Dr Andrew Campbell

Senior Lecturer in Psychology
(The University of Sydney)

Child, Adolescent & Family Psychologist
(Clear Horizons Psychology Services)

clear horizons

Psychology Services
www.clearhorizons.com.au

My Background

- PhD in Cyberpsychology
- Registered Child, Adolescent & Family Psychologist
- 15+ years in researching eHealth & Cyberpsychology
- A father of a 2 year old boy

Agenda for Master Class

- This presentation focuses mostly on current issues of concern for information safety of your child in the online world. It looks at present things to address and future issues that can arise if you don't keep stock of what personal information you put online.
- I've incorporated some of the more popular questions about safety of digital information for young people into this presentation.
- I will give pro's and con's of a range of information based on evidence based research. I will also provide references for you to review these sources at the end of the seminar.
- I may not answer all the questions you have during the talk, but invite you to communicate with Knox post the seminar.

Overview of Keeping a Healthy Digital Footprint

- **What are the important concerns for keeping your child's information safe?**
- **Sexting and how it relates to the law and to contemporary relationships**
- **Social network profiles and their impact on employment and careers**
- **Protecting your identity and whereabouts when online from thieves and predators**

You Can't Stop the Flood…

- You can't stop what has already flooded society – i.e. information technology.
- What you can do: Provide for good digital citizenship!
- No different to learning about all other issues in life, for example:
  - Good Health Habits
  - Community Responsibility
  - Global Stewardship
- I wish to stress…

  It is not about kids knowing more about technology than parents.

  It's about you both learning together about technology!

Things you and your child should know!

- Data is rarely ever erased! Everything you put online can be shared or even claimed to be owned by some other entity, because you gave permission for its use – sometimes unknowingly.

- The input of data online by children is more prolific than that of adults. This is because:

  1. The desire to access a service is greater than their instinct to protect their privacy.
  2. They are unaware of potential use of their data both in then immediate and the future.
  3. The do not want to be 'socially excluded'.
  4. They believe cancelling an account = deleting data
  5. They believe they can outsmart the 'system'.

- In at least one of the five points above the chances your child, or even you, being 'caught out' is high. This is because information you share does get used - but unless you search for it, you may never see it again or….more importantly….know what it was/is being used for!

Common Places you can locate Children's Data

- Between the ages of 5 – 25, children and young adults tend to enter personal details into one of the following services:

1. Social Networks (e.g. Facebook, Twitter, Instagram, Snap Chat, Tumblr)
2. Google Accounts (e.g. Google Play and Google Maps)
3. Mobile Phone Accounts (e.g. Samsung & Apple)
4. iPod and MP3 Accounts (e.g. iTunes, Music Share Applications)
5. Gaming Networks (e.g. Xbox, Steam, PlayStation by Sony)
6. Internet Service Providers (Bigpond, TPG, Optus, etc)
7. Movie Sharing Services (e.g. Netflix, AppleTV)
8. Online Shopping (ebay, Amazon, etc)
9. Miscellaneous (Online Blogs, Magazines, Fansites, etc)

So what is the fuss about??

- All the services that require sign up seldom state the following:

  1. Who they 'specifically' share their data with?
  2. Why they share that data and what they get from it?
  3. How long they will store your data for past the point of cancelling access to their service?
  4. Where your data is stored?
  5. Where it is backed up? (this is a mystery in a lot of cases, even when you read the fine print!)

- With the above points unanswered, the greatest points of concern are:

  1. Is my identity being used for things I am unaware of?
  2. Am I likely to be tracked and by whom?
  (e.g. is what I do online monitored now and in the future?)
  3. How can I delete myself from the internet if I choose to?

Some Good News…

- You can still access the internet safely if you ask simple questions before signing up:

1. If I want to erase myself from this service – is that an option?
2. Do I understand the service agreement?
3. If not, do I accept the risk? (tough one for children to ascertain by themselves)
4. Do I need this 'specific' service, or can I live without it/use an alternative?

By following these steps, you can begin to control your information dissemination risks.

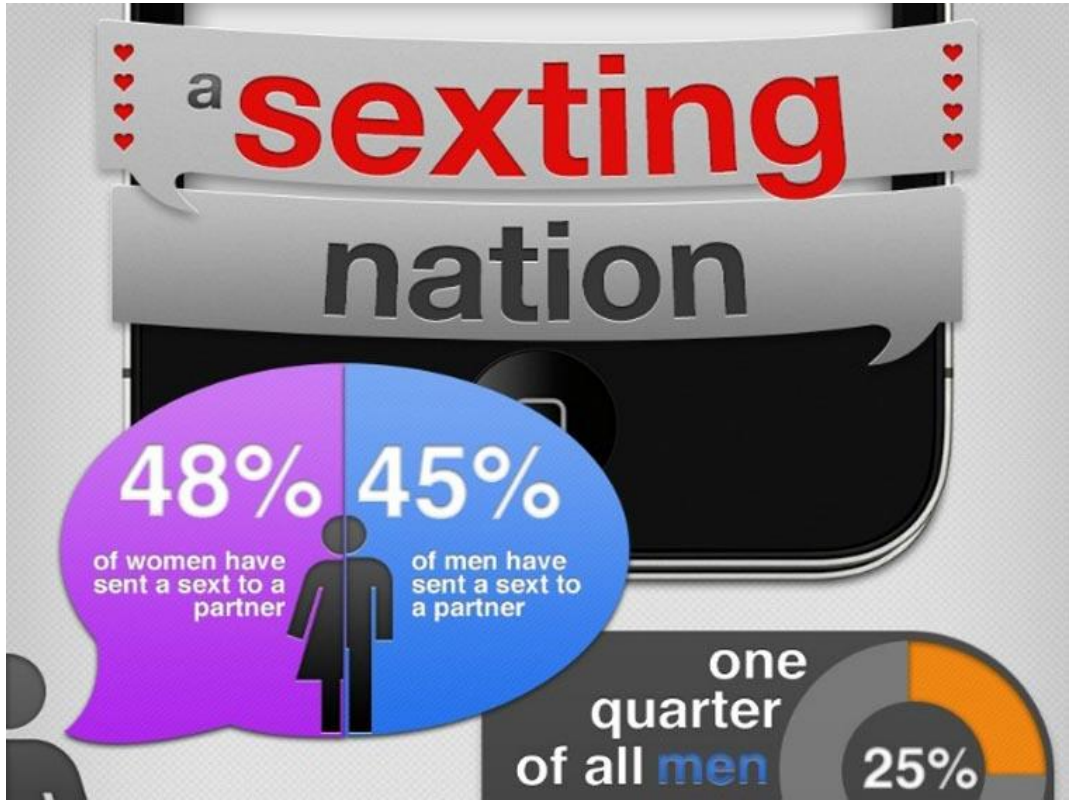
- The best approach to having a healthy digital footprint is to instil the same principles about general 'risk taking'. Have your children asked themselves **"Is it worth it, both for now and in the future??"**

Sexting – What is it?

- Sexting is the act of sending sexual explicit images or messages, usually by mobile phone.
- Sexting has been estimated to be increasing in practice between the ages of 12- 25 year olds, particularly in Western Nations.

  The most problematic age group seems to be those 16-17 which correlates with increased sexual interests due to the maturation progress of puberty (Hinduja, & Patchin, 2010).
- Studies to date are exploratory in nature, but findings in the USA are stating that sexting could be a part of relationship development that is abnormal until full maturation
  (Mitchell, Finkelhor, et al, 2012).
- Clearly, there are urgent concerns around this behaviour:

1. Security of this type of image sharing
2. Protection of minors
3. Illegal use of images by predators
4. Inability to retrieve and delete images



Sexting and the Law

- Australian Law classifies:

  "…anyone who has in their possession a naked, or even a partially naked photo of a person under the age of 18 on their phone or computer, can be guilty of an offence, along with the producing and distributing of the image or video to other parties." (FindLaw Australia, 2014)

- Having said this, State Laws are different. In NSW, consenting 16 & 17 year olds may argue to be exempt from this infringement. However, this is a case-by-case concern.

- The overall legal consensus appears to be that Image capture and sharing of minors (those under 18), regardless of their consent, is illegal.

Further Concerns on Sexting Safely

- No image is ever erased when transmitted. This is because it is 'carried' by a service provider.
- Given that some images placed on social networking sites (such as tumblr) occur frequently, these images can be picked up by search engines. The image 'name' is catalogued and can then be recalled during an 'image search'.
- Images are often duplicated (reposted on social media sites and websites). Therefore requesting the initial carrier to delete it, often doesn't mean reposted images are deleted.
- **Rule of thumb:** only place images of yourself in cyberspace if you are happy for them to live their indefinitely….they are likely to last past your death!

Social Network Profiles

- Just the same as images, social network profiles tend to live on indefinitely.
- Using Facebook as an example, when you ask to close the account, what you are actually doing is asking them to remove your information from search engines. The profile still exists and can be reactivated upon request. Ergo: nothing was ever deleted!
- Hypothetically, if you ask a Social Network Service to delete an account permanently – there is no evidence the Social Network Service can provide you to demonstrate this actually has been achieved.

  You may get statement from them – but can you confirm the personal information contained in that account was deleted if obtained by a third party, such as Google?
- Social Network Profiles, like website, tend to have 'mirror servers' backing up your data. Often we are unable to know where these physical, mirror servers, live in the world.

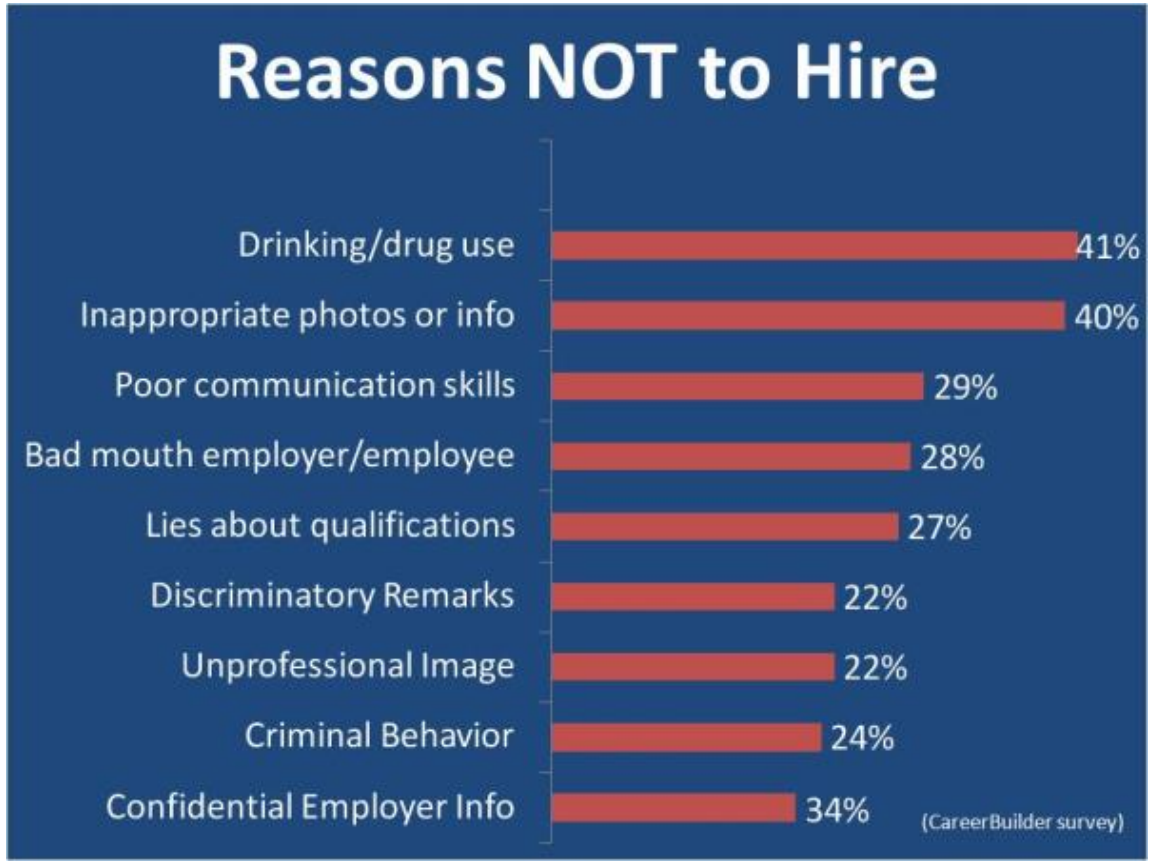
So what should we say on our Social Network Profiles to keep us safe?

- Ultimately, as little as possible!

- It is good practice to do the following:

1. Do not use your real name – if you do, just use your first name or last name.
2. Keep images you post to things you would wear on a T-Shirt…if you aren't embarrassed by them, then it wont matter if they live in Cyberspace indefinitely.
3. Keep your postings civil and sensible (note next section on employment profiling)
4. Look at who you associate with online – are they REAL friends or simply 'Rent a Friend'?
5. Think before you 'Like' – Social Marketing is massive and can be a nusance.
6. If doing synchronous messaging (chat) remember it is a legal document. Don't say it in writing if you think it can be damaging now or in the future.

Your Social Network Profile and Future Employment



- Human Resource Departments, Universities and Individual Employers are high likely to 'Google you'.
- This may not be 'best practice' for selection of employment or higher education, but it is a practice your employer or education institute is able to carry out and, in some instances, may impact their decision on hiring/entrance to their organisation.
- Once employed, your profile is still likely to be reviewed.
- Once on social networking you are always on social networking – however, some privacy settings are getting better for Facebook.
- Google+ has one of the strongest privacy settings for profiles, but keep in mind that no setting is un-hackable by a well resourced and determined IT specialist.
- In short – treat your social network account like you would C.V. – public but professional, or at the very least, a portfolio of social acceptable behaviour.

Tips on Protecting you and your information

- Due to the unregulated environment of the Internet, we must teach young people that it is always a public forum, even when measures are put in place to make you believe otherwise (e.g. security and privacy settings).
- Just like a seatbelt in a car – security and privacy settings will keep you somewhat safe – but never absolutely safe!

- By using the following protocols, your children and teens will be able to maintain a healthy digital footprint:

1. Only provide personal information on websites that have encryption settings (e.g. credit card details or address information). You can check encryption setting visually by looking for the small padlock symbol in your web browser.
2. Keep images of themselves offline as much as possible unless they are happy for the photo to be shared without their knowledge.
3. Know that nothing is ever really deleted – including conversations in chat functions.
4. Deactivate accounts they don't use. This includes email accounts.
5. Try not communicate with people they don't know in the offline world. By keeping to those we physically know, we can keep ourselves safer.
6. Children under 13 should not have a social networking account. This is both provider and national policy.

References

- **Website Reading**

  http://www.findlaw.com.au/articles/4720/sexting-and-australian-law.aspx

  http://www.thinkuknow.org.au/

- **Education Guides**

  Hinduja, S., & Patchin, J. W. (2010). Sexting: a brief guide for educators and parents. Cyberbullying Research Center.

- **Journals and Research Articles**

  Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2012). Prevalence and characteristics of youth sexting: A national study. Pediatrics, 129(1), 13-20.

  Reyns, B. W., Burek, M. W., Henson, B., & Fisher, B. S. (2013). The unintended consequences of digital technology: exploring the relationship between sexting and cybervictimization. Journal of Crime and Justice, 36(1), 1-17.

  Walker, S., Sanci, L., & Temple-Smith, M. (2013). Sexting: young women's and men's views on its nature and origins. Journal of Adolescent Health, 52(6), 697-701.

Q&A Time