identify you. There are some obvious examples of personal information, such as your name or address. Personal information can also include medical records, bank account details, photos, videos, and even information about what you like, your opinions and where you work - basically, any information where you are reasonably identifiable.

Information does not have to include your name to be personal information. For example, in some cases, your date of birth and post code may be enough to identify you.

To be precise, the Privacy Act definition of personal information is:

"... information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

What does the Privacy Act cover?

The Information Privacy Act 2001 (Victoria) regulates how your personal information is handled. For example, it covers:

- how your personal information is **collected**
- how it is then **used** and **disclosed**
- its **accuracy**
- how **securely** it is kept
- an individual's general right to **access** that information.

Under the IPA, State government organisations, local councils and private sector organisations acting as contracted service providers to the Victorian government are all bound to protect the privacy of people's personal information. "Personal information" means recorded information which can identify someone.

Sensitive information

There are certain types of personal information that are especially important to individual privacy, such as health or medical information. This information is classed as 'sensitive information' under the Privacy Act. The Act has particular provisions that require that sensitive information be managed with particular care.

"**sensitive information**" is defined as information or an opinion about an individual's –

(i) racial or ethnic origin; or
(ii) political opinions; or
(iii) membership of a political association; or
(iv) religious beliefs or affiliations; or
(v) philosophical beliefs; or
(vi) membership of a professional or trade association; or
(vii) membership of a trade union; or
(viii) sexual preferences or practices; or
(ix) criminal record –

How does the Privacy Act work?

The Privacy Act is based on a set of Privacy Principles that lay out how organisations and their agents or employees should treat private information and its storage and communication. The principles contained in the Privacy Act are not *prescriptive*. That is, they don't tell agencies and organisations what they must do in each situation. Rather, they offer *principles* about the way in which personal information should be handled, and each agency or organisation needs to apply those principles to its own situation.

Privacy Principles

The privacy principles are summarised below. Each has a hyperlink to the original wording of the principle contained in the act. IPP1, 2, 4, 9 and 10 are particularly applicable in schools. It should also be borne in mind that terms such as 'reasonable' do not, in a legal sense, imply a level of mildness as in "he did reasonably well". Reasonable steps for example, in a school scenario, are those that should be applied to counter risks that a tertiary educated, IT literate educator should, under consideration, be able to foresee or in the normal course of duties would have been expected to be advised of and remain aware of.

IPP 1 Collection
Organisations should only collect personal information that is necessary for one or more of its functions and activities.
IPP 2 Use and Disclosure
An organisation must not use or disclose information about an individual for any other purpose (a secondary purpose) other than the purpose for which the information was collected, except in a number of exceptions specified in the Act.
IPP 3 Data Quality
An organisation must take reasonable steps to ensure that the personal information it collects uses or discloses is accurate, complete and up to date.
IPP 4 Data Security
An organisation must take reasonable steps to ensure that the personal information that it collects is protected from misuse such as unauthorised access, modification or disclosure, or loss.
IPP 5 Openness
An organisation must set out in a document a clearly expressed policy on its management of personal information and make this document available to anyone who asks for it
IPP 6 Access and Correction
If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual.
IPP 7 Unique Identifiers
an organisation cannot use the same identifier that another organisation uses to identify an individual (e.g. Tax File Number, Medicare number.)
IPP 8 Anonymity
Where it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.
IPP 9 Transborder Data Flows

An organisation may not transfer personal information outside Victoria unless the recipient of the information is subject to privacy standards that are similar to the IPA 2000, or in other limited circumstances. The privacy rights an individual has in Victoria must remain, despite the information being transferred to another jurisdiction.

IPP 10 Sensitive Information

An organisation can only collect sensitive information in restricted circumstances.

Student Activity 1

Discussion does privacy matter?

Below is short presentation with some statement about privacy to spark discussion. The original source video can be found here http://video.cnbc.com/gallery/?video=1372176413 the quote from Bruce Schneier can be found here http://www.schneier.com/blog/archives/2009/12/my_reaction_to.html

Discussion primer

https://docs.google.com/presentation/d/1ozB17r8UThn00UuM-ONp9YRrXG7xc8glIQ017MdRoc4/edit

Take home key points on the privacy rights for students

The link below summarises student rights in regard to their information privacy under law in Victoria

https://docs.google.com/presentation/d/1D_47HborvZGHKI4eFUMUR1fmE9NbfroM4MuXtiXZ5Kk/edit

Privacy Online

This section will deal with three key aspects of online privacy. Privacy from unwanted tracking while browsing, protecting individual's personal digital footprint and individual's responsibilities in respecting the privacy of others.

Tracking Online

How

Whenever you visit a website, a record is logged of the address of the computer (or IP) from which you accessed the site, which pages you browsed and for how long, which files you downloaded to keep, the search term you might have used to get there, the last web address you came from and the one you exited to. Often websites will install a cookie or small code file to your browser to assist in this. None of these things are by themselves bad. A cookie, for example, can be added from a website so that you don't keep seeing their pop up notice every time you go to a new page in the site. The cookie file tells the website, each time you open a page, that you have just been on the site and don't need to be shown the pop up again. For some more examples of good cookie use click here

Many internet sites are paid for by advertising. Most users will have noticed sites that have adverts in the sidebar or the banner and sometimes these adverts seem to be very directed at you and your interests. Well they probably are! Advertisements can install so-called "third-party cookies" that can follow your movements from site to site and help the advertiser build a database of your online activity and so target you specifically for advertising based on your browsing habits. Some cookies install adware or spyware applications on the hard drive. Such is the case with the "Atdmt tracking cookie" which can record the sites you visit and ads you click on, thus being a very useful tool for advertisers. But it gets worse: it can also record personal information like credit card numbers and passwords to online accounts. There have been cases of identity theft related to atdmt tracking cookies.

Unfortunately it gets worse. The software company Adobe, invented a new type of cookie to work with its Flash multimedia files. It was originally intended to count the number of unique views of items of multimedia. These so called Flash Cookies or more correctly Local Shared Objects (LSOs) are very difficult to delete as they are stored in many locations and are installed no matter what the security level of the browser is set to. LSOs can capture and store a lot of information about users which can be read by the originator of the cookie, they are therefore, a serious internet security concern.

You can also, whether you are aware of it or not, have your browsing recorded while you are browsing sites that require you to login such as Google or Facebook. Both companies intensively harvest and analyse information about you that can better target advertising to you or make your data more valuable to sell to another party. This is done by cross referencing your browsing habits against the personal information that you consent to supply to them. Many sites, by use of a tracking cookie, are able to this even after you logged out.

Toolbars are another common tracking method. Often free software will install a toolbar to your browser. Many toolbars are able to relay browsing and other information back to their originator in real time.

Sometimes websites can be funded by government grants or charitable institutions or even by donation. Software can be created by developers working for social good under the FOSS model (Free Open Source Software) or development models like Google Summer of Code. However, websites and software always require money to create and maintain, this money has to come from somewhere. *So the rule is on the web, if a site or software is obviously commercial and doesn't seem to have a product to sell*

….THEN THE PRODUCT IS YOU!

For more information about website and social network privacy see the Appendix

Student Activity 2

A guide to internet privacy good practice

https://docs.google.com/document/d/10fsh1oVwyiBV1FE1NHiPd5V-S72X9057tg9pMHu55pQ/edit

Online Security

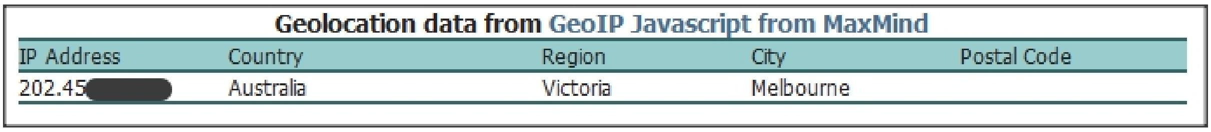
Digital Footprints

A digital footprint is defined thusly; "On the Internet a digital footprint is the word used to describe the trail, traces or "footprints" that people leave online. This is information transmitted online, such as forum registration, e-mails and attachments, uploading videos or digital images and any other form of transmission of information — all of which leaves traces of personal information about yourself available to others online." (source: www.weboepdia.com)

Email

Emails can reveal much more about you than you may realise. Most email clients will allow you to "View Headers" on an email. The header contains information about origins of an email. If you use a client such as

Outlook, Outlook Express or Thunderbird that information can include the originating IP address of the email, ISP, where it has been routed through and even the name and details of the computer from which it was sent. Your IP address can readily supply your location. The example below was extracted from the header of an email sent by me;



Geolocation data from GeoIP Javascript from MaxMind

IP Address	Country	Region	City	Postal Code
202.45[redacted]	Australia	Victoria	Melbourne	

If you connect via 3G the geolocation of your IP can be much more accurate, down to the nearest tower in some cases.

Student Activity 3

So who cares what people know about me? Why does it matter? It's just the internet right?

There are a number of reasons, here are just some;

1. *Just because you do something now that seems Ok doesn't mean it will always seem so to you or everyone else - Tourists deported from U.S. for Twitter jokes and remember the internet never forgets!*
2. *We all accept that there are genuinely bad people out there and we also accept that unless we are very unlucky we will never encounter one. Consider though, there are around 2.3 Billion internet users worldwide that's 2,300,000,000. When you connect to the internet you connect your living room or office or wherever to all those people. Chances are some of them are very bad and will mean you harm, do you really want to be leaving a trail for these people to know all about you? Try this one below. https://docs.google.com/presentation/d/1qI09kc61sdqY0MqAL5KUzW6qqYf-bA-qMV1fMiabZ7E/edit*
3. *Friends don't always stay friends, relationships fail and sometimes with enormous emotional intensity. People of all ages and genders can indulge in stalking on the internet, or Cyberstalking. By leaving no place in which you cannot be found and communicated with you leave yourself at the mercy of a future potential stalker.*

Stalking Sarah

Sarah is a pretty active internet user. She's a regular in chat rooms, often posts info in discussion groups and has visited a heap of websites. She meets some pretty interesting people online as well, people with similar interests...sport, music, movies and stuff like that.

So when some guy follows her through cyberspace, she's pretty freaked out. He emails her, posts comments about her in chat rooms and has somehow found out her mobile phone number.

This clip could be about anyone. Find out what Sarah did to protect herself.

Our digital footprint is very important; below are some tips to help you manage the information about yourself online.

Student Activity 4

Minimising your digital footprint

https://docs.google.com/presentation/d/1tf46BKt4i92XUSVracfzh_sPrpC9ls0RHk6cjWGRVPU/edit

Protecting the privacy of others online

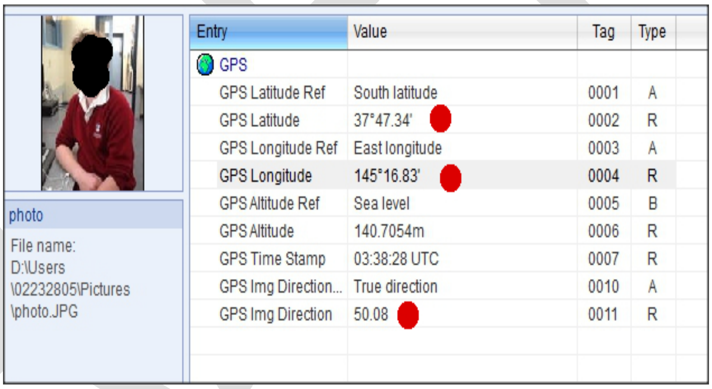
There are a lot of ways in which you can unintentionally compromise the privacy of other people, including friends and loved ones, and of course your own.

Digital Images

A simple image can give away incredible amounts of information about someone. Digital images are not just photographs, they also contain EXIF data. This is data about the image; on location aware devices like iPads and Smartphones this includes location, time, date, direction, altitude, device identity and much more.

Here is an example

This is a volunteer student, whose identity we have hidden for obvious reasons. This image was taken on an iPad 2 in a computer lab here at the College. And below is a screen grab of the location related EXIF data extracted using some freely available software.

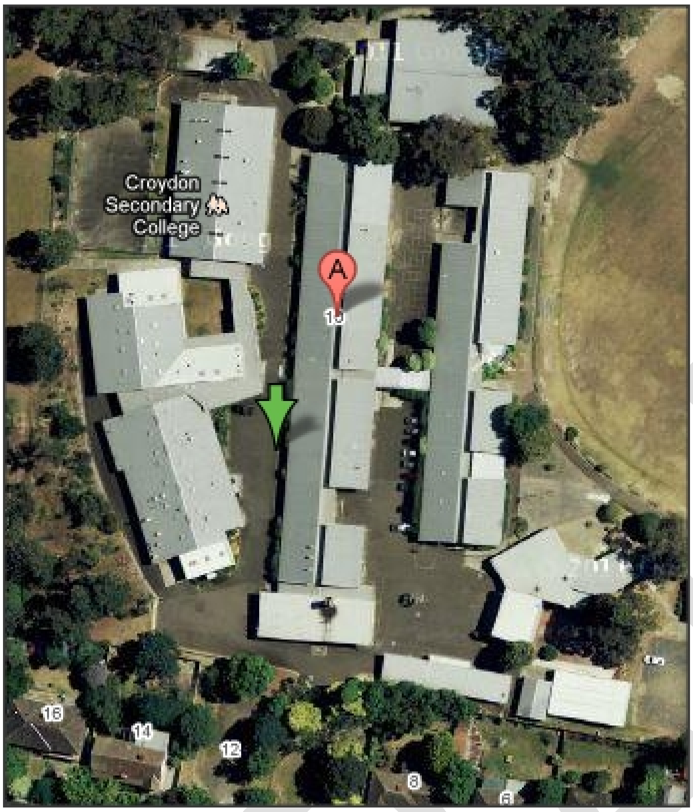


photo

File name:
D:\Users
\02232805\Pictures
\photo.JPG

Entry	Value	Tag	Type
GPS			
GPS Latitude Ref	South latitude	0001	A
GPS Latitude	37°47.34' ●	0002	R
GPS Longitude Ref	East longitude	0003	A
GPS Longitude	145°16.83' ●	0004	R
GPS Altitude Ref	Sea level	0005	B
GPS Altitude	140.7054m	0006	R
GPS Time Stamp	03:38:28 UTC	0007	R
GPS Img Direction...	True direction	0010	A
GPS Img Direction	50.08 ●	0011	R

Plug those coordinates into Google Maps and you get this image to the left. This is accurate to about 1 metre from the actual location of the image. Now imagine for a moment the image was taken in your house. All that remains is to select 'Street View' and you have given away the address of your home and exactly what it looks like seen from the street.



Now further imagine this was someone who intended you harm and this location was your bedroom instead!

Here's what happens when location data, Facebook, images and a very unethical app come together;

http://www.cultofmac.com/157641/this-creepy-app-isnt-just-stalking-women-without-their-knowledge-its-a-wake-up-call-about-facebook-privacy/

Student Activity 5 – Metadata extraction example from above

https://docs.google.com/presentation/d/1B3qYoxWquhdwsiuEtUpwlcXY5XWMZgPiRBjPUAYYKR8/edit

Reverse Image Searching

You have already seen that images are not very anonymous even when there is no name attached to them. However, there are even more direct ways that an image can compromise someone's privacy. Say for example, you place an image of a friend on the internet somewhere that can be indexed by search engines and that image is the same or similar to one they have used, say as a profile image, somewhere where they are intending to stay anonymous. It is a very simple matter to reverse search an image using Google, Tineye or a range of other tools. You have just blown their cover! Maybe it may only cause embarrassment, but it can be much more serious as you have already seen. The internet may be vast, but a great deal of it is exhaustively indexed in ways that can catch people out. Have a look at this example.

Student Activity 6 – Reverse Image searching

An example

https://docs.google.com/presentation/d/1aWxiAZb2-hnZ-Ix3RBVHxLbMyUUCCbnGoUo75S7vggs/edit

Using reverse image search to avoid a scam.

http://www.stateofsearch.com/using-google-image-search-to-identify-id-fraud-image-theft-your-risk-as-an-seo/

Appendix

Easy Guide to Social Networking
http://www.dbcde.gov.au/easyguide
Men more likely to be cyber-stalking victims
http://www.v3.co.uk/v3-uk/news/1940758/men-cyber-stalking-victims
Official databases fail to protect personal data
http://www.v3.co.uk/v3-uk/news/1977227/official-databases-fail-protect-personal
Sony PlayStation Network hacked – millions of card details at risk?
http://www.infosecurity-magazine.com/view/17613/sony-playstation-network-hacked-millions-of-card-details-at-risk/
AusCERT loses passwords to Govt service
http://www.itnews.com.au/News/307958,auscert-loses-passwords-to-govt-service.aspx
Government passwords cracked in probe
http://www.theage.com.au/technology/security/government-passwords-cracked-in-probe-20110327-1cbsz.html
Privacy guide to cloud computing.
https://www.privacy.vic.gov.au/domino/privacyvic/web2.nsf/files/cloud-computing/$file/info_sheet_03_11.pdf
Privacy guide to employment applications
https://www.privacy.vic.gov.au/domino/privacyvic/web2.nsf/files/job-applications-referee-checks-and-privacy/$file/info_sheet_02_09.pdf

Feedback

Please provide any feedback on this document here or paste this link into your browser

https://docs.google.com/spreadsheet/viewform?formkey=dDNfZGRhQnAyTWdkZjRPWFgzcmR2S0E6MQ