Social Networks and Privacy

David Wietstruk
Technische Universität Wien
Karlsplatz 13
1040 Wien

ABSTRACT

Social networks have permeated the lives of many of us. They are topics of discussion at social gatherings and even influence decisions within groups of friends. Social networks provide alternative ways of keeping in contact among a group of friends, instead of writing e-mails, people use status updates and picture sharing. However, social networks have brought about a revolution in the way we, as a society, define personal privacy and draw the line of where privacy begins and ends. No longer are we living in large anonymous cities anymore, but rather living in small, virtual villages where everyone can see everyone and there are few places to hide.

Categories and Subject Descriptors

K.4.1 [**Computers and Society**]: Public Policy Issues – *privacy*

J.4 [**Computer Applications**]: Social and Behavioral Sciences – *psychology, sociology*

General Terms

Management, Security, Human Factors, Theory, Legal Aspects

Keywords

Privacy, Social Networks, Facebook, MySpace

1. INTRODUCTION

The *American Heritage Dictionary of the English Language* defines the word "privacy" as, "the state of being free from unsanctioned intrusion". Privacy has become a very important topic in the ever-changing digital world. People have asked what privacy is and if the previous definitions of privacy still apply today. Is it possible to maintain any sense of privacy when the vast majority of human beings use the Internet in some way and leave tracks of what they have done that are often open for anyone to see? What about those of us that use social networks? Have we come to define privacy in a new and revolutionary way, or has personal privacy simply become a thing of the past and is no longer relevant in our lives?

2. WHAT ARE SOCIAL NETWORKS?

Social networks are websites where users can share photos, videos and blogs and in turn, their friends can share material with their friends. The two largest social networks are MySpace and Facebook and will be the two social networks mostly dealt with in this paper.

Both of these social networks started out as small websites catering to a niche in a market but have rapidly grown to be icons in modern pop culture. MySpace was the first of the two giants and began as a place where independent musicians could put their work on display for the public and other musicians and promote themselves free of charge. However, as soon as large-name celebrities made profiles on the site, MySpace grew to become a juggernaut. Facebook, on the other hand, started as an international semi-private club for students of universities and colleges around the world. The site required that users link their profiles with a valid student e-mail address to confirm that the user was indeed a registered student at an institution of higher education. Facebook, however, did eventually go public and created a large stir among its member base with the decision to allow anyone to join, much like MySpace. Since then, though, the site has experienced tremendous success and has surpassed MySpace as the largest social network on the Internet. Going public has also made Facebook millions of dollars in ad sales and potentially millions more in the form of market research.

3. PRIVACY CONCERNS WITH SOCIAL NETWORKS

3.1 How Much Are Users At Risk?

With millions of users logging into both Facebook and MySpace daily, trading information and pictures, it is hard to imagine it being completely fault-free. Any time a system becomes larger and more complex, it becomes harder and harder to find mistakes and holes in the system that others can exploit. How much are users truly at risk, though?

There have been attacks on Facebook and MySpace, but none of them have been entirely damaging to users since neither service requires any kind of credit card or financial data from users to allow them to use the network. A user, however, does increase their risk of being hurt in some

other way every time they log on and post something about themselves. The more a user shares on the network with others, the more opportunities there are to exploit this openness. Clearly, the person who uses MySpace passively for exchanging messages with friends and the occasional photo has put themselves at much less personal risk than, for example, someone who logs in multiple times a day and constantly uploads media.

3.2 Who Can See What?

In the beginning, social networks had much fewer controls over what users put out on the web. Since their inception, however, there have been numerous calls for more privacy controls to be implemented and many of those calls have been answered.

The problem remains, however. Why? The answer is simple: naivety. Most users are not aware of the controls available to them; much less how much of what they post is made public across the Internet. Simply tagging a friend in a photo then makes that photo (without the proper privacy controls enabled) available to friends of the person tagged and then when people start commenting, then it makes the photo all the more reachable and open. So again, we have a problem of people not understanding exactly how these websites work and not taking the necessary steps to protect themselves on the Internet.

3.3 How Can User Data Be Used?

It is clear to anyone that social networks are potential gold mines for market research data. Users post what things they like and do not like and the reasons why readily all over various pages of the networks. There are also numerous fan clubs available for users to join and further differentiate themselves from their fellow users.

To give an example of legal market research using user data on a social network, Apple Computers manages and sponsors its own fan club page on Facebook. This provides Apple Computers with an easily searchable location where customers or potential customers can talk about what they would like the company to do. This gives Apple a unique way of predicting market trends.

Social networks are also places that allow brands to maintain their images or change their images in the public eye. For instance, Company A wishes to advertise to a specific demographic that listens to Band A. Band A also has a MySpace page that receives 100,000 unique visitors per day on average. Company A can purchase ad space on Band A's page and then see if their sales improve after being associated with Band A. Auto manufacturers and other companies do this all the time in automotive racing through sponsorship of teams and events.

Facebook, however, has a notorious but little known reputation for abusing the data exchanged over its networks between users. Facebook offers applications to its users and the API (Application Programming Interface) is open to any developer wishing to participate. The problem with the Facebook API, however, lies within the data made available to third-party developers. The API provides developers with information including your personal name and email all the way up to your private photos and interests that would otherwise remain private. This very flaw within the API, however, is built into Facebook's framework and to change it would mean that Facebook would cause many applications, many of whom are becoming large income-generating pieces of software, to no longer function. Instead of repairing the flaw in the system, Facebook instead chose simply to reword their user agreement but made no technical changes. What this means, is that it would be a rather simple matter of collecting all the available data made available to a programmer via an application and selling it off to the highest bidder.

4. SOCIAL NETWORKS AND PRIVACY LAWS

Cases involving social networks and personal privacy are appearing more often in courtrooms around the world. Whether it is users posting scathing blog posts that could be potentially construed as libel or governments monitoring citizen use of social networks, it is constantly a question of how far a user's personal sphere of privacy extends on the Internet.

4.1 Government Snooping

It is interesting to note two cases where governments are monitoring citizen use of social networks and the Internet. One is in the United States in a typically conservative and traditional region of the country in the state of Georgia. The state government has enacted a law requiring registered sex offenders to hand over passwords to personal web pages in addition to a federal law from 2006 that requires law enforcement officers to track the web addresses of registered sex offenders. Certainly, this could be seen as a very noble attempt to protect children and other citizens from sexual predators, but where does one draw the line? Sex offences in the United States have very wide reaching definitions and include such minor charges as statutory rape. Should someone convicted of a one-time offense for consensual sexual conduct with someone underage be subjected to a life of constant privacy invasion by the local government? What about extending the law to other people convicted of crimes? Where does one draw the line to what is and what is an unacceptable invasion of privacy?

The United Kingdom has also admitted to monitoring user activity on social networks. Government officials claim that they monitor the private message traffic between individuals. They say that they are not interested in the content of the messages, but rather who the sender and

receiver of messages are. The British government has also said that they will monitor the web browsing of citizens, record this data, and store it all in a central database. This would potentially allow a government agency to put together a very detailed picture of every citizen and/or household with an Internet connection. National security and protection against terrorism are definitely important issues, but the question comes again, where does one draw the line?

4.2 Private or Public?

Blog and forum posts have also gotten many a person in trouble ever since social networks became popular with your average citizen. People have lost their jobs because of indiscretion on their Facebook or MySpace page and others have suffered public humiliation via retaliation over remarks they made.

For instance, a court case in California established that privacy laws do not protect a rude blog post that a user made about what she thought of her hometown on her public MySpace page. The user in question had not put any kind of privacy restrictions to prevent others from viewing the blog page, therefore making it open to anyone that wanted to see it. This made the blog post officially something said in the public sphere and thus legally subject to the criticism in newspapers that it received.

There is another example of potential privacy invasion that is currently in the American court system right now. It involves two workers who were fired from a restaurant because of comments they made about customers and a manager in a private discussion group on MySpace. The group was password-protected, but that did not help them when another member of the discussion group gave the password to the group to managers of the restaurant. The managers then read the various commentaries about the restaurant from workers and decided to fire two of them. Now the fired workers are suing the company over invasion of privacy because the managers were not invited to join the group and should not have been reading what was posted in the forum.

4.3 Industry Regulation

The European Union is also heavily involved with social networks and has advocated heavily for protection of personal privacy on the Internet. While the EU does admit that, for businesses, the personal data that can be gleaned via social networks is very useful for market research, it believes that much of the data mining that is done crosses the boundaries of personal privacy. Thus, the EU has put together a task force with a charter "to improve the safety of children using social networks and to agree on a set of guidelines for use of social networks by youngsters".

This task force has already put together guidelines along with industry representatives that will allow the industries to help govern themselves. This is expected to help in a world where the rules are constantly changing and evolving faster than typical government agencies can keep up with and provide easy to follow rules and regulations.

5. SOLUTIONS

There is, however, no single, silver-bullet solution to the problems with maintaining personal privacy with a social network. Privacy solutions must be approached from multiple angles.

5.1 Social Solutions

Perhaps the largest cause of issues with personal privacy comes from the way that society has viewed the Internet. Many view it as the gateway to free knowledge and connecting the world. The issue most ignored, however, is that there is a dark side to the Internet. There are people and entities that use the Internet for less than moral purposes. Therefore, people that use social networks must acknowledge the risks that they expose themselves to and how they can reduce their personal risk.

The best way to solve the social problem is through education. Eight years ago, children were taught never to reveal anything personal about themselves outside of perhaps their first name and age and in what state or country they live in. Nowadays, children that are ten years old have social network profiles and reveal all kinds of details about themselves and have no idea what they are doing or how to protect themselves. Parents are also always slow to catch up to the ever-changing technological landscape. Parents need to *understand* what their children are doing, not only *know* what they are doing. If a child is using MySpace, then the parent needs to make sure that they know everything there is to know about MySpace so that they can protect and educate their child.

5.2 Legal Solutions

Governments also need to acknowledge that social networks pose significant risks to society and also, potentially, national security. Legislators need to draw specific guidelines that define what is public on the Internet and what is not. Without clear and concise laws, people will continue to be at risk and law enforcement officials will never have a clear answer of what they can and cannot do to protect citizens from danger.

As mentioned before, the European Union has taken significant steps towards protecting children and young adults from Internet predators. Industry representatives have been consulted by and worked with the EU in creating laws and guidelines to define privacy in a digital world.

5.3 Technical Solutions

Social network companies also need to step up and be responsible and control how members are using their networks.

MySpace has perhaps become the safer of the two largest social networks. MySpace has implemented security software that scans member pages and looks for abuse in profiles and for evidence of potential underage users. In the past, they have also increased the staff reviewing reports of abuse. The company also works with child safety groups in producing public safety ads to help warn and educate users about the potential consequences of being too open on a social network.

6. CONCLUSION

The Internet has become an aspect of daily life for the majority of the people around the world. Within this majority, social networks have also grown to be embraced by many of the Internet users as an alternative form of communication. However, with this embrace have come many unforeseen problems and threats. The idea of privacy has been changed and continues to change as people struggle to grasp and define a separation to the real world and the digital world and define laws to govern the digital world. There have been steps made in the proper direction, but there is still much to be done.

7. REFERENCES

[1] Associated Press: *Georgia Sex Offenders Must Hand Over Internet Passwords*, 30 December 2008, http://www.foxnews.com/story/0,2933,474285,00.html, called on 10.5.2009.

[2] S. Barnes: *A privacy paradox: Social networking in the United States*, *First Monday*, 11(9), September 2006.

[3] BBC: *Social Network Sites "Monitored"*, 25 March 2009, http://news.bbc.co.uk/2/hi/uk_news/politics/7962631.stm, called on 10.5.2009.

[4] J. Cline: *Planning a Company Social Network? Don't Forget Privacy Issues*, 10 April 2008, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9076678, called on 10.4.2009.

[5] B. Collins: *Privacy and Security Issues in Social Networking*, 3 October 2008, http://www.fastcompany.com/articles/2008/10/social-networking-security.html, called on 10.4.2009.

[6] C. Dwyer, S. Hiltz, K. Passerini: *Trust and Privacy Concern within Social Networking Sites: A Comparison of MySpace and Facebook*, *Proceedings of AMCIS 2007*, Keystone, Colorado.

[7] R. Padmore: *EU Presses for Web Users' Privacy*, 31 March 2009, http://news.bbc.co.uk/2/hi/europe/7973634.stm, called on 10.5.2009.

[8] W. Riddle: *MySpace Diatribe Not Protected by Privacy Rights, Says California Court*, 8 April 2009, http://www.switched.com/2009/04/08/myspace-diatribe-not-protected-by-privacy-rights-says-californi/, called on 10.5.2009.