The Security Implications Of Ubiquitous Social Media

Chris Rose, Walden University, USA

ABSTRACT

Social media web sites allow users to share information, communicate with each other, network and interact but because of the easy transfer of information between different social media sites, information that should be private becomes public and opens the users to serious security risks. In addition, there is also massive over-sharing of information by the users of these sites, and if this is combined with the increased availability of location-based information, then all this can be aggregated causing an unacceptable risks and unintended consequences for users.

INTRODUCTION

The dot-com bubble in 2001 was an economic disaster and marked a turning point for the Internet. At that time many pundits claimed that the importance of the Internet as a vehicle for commerce was overstated, however, in many of these instances a collapse was just a result of evolving technologies and the rise of Web 2.0. "The concept of "Web 2.0" began with a conference brainstorming session between O'Reilly and MediaLive International. Dale Dougherty, web pioneer and O'Reilly VP, noted that far from having "crashed", the web was more important than ever, with exciting new applications and sites popping up with surprising regularity" (O"Reilly, 2005).

At the Open Government and Innovations Conference in Washington in 2009, speakers noted that people talk about Web 2.0 as if it is a fully evolved media when in fact it is not. The deputy associate director of national intelligence for intelligence community information assurance at the Office of the Director of National Intelligence Mark Morrison stated "From a security perspective, you lay yourself open for more vulnerabilities and more attacks by allowing the protocols, communications and the acceptance of data from outside sources that cannot be trusted and you do not know" (Beizer, 2009).

Social media have become some of the most dominant features on the Internet during the growth of the interactive (Web 2.0) Internet. Social media can be described as a website that not only provides information, but interacts with you while it is giving you that information. Examples would include Myspace, Facebook, LinkedIn, Foursquare and Twitter or any other site that allows users to share personal information. In a traditional web site, the content is delivered to the end user but they are not allowed to update or participate in the creation of the content on the web site. In social media, people are communicating, sharing, networking and interacting with others.

The social networking website, Facebook, has had phenomenal growth and has overtaken Google's popularity among US Internet users. Facebook's membership has more than doubled in the past year, passing the 200 million mark last April and 400 million in February. Industry data shows it has scored more visits on its home page than Google. "In a sign that the web is becoming more sociable than searchable, research firm Hitwise said that Facebook and Google accounted for 14% of all US Internet traffic. Facebook's home page recorded 7.07% of traffic and Google's 7.03%. Internet users worldwide spent more than 5.5 hours a month on social networking sites such as Facebook and Twitter in December 2009, an 82% increase over the previous year, according to the Nielsen Company research firm" (Nuttall & Gelles, 2010).

The rise of Facebook has also brought with it increased scrutiny from regulators and privacy advocates. Regulators all over the world are grappling with the problem of how to contend with a phenomenon that in five years has become the top site on the Internet. In fact, privacy advocates question the direction social media sites are

heading since Facebook recently implemented changes that made most of its users' personal information public by default and even allows the sharing of user information automatically with some third-party websites (Gelles, 2010).

LOCATION BASED INFORMATION

Location-based information sharing has become very popular recently and if used carefully can be a very helpful tool for users. For example, Google Maps has a feature called Latitude, which allows users to see the location of their family or friends in real time, provided the other party agrees to share their information. The benefits are obvious in certain situations, such as parents wanting to keep track of where their children are at any given time.

On Twitter a new feature has the option of including your location when the user tweets using a tracking tool they can turn on or off. When activated, tweets link to a Google map of the area the user is in. This trend towards location sharing used by Foursquare, Gowalla and Loopt –is also expected to be included into Facebook . Twitter believes the tool makes it useful for anyone looking for real-time information (McCabe, 2010).

Google introduced a social media application designed to integrate into their Gmail email service called Google Buzz, however it was strongly criticized for ignoring privacy. When someone uses Google Buzz it posts the location of the user and on the mobile version of Buzz, it integrates with Google Maps to display the location of all users of Buzz who are near them because posts made by Buzz are public. Initially, there was an uproar by privacy advocates who threatened lawsuits but surprisingly very few users seemed to be concerned and Sergey Brin of Google downplayed the problem. "Within four days of its launch, millions of people proved Brin right by using the messaging service to publish 9 million posts" (McCullagh, 2010a). In fact, there appeared to be a backlash to the backlash with people pointing out that only if you had elected to publish that information would the Buzz publish the location.

Society is changing, norms are changing, confidentiality is being replaced by openness. If you join YouTube, Loopt, Facebook, FriendFeed, Flickr, and other social media sites, this means giving up some privacy, but millions of people are willing do so just to be a part of this social media phenomenon. "Of people with an online profile, nearly 40 percent have disabled privacy settings so anyone may view it, according to a Pew Internet survey released a year ago. The percentage is probably higher today. The truth about privacy is counter-intuitive: less of it can lead to a more virtuous society" (McCullagh, 2010a). Ironically, US deputy CTO Andrew McLaughlin was among those who belatedly realized that the Google Buzz Gmail add-on had publicly exposed the people he emails and chats with the most. "McLaughlin joined the Obama administration after serving as Google's chief lobbyist - its head of global public policy. The blog counts 28 Google employees in his contacts list, including several top Google lobbyists and lawyers. By default, Buzz adds the people you e-mail most as your 'followers', and then lists them on your public Google Profile Page" (Metz, 2010).

At a technology conference in January, Facebook CEO Mark Zuckerberg told his audience that Internet users don't care as much about privacy anymore and in the seven years since he started the company, "people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people--and that social norm is just something that has evolved over time." Zuckerberg defended the company's decision in December to push users to reveal more, saying "we decided that these would be the social norms now and we just went for it" (McCullagh, 2010a). Facebook has also just introduced a "like" button, however, "a fact that is often overlooked in the rush towards ubiquitous social connectivity is that Facebook users still don't know what they are sharing, with whom, or why it matters. It is a powerful tool, but my bet is most Facebook users will have no idea where, when, or how their Likes will show up on the Web. Or for how long" (Costa 2010).

Unlike government invasion of privacy, these are all voluntary declarations. Perhaps the real issue is not technological but psychological, "if one can choose how much or how little to divulge about oneself to another voluntarily, privacy is maintained," Irwin Altman, a professor emeritus in the University of Utah's wrote, "If another person can influence how much information we divulge about ourselves or how much information input we let in about others, a lower level of privacy exists" (McCullagh, 2010a).

OVERSHARING

People are becoming more comfortable using the Internet. A few years ago most people were extremely hesitant to even disclose their real names online, but perhaps they are becoming too comfortable. (Groeneveld, Borsboom & van Amstel, 2010). "A 2008 Harris Interactive/CTIA survey of more than 2,000 American teens confirms that youth are least worried about privacy. Only 41 percent were concerned; 59 percent were happy to provide personal information to marketers. Compare this to a Harris poll conducted in 1998, the same year Google was founded, that found a remarkable 80 percent of people were hesitant to shop online because of privacy worries" (McCullagh, 2010a). "Humans have a natural inclination to want what they cannot have. The voracious human appetite for sharing information, combined with the countless ways to access the Internet have frustrated attempts to block access to social media sites. No matter what, people will find ways to socialize and share during work hours" (Ferenstein 2010).

One common problem on social media web sites is over-sharing whereby people disclose too much information which in the long run might mean more risk and have unintended consequences. With social media people are now sharing information about their exact location but sharing location-based information just means there is another layer of personal information exposed which, in most cases, is not really necessary. Most social networks allow the users to send messages to different sites and it is extremely easy to forget what information was divulged and who has access to it. In addition, most social networks have a good integrated search function which people use to find friends or things they are interested in but this also means that people, other than their friends, can also find their information and also find them. If you allow messages between different social networks, what you intended to be private can become public. "For example, you might relay your Foursquare location to your public Twitter account and by doing this expose the message to the whole world" (Groeneveld, Borsboom & van Amstel, 2010).

INFORMATION AGGREGATION

Please Rob Me is a web site that consists exclusively of an aggregation and updates of public Twitter messages that have been routed through the location-based networking site Foursquare, a service that encourages people to share their whereabouts with their friends. The site automatically scans Twitter feeds to find location check-ins that people are sending out through Twitter. It shows the messages and then sends a message on Twitter such as:

Hi @NAME, did you know the whole world can see your location through Twitter? #pleaserobme.com

The Please Rob Me site explains its rationale. "If you're pushing a "check-in" from Gowalla, Brightkite, or Foursquare to a local restaurant out to your public Twitter stream, you're broadcasting that you aren't home. Which could be taken to mean that your home is ripe for burglary" (McCarthy, C. 2010). "The danger is publicly telling people where you are. This is because it leaves one place you're definitely not… home. So here we are; on one end we're leaving lights on when we're going on a holiday, and on the other we're telling everybody on the internet we're not home"(Siegler, 2010).

Hamas has also accused Israel of using Facebook to recruit Palestinian spies from among the Gaza strip community. Israel has always maintained agents in the West Bank and Gaza but Hamas thinks that fans of Facebook and similar services are revealing too much personal information on social networking which leaves them open to attempts to coerce them into becoming spies. In reality it seems more likely that Israel is using social networking to map contact networks. It is suggested that Israeli may be monitoring social networking sites to identify networks on contacts with links to either Hamas or local criminal networks (Leyden 2010).

Pete Warden, the "Facebook Whisperer," has an unusual hobby he took up more than a year ago. By using ordinary Web crawling software, he has assembled a database of 210 million Facebook public profiles: Names, "fan" pages, friend listings, and locations and used that data to find, for example, where a certain name or term was the top fan site, the geographic reach of virtual social networks, and more. Warden soon realized that full-time social science researchers might take his data in new directions and was about to distribute the data when Facebook shut

down his project. "The fundamental problem here is that the data I was planning to release is still crawlable by anyone else and there's a lot of commercial companies that have grabbed the same dataset"(Kuang, 2010).

RISKS THROUGH DIRECT DISCLOSURE

Many persons in sensitive positions do not think clearly before placing their private thoughts in their social media accounts. A few recent examples aptly demonstrates this security risk.

Recently it was reported that the Israel Defense Force had to call off a raid after a soldier who had been briefed on an upcoming operation posted the confidential information about the operation, including the time and place, on Facebook. The soldier posted "On Wednesday, we are cleaning up (the village). Today - arrest. On Thursday, God willing, we will be home,"(CNN.com, 2010)

In Fort Pierce, a prosecutor composed a Gilligan's Island remix, but in it he included facts about a felony assault trial he was involved in, and he then posted this to his Facebook account:

"Just sit right back and you'll hear a tale, a tale of a fateful trial that started from this court in St. Lucie County. The lead prosecutor was a good woman, the 2nd chair was totally awesome. Six jurors were ready for trial that day for a four hour trial, a four hour trial.
The trial started easy enough by then became rough. The judge and jury confused, If not for the courage of the fearless prosecutors, the trial would be lost, the trial would be lost. The trial started Tuesday, continued til Wednesday and then Thursday With Robyn and Brandon too, the weasel face, the gang banger defendant, the Judge, clerk, and Ritzline here in St. Lucie."

The judge declared a mistrial and a reputed gang member was freed (Wright 2010).

"Keri McMullen and Kurt Pendleton left a status update on Facebook Saturday night that said they wouldn't be home because they were going to a concert in nearby Louisville at 8 p.m. Two burglars entered their house, using a screwdriver to force open a back door. They had recently installed a surveillance system in their home. The cameras caught the entire episode on tape. The video shows the two men going through McMullen's purse, stealing electronics -- more than $10,000 worth -- including a plasma television right off the wall. The burglars are then seen driving away with a laundry basket filled with the stolen goods. After posting images of the suspects on Facebook, McMullen realized one of them had "friended" her about six months ago. She says he grew up across the street from her and hasn't seen him in more than 20 years" (CBS News)

In all these cases it was over-sharing and the aggregation of information that could be made public with information that should remain private that led to the security breach.

RISK BY DESIGN

Facebook has also recently changed its privacy policy. The new policy talks about being able to tag Facebook friends by "place," not just by name in photos or videos. Another section "allows "pre-approved third party Web sites and applications" that use Facebook Platform to obtain general information about you, including name, photo, friend list, and public information from your account--as long as you're still logged into Facebook. That means "you and your friend can be connected on that Web site as well as long as both of you have an account on that Web site" (McCullagh, 2010b). However, there are hundreds of thousands of developers approved by Facebook to create games, quizzes and other applications and some of those developers are able to access the same basic information about users after a Facebook friend has started using their application(Gross, 2010). In fact, many Facebook users were shocked to find that many of the applications on Facebook, such as a quiz "could access almost everything on a user profile, including hometown, groups you belong to, events attended, favorite books, and more. What's worse is that your profile information becomes available to developers when your friends take the same quiz"(Perez 2010).

Facebook wants to replicate the Facebook experience wherever you go on the Internet. It is started with a few launch partners for the new "Facebook Platform". For example, "if you're logged into Facebook and go to Pandora for the first time, it can immediately start playing songs from bands you've liked across the web. And as you're playing music, it can show you friends who also like the same songs as you, and then you can click to see other music they like." It is great to be able to see what your friends have been listening to but perhaps those friends have no idea they are sharing with you (Technology Live 2010).

CONCLUSION

The digital revolution has changed the way we carry out everyday tasks. Society is changing, norms are changing, confidentiality is being replaced by openness but privacy advocates say that convenience has come at the cost of privacy. Almost everything that is done in today's society leaves a track, some sort of digital footprint that can put your personal information at a higher risk. In fact, according to an annual survey released by Javelin Strategy and Research, in 2009 more than 11 million U.S. consumers were victims of identity theft. (Oppmann, 2010) "Facebook is, by its nature, a social experience. But as the undisputed king of social networking expands ways for its users to interact, it's raising more questions about how much of their information is made available to people they don't know. In some cases, users may not even realize it's happening." (Gross, 2010)

Therefore as long as social media sites can share information with other social media sites and location-sharing is allowed (and people are becoming comfortable with disclosing such information), then persons who should not know certain information will readily be able to get that information. Combine this with overly enthusiastic users, who intentionally or not, share too much personal information and developers who can access private information, then ubiquitous social media will present a very severe and often overlooked security risk.

REFERENCES

1. Beizer, D. (2009, July 24). Security risks evolve alongside social media. Federal Computer Week. Retrieved April 3, 2010 from http://fcw.com/Articles/2009/07/27/WEEK-Web-security-risks.aspx
2. CBS News. (2010, March 25). Facebook "Friend" Suspected in Burglary. Retrieved April 5, 2010 from http://www.cbsnews.com/stories/2010/03/25/earlyshow/main6331796.shtml?tag=cbsnewsSectionContent.2
3. CNN.com. (2010, March 4). Israeli military calls off raid after soldier posts details. Retrieved April 3, 2010 from http://www.cnn.com/2010/WORLD/meast/03/03/israel.raid.facebook/index.html
4. Costa, D. (2010, April 22). Facebook: Privacy Enemy Number One?. PC Magazine. Retrieved April 24, 2010 from http://www.pcmag.com/article2/0,2817,2362967,00.asp?kc=PCRSS03079TX1K0000585
5. Ferenstein, G. (2010, April 14). Why Banning Social Media Often Backfires. Mashable. Retrieved April 18, 2010 from http://mashable.com/2010/04/13/social-media-ban-backfire/
6. Gelles, D. (2010, April 11). Facebook under privacy microscope. Financial Times. Retrieved April 11, 2010 from http://www.ft.com/cms/s/0/a807eaf6-4593-11df-9e46-00144feab49a.html?ftcamp=rss
7. Groeneveld F, Borsboom,B. & van Amstel, B.(2010, February 24). Over-sharing and Location Awareness. Center for Democracy & Technology. Retrieved February 24, 2010 from http://www.cdt.org/blogs/cdt/over-sharing-and-location-awareness
8. Gross, D. (2010, April 1). Sharing vs. your privacy on Facebook. CNN. Retrieved April 6, 2010 from http://www.cnn.com/2010/TECH/ptech/04/01/facebook.developers.privacy/index.html?hpt=Sbin
9. Kuang, C.(2010, April 5). Facebook Whisperer Speaks About Why Facebook Threatened to Sue Him. Fast Company. Retrieved April 7, 2010 from http://www.fastcompany.com/1607273/exclusive-facebook-data-guru-speaks-about-why-facebook-threatened-to-sue-him
10. Leyden, J. (2010, April 7). Israel using Facebook as 'spying tool' in Gaza. The Register. Retrieved April 10, 2010 from http://www.theregister.co.uk/2010/04/07/facebook_spying_gaza/
11. McCarthy, C. (2010, February 17). The dark side of geo: PleaseRobMe.com. CNet News. Retrieved on April 4/2010 from http://news.cnet.com/8301-13577_3-10454981-36.html
12. McCullagh, D. (2010a, March 12) Why no one cares about privacy anymore. CNet News. Retrieved April 5, 2010 from http://news.cnet.com/8301-13578_3-20000336-38.html

13. McCullagh, D. (2010b, March 26). Revised Facebook policy hints at location tagging. CNet News. Retrieved April 5, 2010 from http://news.cnet.com/8301-13578_3-20001303-38.html?tag=newsEditorsPicksArea.0
14. Metz, C. (2010, April 2). Buzzed Gmail outs Googly ties of Obama's deputy CTO. The Register. Retrieved April 6, 2010 from http://www.theregister.co.uk/2010/04/02/google_buzz_outs_andrew_mclaughlin_contacts/
15. Nuttall, C. and Gelles, D. (2010, March 16). Facebook becomes bigger hit than Google. Financial Times. Retrieved April 6, 2010 from http://www.ft.com/cms/s/2/67e89ae8-30f7-11df-b057-00144feabdc0.html
16. Oppmann, P. (2010, April 14). In digital world, we trade privacy for convenience. CNN.com. Retrieved April 16, 2010 from http://edition.cnn.com/2010/TECH/04/14/oppmann.off.the.grid/index.html?hpt=C1
17. O'Reilly, T. (2005) What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software. Oreilly.com. Retrieved April 23, 2010 from http://oreilly.com/web2/archive/what-is-web-20.html
18. Perez, S. (2010, April 22). How to Delete Facebook Applications (and Why You Should). ReadWriteWeb. Retrieved April 23 2010 from http://www.readwriteweb.com/archives/how_to_delete_facebook_applications_and_why_you_should.php
19. Siegler, M. (2010, February 17). Please Rob Me Makes Foursquare Super Useful For Burglars. RechCrunch. Retrieved April 23, 2010 from http://techcrunch.com/2010/02/17/please-rob-me-makes-foursquare-super-useful-for-burglars/
20. Technology Live.(2010, April 23). What new Facebook updates might mean for your privacy. Retrieved April 24, 2010 from http://content.usatoday.com/communities/technologylive/post/2010/04/what-new-facebook-updates-might-mean-for-your-privacy/1
21. Wright, T. (2010, April 19). Lawyer Marooned After "Gilligan's Island" Facebook Poem. MSNBC. Retrieved April 21, 2010 from http://www.msnbc.msn.com/id/36711298

