Social Networking Searching and Privacy Issues

Man Qi Denis Edgar-Nevill

Department of computing
Canterbury Christ Church University
CT1 1QU
Canterbury, UK

Abstract

The explosion of social networking sites has not only changed the way people communicate, but also added a new dimension to the way for searching or investigating people. As users share a wide variety of information on social networking sites, concerns are growing about organisations' access to personally identifiable data and users are increasingly worried about privacy on social network sites. The main threat with data gathering is not only from where gathering it, but also where it goes afterwards. Neither social network sites providers nor the governments have any way to effectively protect users against privacy violations. However, a variety of efforts need to be explored to change the situation. Social network sites should continue work to strengthen privacy settings. Laws and policies should be improved to regulate the social networking searching in its legality, necessity and proportionality.

Keywords: social networking searching; information revelation; privacy issues; privacy setup; laws and policies

Introduction

Social networking sites, from Facebook and Twitter to LinkedIn, have become popular tools that millions of people use to communicate with friends, family, and colleagues. As of July 2011, Facebook has 750 million users around the world. Twitter has 250 million users and LinkedIn has 115 million users [Google, 2011].

Each of the social networking sites differ in various ways relating to style, layout, functionality and purpose. However most sites allow users to create personal profiles; write status updates or blog entries and post photographs, videos, and audio clips. Besides creating profiles and posting information, users can also compile lists of friends that they can link to, post public comments on their profiles, and send private messages. Users can also create groups of people with similar interests and announce events and invite people to these events.

Social networking sites means a user can not only see everything about his/her friends, but also who his/her friends know, who his/her friends' friends know, and so on. It is not uncommon for a person on a social networking site to have 300 plus friends around the world. Social networking sites truly have a wealth of information.

The explosion of social networking sites has not only changed the way people communicate, but also added a new dimension to the way that organisations search or investigate people.

More and more institutes and law enforcement agencies are using the sites for various search and investigation purposes. Concerns are growing about organisations' access to personally identifiable data and users are increasingly worried about privacy on social network sites.

Given the growing role of social networking in our society it is important users be aware of the high potential privacy risks about information sharing on these sites. As social networking search and investigation become more popular, the public needs to know the processes and the rules regulated these activities. Understanding the extent of data disclosure on the social network is the first step for all.

Information Revelation on Social Networks

Although the Internet has made it possible to publish personal information online for a decade, social networking sites are unique in that they standardize, centralize, and encourage the publication of personal data to an unprecedented extent [Art Institutes, 2011]. The sites are often thought of as places to catch up on the personal information and current activities of social ties.

Users share a wide variety of information on social networking sites. The information includes personal details and friends connections. Users online profiles may include a photo of themselves, contact information, personal information, and post additional photo albums or personal blog posts.

Activity on social networking sites can be very revealing. Many people will provide the most intimate and revealing details on their personal profiles. Revealing information on social networking sites will most often include marital status, education, address, personal identifiers etc. The information provided by the individual user and the comments from other participants, provide insight into a person's values, morals, activities, biases and self-image. Many people will be very detailed in explaining where they work, how they like their job and employer, their past education even back to their primary school, their political views as well as current interests and hobbies. In summary, there is an enormous amount of information telling you one's personality, likes and dislikes, then the type of person they were and are.

Social Networking Searching

Social networking sites have been used to search general people and seek information for employment, surveillance or investigation etc.

A June 2009 CareerBuilder.com survey of 2,600 hiring managers showed that more than 45 percent said they'd used social networking sites to seek information on job candidates. "Of those (managers) who conduct online searches/background checks of job candidates, 29% use Facebook, 26% use LinkedIn and 21% use MySpace. 11% search blogs while 7% follow candidates on Twitter," according to the survey [Haefner, Rosemary, 2009].

The survey also found that 35% of these managers decided against hiring a candidate based on information uncovered via social media sites.

CareerBuilder.com suggests that social media users keep their profiles clean of incriminating photos and gripes -- and act selectively in accepting a "friend" request.

University administrators may use social networking sites to learn about their students and their students' activities. They may take evidence posted to bring formal disciplinary charges against students.

In October of 2005, Cameron Walker, a second year student at Fisher College in Boston, MA, USA was expelled from the school and barred from the campus. Fisher College explained the reason for the action was that Walker created a Facebook group committed to the dismissal of a campus security officer believed to regularly overstep the limits of his line of duty. The college monitored Facebook, pressured Walker to remove the group, and ultimately cancelled Fisher's student status [Harvey Jones, José Hiram Soltren, 2005].

Law enforcement and other organisations may search social networking sites for evidence of people breaking laws or regulations. The sites are increasingly being used in legal and criminal investigations. Information posted on these sites has been used by police to prosecute users.

Law enforcement agents and prosecutors mine social networking sites for evidence. The evidence can reveal personal communications, establish motives and personal relationships, provide location information, prove and disprove alibis and establish crime or criminal enterprise [John Lynch, Jenny Ellickson 2010].

We know that social network sites have played key role in recent England riots. Similarly, police forces also successfully identified some rioters using the sites. According to Daily Mail [Daily Mail, 2011], In East Sussex, a 27-year-old man was remanded in custody after he allegedly encouraged looting on Facebook. Two men from Lancashire have also been charged after posting messages encouraging disorder on the social network site. A Facebook bragger of 19 was arrested after the photo of a looter and his haul appeared online [Chris Greenwood, 2011].

Here are two other cases in recent years where social networking sites helped law enforcement agencies to identify the criminals.

In August 2006, police officers at the University of Illinois at Urbana-Champaign, USA arrested two students. One student eluded arrest and the other lied about knowing the escapee. The officers were able to use Facebook to identify the escapee and show the two were "Friends" according to their Facebook pages. The dishonest student was charged with obstruction of justice [Martinez, Kiyoshi. 2006].

In October 2010, a collector's edition Wayne Gretzlcy jersey was stolen from an apparel store in Ottawa Canada. Within 15 minutes, the store staff identified the perpetrators using the store's Facebook page to review the list of 324 people on their "friend's list" who "like" the store, which included the 4 thieves. Police found the suspects and recovered the jersey valued at $1,000.00 [Butler, Don, 2010].

Numerous cases show that prosecutors are taking full advantage of social networking evidence and using it in every stage of the criminal process, including bail hearings, trials, sentencing hearings, and fugitive apprehension. [Thomas G. Frongillo; Daniel K. Gelb, 2011]

A prosecutor in USA made the following point: "As a prosecutor, the first thing I do when I get a case is to Google the victim, the suspect, and all the material witnesses. I run them all

through Facebook, MySpace, Twitter, YouTube and see what I might get. I also do a 'Google image search' and see what pops up. Sometimes there's nothing, but other times I get the goods — pictures, status updates, and better yet, blogs and articles they've written." [Thomas G. Frongillo; Daniel K. Gelb, 2011].

Sometimes undercover operations are used to communicate with suspects/targets, gain access to non-public info and map social relationships/networks [John Lynch, Jenny Ellickson 2010].

Comparing with other organisations, law enforcement agencies have 'superpower' as most social networking sites have established protocols to work with law enforcement.

Privacy Issues

Social networking sites as Facebook and MySpace hold an incredible amount of information about their users. A fully-completed Facebook profile contains a wealth of personal information: name, gender, sexual preference, birthday, political and religious views, relationship status, educational and employment history, and more. When a single entity collects and controls so much personal data, it raises a host of privacy concerns because of the potential that such data could be misused.

There are considerable discussions regarding the legality of accessing the information held on such sites. The discussion here is about informational or data privacy. Although there is some evidence suggesting that the majority of users are willing to share some private data under the right circumstances, privacy issues should be adequately addressed. In 2005, Harvey Jones and Jose Hiram Soltren, two students from MIT were able to gain access to over 70,000 Facebook profiles, then published the results of their experiment in the article "Facebook: Threats to Privacy." [Harvey Jones, José Hiram Soltren, 2005]. The study explains that many privacy issues are created by the social network users themselves. They stated that "Users disclose too much," "and third parties are actively seeking out end-user information."

Social networking sites can be a real disadvantage to job hunters or employees. Bosses can easily search for information on potential candidates and current employees. So users need to be careful with postings.

Recently privacy concerns raised as Facebook uses facial recognition software, which suggests your name to friends if they upload pictures which include you. Facebook knows what you look like, as well as where you live, who your friends are, and what you ate yesterday – because you, or people you know, have freely shared the information.

Social network sites which store information on hundreds of millions of their users have been targeted. A British advertising company WPP claims to have built the world's largest database of individuals' internet behaviour, which it says will track "almost 100 per cent" of the UK population. The company said it was pooling data from many of the world's major websites including Facebok etc. This raises great privacy concerns [Foley, Stephen 2011].

The greatest problem with data gathering is not from where gathering it, but where it goes afterwards. The safest protection should be for the minimum amount of data to be captured wherever possible.

In 2010 when Iran shut down protesters using social media and other online sites, governments can trample on freedom of association by making intrusive demands on the sites for personal information. Similar concerns existed in Egypt until President Mubarak stepped down [Swire, Peter, 2011].

Neither social network sites providers nor the government have any way to effectively protect users against privacy violations [Chahal, Shirin, 2011]. Indeed, in response to the Spring 2010 backlash, Facebook CEO Mark Zuckerberg stated that Facebook's obligation was merely to reflect "current social norms" that favored "exposure over privacy." [Chahal Shirin, 2011].

"Everything on the internet is recorded in perpetuity, therefore it's very important to govern what one says and does on the internet at all times," according to Krishna M. Sadasivam, a Media Arts & Animation instructor at The Art Institute of Tampa (a branch of Miami International University of Art & Design) [Art Institutes, 2011]. He asserts that finding a comfortable balance between sharing updates and photos with loved ones and protecting personal information is key to protecting privacy online.

Privacy Setup on Social Networking Sites

Social network sites work to strengthen privacy settings. Facebook and other social networking sites limit privacy as part of their default settings. It's important for users to go into their user settings to edit their privacy options.

These sites like Facebook give users the option to not display personal information such as birth date, email, phone number, and employment status. For those who choose to include this material, Facebook allow users to restrict access to their profile to only allow those who they accept as "friends" to view their profile. But even this level of security cannot prevent one of those friends from saving a photo to their own computer and posting it elsewhere. However, still fewer social networking site users have limited their profiles.

For users concerned about the privacy of their photos and personal information, there is one solution that will protect them -- don't join social media sites. But in a world where social media is quickly becoming a major form of networking and communication, joining may be unavoidable.

Facebook could clearly state that they could provide no guarantees regarding the security of their data, and that if users make their profiles public, all information contained therein may be viewed by job interviewers and college administrators.

Remember most social networking sites facilitate to opt out of applications, hide friend list and hide interests. However much information is still public by default.

It is vital that all social networking sites users restrict access to their profiles, not post information of illegal or policy-violating actions to their profiles, and be cautious with the information they make available.

Laws and Policies (EU Regulations)

In European Union fundamental rights in informational privacy are established in law.

The European Court of Human Rights (ECHR) [Ovey, Clare; White, Robin C. A. 2006] has made their opinion clear that there is an expectation of privacy on the internet and that there are varying degrees of privacy. Clearly a video posted on a publicly accessible web site is intended for public view, however it is unlikely that the owner intended that a third party (e.g. law enforcement) should see and use this information. Thus it must be assumed that all internet content is private information for the purposes of any activity.

The Regulation of Investigatory Powers Act 2000 (RIPA) [Crown Copyright Office, 2000], was introduced to regulate and control the activities of law enforcement and government bodies in the levels to which they intrude on the private lives of individuals. It creates a framework under which the rights of an individual are protected which is conducive with the European Convention on Human Rights. ECHR was established in UK legislation by The Human Rights Act 1998 and Amendments 2004/2005 [Crown Copy Office, 1998]. Of the various provisions of ECHR the most relevant is Article 8 – The rights to privacy.

ECHR places restriction on the justification for intruding on a person's right to privacy, based on the following tests:

Legality

Any technique used must have a foundation in domestic law. Any technique used must not interfere with the right to privacy unless there is a specific rule allowing it.

Necessity

The intrusion into a person's private life must be necessary in that it must fulfil a pressing social need and be in pursuit of a legitimate aim.

Proportionality

There must be a balance between the aim pursued and the methods used. Any method used must be the minimum possible level of intrusive behaviour by which the legitimate aim can be achieved, and must be commensurate with the pressing social need it is aimed to protect.

Only if these three tests can be met, can an intrusive behaviour be permissible.

S26(10) of The Regulation of Investigatory Powers Act 2000 (RIPA) makes it clear that private information in respect of a person includes any information relating to their private life. It is also important to consider that although information is available on the internet, that it can still be considered to be private, regardless of the fact that the owner 'published' it on the web.

Therefore if actions are for any cause other that immediate response to a report or incident, it is required to secure authority for a Directed Surveillance Authority (DSA) under S26(2) of RIPA.

In every surveillance action it is possible to encounter innocent 3rd parties who for whatever reason come into and fall out of the investigative process. RIPA requires to have due consideration for this intrusion and establish clear methods to limit the levels of incidental intrusion into innocent parties private lives. It is also required to establish, document and exercise processes to handle and protect any information we gather in the course of the investigation which relates to unrelated 3rd parties. By far the most common approach to this is to exclude such persons from the investigation as soon as their nature is identified.

In the case of real-life undercover activity, there are lots of procedural rules around how and when law enforcement performs an impersonation, but for a social network impersonation the barrier of entry is obviously very low, so any agent with a computer and an account could take on a persona." [Prince, Brian, 2010].

A Hypothetical Case of Police Searching

Social network sites are increasingly being used in legal and criminal investigations. Information posted on these sites has been used by police to prosecute users of said sites [Wikipedia, 2011].

As an example, to envisage the process undergone, the data collected and privacy concerned, we will look at a hypothetical case of police investigating on a social network site in UK [Letherby Andrew, 2008]. It also shows various levels of authority required at the various stages for the lawful investigation of these sites.

A person or group named 'ABC' is suspected to organise high street looting on Facebook. Publicity details are posted to Facebook under the guise of 'ABC' community.

To access accounts on Facebook a valid user account is needed. Once police have registered to the website, a simple search can be performed for the 'ABC'. This returns a suitable hit and allows access a group. When police access the group they find a photo of their target together with an email address. Also of note is the address bar. There is a group identity number used by Facebook to identify this group. It can also be used as part of a formal request under RIPA to Facebook for the production of material held should this become necessary. However the information available is limited. To get more information, it is necessary to join the group. This is the point at which careful thought needs to be given to authority and actions. In the case of Facebook the action of joining a group is incidental as does not require the approval of an administrator or owner. However, if such assent is required this can be construed as establishing an online relationship. In such a case a further authority will be required to deploy and use a Covert Internet Investigator to establish an online relationship. As soon as it becomes necessary to establish such a relationship, a normal investigator is not authorised to proceed as this is a Covert Human Intelligence Source role as defined under S26(8) of RIPA requiring further specialist training and higher levels of authority.

By joining the group police now reveal the membership and obtain vital trace information about members. The posts to the group are showed which can be examined and the address bar now displays the uid (user identity) number of the person posting. By selecting the users link police can see the details of the user they allow to be publicly available. Then the group

members are explored. Police would be able to see the users personal profile, photographs, comments and published communications.

Within social networking sites users often post what they consider to be incidental information such as school alumni and dates of birth which assist in the investigative process.

Lastly final details such as the administrator uid are gathered.

Once this searching is completed further enquiries can be made using the gathered Group and User Identities under RIPA to recover the user details and full profile information for the users concerned in the group.

Conclusion

The explosion in the popularity of social networking sites has generated a wealth of information. Comprehensive discovery of evidence from social networks is now imperative. The intervention to the sites can raise concerns about privacy and civil rights, particularly when it is associated with collecting and pooling large amounts of data generated by individuals. While this may be more than offset by the benefits of increased security when used by law enforcement, business applications will need to be justified. All searching and investigating activities need to comply with the relevant laws (e.g. ECPA) and policies.

Because social networking sites are still new (Facebook had its seventh birthday recently) but grow fast (exponential growth in the number of users), the ways that associations are formed may evolve rapidly, as might government efforts to regulate for privacy or other purposes.

References

Art Institute, Online Social Media: An Open Door to Your Privacy? http://insite.artinstitutes.edu/online-social-media-an-open-door-to-your-privacy-20838.aspx (last visited 15th August 2011)

Butler, Don, "Facebook helps store owner track thief" Yahoo News, 31 Oct 2010

Chahal Shirin, Balancing the Scales of Justice: Undercover Investigations on Social Networking Sites, The Journal on Telecommunications and High Technology Law (JTHTL), no1 vol 9, 2011

Chris Greenwood, Facing justice, riot rat pack: Suspects accused of four of the week's most infamous crimes are all behind bars. Daily Mail, 13th August 2011, http://www.dailymail.co.uk/news/article-2025392/London-riots-rat-pack-face-justice-Ealing-murder-Facebookbragger.html?ito=feeds-newsxml (last visited 15th August 2011)

Crown Copyright Office, Regulation of Investigatory Powers Act 2000, Crown Copyright Office of Pubic Sector Information -ISBN 10 0105423009

Crown Copyright Office, The Human Rights Act 1998 - Crown Copyright Office of Pubic Sector Information - ISBN 13: 9780105442981

Daily Mail, 12th August 2011, http://www.dailymail.co.uk/news/article-2024767/Man-charged-riot-incitement-Facebook-looters-guilty.html (last visited 15th August 2011)

Foley, Stephen 2011 Database boasts it will track web behaviour of everyone in UK, http://www.independent.co.uk/news/media/online/database-boasts-it-will-track-web-behaviour-of-everyone-in-uk-2303657.html (last visited 15th August 2011)

Google, Social network user statistics as of July 2011, http://google-plus.com/598/social-network-user-statistics-as-of-july-2011/ (last visited 15th August 2011)

Haefner, Rosemary, More Employers Screening Candidates via Social Networking Sites, http://www.careerbuilder.com/Article/CB-1337-Interview-Tips-More-Employers-Screening-Candidates-via-Social-Networking-Sites/ (last visited 15th August 2011)

Harvey Jones, José Hiram Soltren, 2005, Facebook Threats to Privacy, http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf, (last visited 15th August 2011)

John Lynch, Jenny Ellickson, 2010, Obtaining and Using Evidence from Social Networking Sites, http://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf, (last visited 15th August 2011)

Letherby Andrew, 2008, Social Networking Searching, Technical Report, 2008

Martinez, Kiyoshi. Student arrested after police Facebook him, Daily Illini.com 1 Aug 2006

Ovey, Clare; White, Robin C. A. (2006). Jacobs & White: The European Convention on Human Rights (4th ed.). Oxford University Press. ISBN 0-19-928810-0.

Prince, Brian, 2010. Social Network Privacy Concerns Raised by Undercover Police Tactics http://www.eweek.com/c/a/Security/Social-Network-Privacy-Concerns-Raised-by-Undercover-Police-Tactics-409306/ (last visited 15th August 2011)

Swire, Peter, Social Networks, Privacy, and Freedom of Association, 2011, http://www.americanprogress.org/issues/2011/02/pdf/social_networks_privacy.pdf (last visited 15th August 2011)

Thomas G. Frongillo; Daniel K. Gelb, 2011, It's Time to Level the Playing Field - The Defense's Use of Evidence from Social Networking Sites http://www.nacdl.org/public.nsf/01c1e7698280d20385256d0b00789923/363336b5ff64b443852577c100550272?OpenDocument

Wikipedia, 2011, Use of social network websites in investigations http://en.wikipedia.org/wiki/Use_of_social_network_websites_in_investigations (last visited 15th August 2011)