How safe is Your Facebook Profile?  
Privacy issues of online social networks

R. Wallbridge
ANU College of Law, The Australian National University, Acton ACT 0200, Canberra, Australia

Online social networking sites have become one of the greatest social technological phenomenon’s of the 21st century. However, most users are unaware of the many privacy issues that come with having a profile page on a social networking site. By placing personal information on the world wide web users make themselves vulnerable to online predators, selling of their information to third parties and in some instances, websites owning everything an individual places on their profile page or friend’s page, including photos. The problem is intensified because of the fact that communicating online via social networking sites has become not only popular but fashionable and for many young people, necessary to maintain their social status among friends. Because of this, young people are especially at risk of exposing themselves when sites are joined without any thought as to what may happen to personal information, photos and postings that are entered or placed on their or their friend’s profile pages. This paper looks at privacy issues of online social networking sites from around the world including Australia, USA, Japan, Korea, Brazil and India. It intends to raise awareness of privacy issues that people may face when creating their online identity with the hope that more care may be taken both by corporations and individual users.

INTRODUCTION

Social networking sites are an unmatched technical development of the 21st century. Millions of young people aged 14 to 24 years old from all over the world participate and interact with their favourite social networking site on a daily basis. Some of the most popular sites that will be discussed include Korea’s Cyworld, Orkut a popular site in both Brazil and India and Facebook and MySpace which are popular in the United States and Australia. There are hundreds of different social networking sites that offer a range of services from blogging, to photos and video sharing and sites where travel plans can be shared. 1 However this study is limited to those that focus on an individual creating a personal profile, as it is this kind which involves posting particularly personal information on public domains. Once a profile is created participants can invite each other to become friends, usually approval by both people is required for this to occur. Once friends, a small link connects their profiles, usually by a photo and/or a name and users can then interact with each other’s profiles by writing comments, sending messages, videos and photos. 2

While this paper mainly focuses on the negative aspects to online social networks, it is important to be aware that there are many benefits that individuals gain by participating and interacting on such sites. 3 Boyd argues that it is important not to exaggerate the risk presented to users and suggests that just as a parent would give their teen some space in the offline world, parents should do the same online. 4 There is research suggesting that for the socially isolated or those with low self-esteem, online social network sites can actually be of significant benefit, as it is easier to form links and make friends online. The research showed that the more intensively those with low life satisfaction or low self esteem use Facebook, the more social capital they gain. 5

1 See examples of sharing photos at <http://www.picasaweb.com>, sharing videos at <http://www.youtube.com> and sharing travel plans at <http://www.dopplr.com>
3 Danah Boyd, Identity Production in a Networked Culture: Why Youth Heart MySpace (Speech to be delivered at the American Association for the Advancement of Science, USA, February 19, 2006).
4 Boyd, above n 2, 22.
5 Nicole B. Ellison, Cliff Lampe and Charles Steinfield, ‘The Benefits of Facebook “Friends:” Social Capital and College Students’ Use of Online Social Network Sites’
1. TRENDS

“If you’re not on MySpace, you don’t exist.”

1.1 Why socialise online?

1.1.1 Creating online personal profiles has mainly occurred due to the human need and attraction to connect with people. For many young people, social networking sites are just another place to ‘hang out.’ Young people will continue to work out identity issues, hang out and create spaces that are their own, regardless of what technologies are available. Socialising is especially important to teenagers as inclusion and peer support are vital to getting through awkward teenage years.

1.2 Why are young people volunteering so much personal information?

1.2.1 When young people create personal profiles online, they often include identifiable information like full names, date of birth, home town, school, relationship status, sexual preference, mobile numbers and email addresses. PEW research on American teens showed that 82% of teens with online profiles post their first name, 79% a photo of themselves, 61% their city/town name, 49% include the name of their school and 29% their last name.10

1.2.2 Why young people are so willing to share personal information with often complete strangers they met online is an interesting phenomenon. A common misconception is that young people use social network sites to form new friendships or relationships, when in fact most use it to maintain connections that already exist. For example PEW research revealed that 90% of teens on MySpace use the service to stay in touch with people they already know.12 In Korea too, 85% of participants in a survey on Cyworld said they joined to maintain existing friendships.13 Given this, young people are more willing to place personal information on their profiles as they believe or assume that most people who will view their page will be ‘friends.’ However, it is much easier to become a ‘friend’ online than offline and many users do not restrict their privacy settings to only friends. The risk is illustrated by the PEW study which indicated that 31% of American teens with profiles have ‘friends’ who they have never met.15 These privacy concerns are further compounded by the new instant ‘chat’ feature where more personal conversations can take place with ‘friends.’

1.2.3 Personal information on social network sites is also being volunteered because of changing cultural trends, increased familiarity and confidence in technology and lack of exposure or memory of misuse of personal data.16 It was also obvious from the survey that 18-34 year olds are much more likely to be comfortable providing detailed personal information to join social network sites than those above 50 years old.17 This is because young people have grown up with the internet where it has become normal to provide personal information to use certain online services.

2. PRIVACY ISSUES

2.1 While many privacy concerns are common to all people using social networking websites, some illustrate more privacy issues than others. Issues to be discussed include consent, control of personal data, data collection, data deletion and accountability. Personal data is defined to mean any information or content which can be reasonably identifiable to an individual.18 All of these will be discussed within the context of the eight OECD

---

6 Girl, 18, to her Mother as cited in Boyd, above n 2, 1.
7 Boyd, above n 3.
8 Ibid.
9 Ibid.
10 Amanda Lanhart and Mary Madden, Teens, Privacy & Online Social Networks: How teens manage their online identities and personal information in the age of MySpace, PEW Internet & American Life Project (18 April 2007) iii.
11 Ellison, Lampe and Steinfield, above n 5, 1155.
12 Amanda Lanhart and Mary Madden, Teens, Privacy & Online Social Networks: How teens manage their online identities and personal information in the age of MySpace, PEW Internet & American Life Project (18 April 2007) ii.
14 Ibid, above n 12, ii.
15 Ibid, 32.
18 Definition adapted from the Privacy Act 1988 (Cth) Section 6.
1980 Privacy Principles which were designed to be flexible and adaptive to technological change.19

2.2 Consent

2.2.1 A reoccurring issue is ‘consent’ which encompasses the Openness Principle which states that the way in which data will be used should be open and accessible and the Purpose Specification Principle which states that data should only be used in ways in which are expressed at the time of agreement.20 The issue of consent can be broken down into several parts. Firstly, whether or not fully informed consent is given to all aspects of the social network service at time of registration, secondly, whether what is done with the registration information is consented to and lastly, whether the information that users voluntarily provide on their profile pages is within the boundaries of what was originally ‘consented’ to. Other issues include consent in relation to minors and third parties.

Before Registration: visibility of privacy notices 21

2.2.2 The visibility of privacy policies is directly related to the Openness Principle. Cyworld, Orkut, Facebook and MySpace all possess a link to the site’s Terms of Use and Privacy Policy from their respective home pages. Many policies are not written in plain English or may be difficult to find. Orkut’s policies are the same as Google’s Privacy Policy, yet to locate it several links must be followed as well as information being located in several different documents.22

2.2.3 Before registering, on most social networking sites, users are required to tick a box indicating they have read and accepted the site’s Privacy Policy and Terms of Use. While this theoretically makes users aware of what their personal information and content they may post may be used for, in reality the boxes are ticked without any reading. This is evident through research done on college users of Facebook where 30% of those surveyed did not know that they could manage who can search for their profile and 18% did not know that they can control who can access their profile page, which is an option clearly stated in the Privacy Policy.23

Registration

2.2.4 An aspect which relates to both the Openness Principle and the Security Safeguard Principles (personal data should be protected) is that Facebook asks users to type in their current email account password so the site can access the account’s contact list in order to find email addresses that are not already registered as members to Facebook.” 24 Facebook states below this request that it won’t store the login information and will not contact any of these contacts without the user’s permission.25 The issue is however that the site is obtaining access to email accounts and passwords. While it is possible to skip this step, the option is not obvious and many teenage users would assumingly do this without much thought as it is towards the end of the registration process.

Consent in relation to information voluntarily offered on profile pages

2.2.5 Information on profile pages is a particularly difficult area, as users are volunteering information which they have a right to do. However many young people are simply not aware of what may happen to the information they place on these profiles. For example, Orkut’s policy makes it clear that while the user owns the content that is placed on Orkut, Google clearly states that it has full and irrevocable control of any information posted, including

19 The OECD has 30 member states, including the countries discussed in this article; Australia, US and Korea. The organisation is also currently offering “enhanced engagement with view to membership” with Brazil and India. To view the Eight Privacy Principles see; Organisation for Economic Co-Operation and Development, OCED Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2002).

20 Ibid.


24 To register and view this process go to <http://www.facebook.com.>

25 Ibid.
How safe is your facebook profile?

‘private’ messages. Google also states that it can make the content available to other organisations or individuals that Google has a ‘relationship’ with. This clearly violates the Collection Limitation Principle as data collection must be limited. The Purpose Specification Principle and Use Limitation Principle is implicated as all postings and messages (including content) can be linked to an individuals identity and that information is not being used in a manner which is relevant to providing the service.

Minors and consent

2.2.6 Children and those under 18 years old are particularly vulnerable to becoming victims of sexual assault and paedophilia that may begin from meeting strangers online. It is therefore vital that they are adequately protected by social networking sites and parents alike. Cyworld and Facebook’s minimum age to become a member is 13 years old, while for MySpace it is 14 years old. Facebook do not permit those 18 years or older to view the profiles of any person under 18. Facebook do not permit those 18 years or older to view the profiles of any person under 18. However, the Openness Principle is violated in regards to minors’ being permitted to join sites as their ability to understand privacy policies and terms of use agreements is severely reduced. If most young people or adults have trouble deciphering privacy policy information, then minors’ will find it extremely difficult to comprehend the implications regarding their personal information both what they surrender at registration and what they post on their profile page. It is therefore imperative that the most fundamental clauses be written in simple English aimed at children as well as requiring users to select their privacy settings before registration.

Consent and third parties

2.2.7 Facebook and MySpace both allow third party widgets to access its core functions. Facebook permits any company or person to develop an application that will end up looking as though it is part of Facebook itself and users can opt-in to use the additional feature. In order for the application to be added it requires access to personal information. It is not at all clear to the user exactly what information they may be gaining access, it was only through personal email correspondence with Facebook that it was clarified to mean only the information visible on a participants’ profile page.

2.2.8 Also implicated is the fact that many users may not be aware that third parties or related partners of the social network sites may be able to obtain information about a user. For example Cyworld and Facebook both have clauses to the effect that they will supply third parties with personal information only when ‘it is reasonably necessary to offer the service.’ This ambiguous phrase has the potential to be interpreted however the company wishes and breach the Use Limitation Principle which states that data cannot be used for purposes other than for the purpose the website states.

2.3 Control of Personal Information

Although in many ways a user offers ‘consent’ when they sign up to an online site, most are unaware of the implications of voluntarily providing personal information on profiles as well as not being aware of how this information may be processed. An individual can lose control of their data when a digital dossier of personal information is generated. This occurs when profiles on social networks sites can be downloaded and stored over time by site operators for back up purposes so as to

---

27 Ibid, 11.2.
29 Ibid.
incrementally create a digital dossier of personal information.\textsuperscript{34} This can also occur out of the control of the user as users’ ‘friends’ on their sites can write a comment about them on another friends profile or ‘tag’ the individual in photos. It is in this way that profile information has the potential to be used in ways that the user did not intend and stored for indefinite periods.\textsuperscript{35} Since the cost of disk storage and downloading is constantly being reduced, it is possible to take ‘snapshots’ of a whole network for storage or back up purposes.\textsuperscript{36} The main threat associated with digital dossier aggregation for young users is when future employees or colleges are able to perform searches that may bring up data or even compromising photos that an individual thought either no longer existed or not possible for that source to obtain.\textsuperscript{37} For example a gay student attending a Christian college in the US was expelled after administration officials viewed photos of the student dressed in drag on Facebook.\textsuperscript{38}

2.4 Data Collection

Limiting data collection

2.4.1 The Collection Limitation Principle states that the collection of personal data should be limited.\textsuperscript{39} At registration online social network sites require certain pieces of information such as birthdays, and addresses which are debatably not vital to creating and maintaining the service. For example, Facebook, Orkut, Cyworld and MySpace all require a full name, date of birth and email address with Orkut additionally requiring an address and gender.\textsuperscript{40}

2.4.2 Korea’s Cyworld registration requires the potential site member to supply their national identity number which breaches the limitation requirement. The national ID number is a highly sensitive and unique number given upon registration of birth which serves important functions such as opening bank accounts.\textsuperscript{41} Korean applicants must also provide Cyworld with their real full name which is then validated online in cooperation with Seoul Credit Rating which makes it more difficult for users to create pseudo names.\textsuperscript{42} While this may be a breach of the Collection Limitation Principle, it process assists in protecting minors from joining the website and keeps the site relatively free of illicit material and cyber predators due to the fact that offenders are highly identifiable.\textsuperscript{43}

2.5 Data Deletion

2.5.1 An individual’s right to have their personal data completely deleted is an important right to users of online social networks as it can otherwise impinge on their privacy later in life. The Individual Participation Principle guides such usage, allowing individuals to request data.\textsuperscript{44} Most social network sites researched require the user to de-activate their account through functions on their website; however Cyworld requires the user to email site administration while Orkut requires a written letter to Google requesting a deletion which is extremely onerous.\textsuperscript{45} To network operators, complete deletion is costly and technically demanding which means personal information can be stored indefinitely even though a user may believe that all aspects of their account has been deleted.\textsuperscript{46} Even when an account is ‘deleted’ all the social networking sites researched state they may still retain data on backup copies for an unspecified period.\textsuperscript{47}

\textsuperscript{35}Ibid.
\textsuperscript{36}Ibid.
\textsuperscript{37}Ibid.
\textsuperscript{38}Mr. Byung Wook Kwan, OECD employee, Interview on the issue of the national identification number, 10 January 2008.
\textsuperscript{39}Choi, above n 13, 176.
\textsuperscript{40}Kwan, above n 43.
\textsuperscript{41}OECD, above n 19.
\textsuperscript{43}OECD, above n 19.
\textsuperscript{44}European Network and Information Security Agency, above n 37, 8.
\textsuperscript{45}Cyworld, above n 46. Orkut, Privacy Notice (21 May 2008) <http://www.orkut.com/html/en-
2.6 Accountability

2.6.1 The Accountability Principle requires that those who give effect to the Guidelines be held accountable for their compliance. All social networks sites in some way provide users mechanisms to get in contact with administrators regarding their privacy concerns. It has been suggested that even if a user felt the website had broken promises it made in the privacy policy, it is doubtful that the user could sue the website for breach of contract on the basis of the policy loopholes and vague language contained in the agreements.48

3. CONCLUSION

3.1 It is difficult to balance the right of privacy and control of personal information when individuals voluntarily place personal information on their profile. Once information is placed on public domains users can easily lose control over who sees it and who may use it. While privacy settings are there to protect users, in practice this is not always the case, whether it is because of slack web design or through lack of knowledge or care by the user.

3.2 The underlying issue is that young people are simply not concerned with giving personal data to social networking sites or placing detailed information on their profile pages. Because a change in teen culture is unlikely, the corporations behind social networking sites must act with more responsibility. Action must be taken on a multi-lateral scale such as cross border agreements on privacy standards to reduce the prevalence of pornographers, identity theft and other types of privacy concerns as there is obvious difference between privacy regulations between countries such as Australia and the US compared to Brazil. Organisations such as the OECD, APEC and other regional organisations have the potential to be instrumental in developing tighter cyber privacy laws. This must be encouraged and insisted upon in order to ensure social networking sites better protect its users, especially its young participants.

REFERENCES

1.  Articles/Books/Reports


Boyd, Danah, Identity Production in a Networked Culture: Why Youth Heart MySpace (Speech to be delivered at the American Association for the Advancement of Science, USA, February 19, 2006).


Lenhart, Amanda and Madden, Mary, Teen Content Creators and Consumers: More than Half of Online Teens have Created Content for the Internet; and Most Teen Downloaders Think that Getting Free Music Files is Easy to do, PEW Internet & American Life Project (2 November 2007).

Lenhart, Amanda and Madden, Mary, Teens, Privacy & Online Social Networks: How teens manage their online identities and personal information in the age of MySpace, PEW Internet & American Life Project (18 April 2007).


2.  Legislation


Privacy Act 1988 (Cth)

3.  Internet Resources (Primary)


Mixi Home Page: <http://mixi.jp>


