Lack of Privacy Awareness in Social Networks

Social networks have opened up a new avenue of communication for millions of people around the world. The major attraction of this technology is the ease with which people can share their personal information with their friends. In analyzing this new technology, one needs to first understand the clear meaning of social networks. The following definition will be used in the analysis of this concept: Social networks are facilitated by web technology that allows several users to publish content freely on any subject for use by friends and others. Such sites allow users to create personal profiles visible to the people they allow.

This phenomenon started with the tool known as Six Degrees, launched in 1997 by Andrew Weinrich in New York, New York, USA. This was the first social network. In 2000, Richard Ericsson launched a social network in Sweden called the Lunar Storm for use by teenagers. This social network became extremely popular.1

The next significant event in social network evolution occurred when Friendster was launched in San Francisco, California, USA, by Jonathan Abrams in February 2005. Friendster grew too rapidly and was unable to maintain a high quality of service.2 Future social networks MySpace and Facebook learned from the failures of Friendster. In May 2003, Reid Hoffman launched LinkedIn from San Francisco, California, USA, with a focus on connecting all business people. Today, with over 160 million users, LinkedIn is one of the four major social media networks.3 Popularity of social networks seemed evident and so Orkut Buyukkokten of Stanford University (California, USA), created Club Nexus for use by Stanford University students in 2001. Google helped him launch this network as Orkut in January 2004, a watershed year in the rapid growth of social networks. Orkut was the dominant social network in Brazil until 20114 and widely popular in India as well. The next major entrant to the social network scene was MySpace by Tom Anderson and Chris DeWolfe, from Los Angeles, California, USA, in August 2003. MySpace grew rapidly and became the network of choice among high school and college students.5 Today, MySpace has switched its focus to music-related activities.6

In concluding the history of social networks evolution, it is important to mention the two major players in the field: Facebook and Twitter. Facebook was launched by Mark Zuckerberg and his friends from Harvard University (Cambridge, Massachusetts, USA) in 2004. Facebook adopted a staggered-launch approach to meet the demand. Today, Facebook has grown to be the number-one social network around the world with a subscriber base of 845 million.7 Jack Dorsey and his friends launched Twitter in 2006 from San Francisco, California, USA, as a way to share one’s thoughts with 140 characters at most in the message. Today, Twitter has more than 600 million customers worldwide.8 Many people follow the tweets of others, not necessarily their friends.

In all the tools identified so far, the major goal has been ease of use and sharing of information. With this came the concern of excessive information sharing, often without the knowledge of the user. Compounding this problem have been the periodic changes in privacy policies that resulted in users losing control of their personal information posted online. Facebook, with several hundred million users worldwide, has also contributed to the concerns about privacy, according to a 2011 report from the Federal Trade Commission.9

USER PERCEPTIONS

Social media users believe that convenience comes first. Users do not have any reservations about providing personal information as part of their profile.10 When the user gives personally identifiable information (PII), such as address and date of birth, the intent is for the benefit of friends. Users believe that their friends already know the PII and they are sharing something that only provides clarity to their circle of friends. Issues arise when access to the information is extended beyond the circle of friends by

S. Srinivasan is professor of information systems (IS) and chairman of technology studies at the Texas A&M International University (TAMIU), Laredo, Texas, USA. Prior to joining TAMIU, Srinivasan was at the University of Louisville (Kentucky, USA). He started the information assurance (IA) program at the University of Louisville in 2003. This program was designated a national center of academic excellence in internal audit (IA) education by the National Security Agency and the Department of Homeland Security (NSA/DHS). Srinivasan’s research interests are in information security. He can be contacted at srini@tamiu.edu.
transferring of privileges. This is where the initial privacy compromises take place.

In many cases, the customer is unaware of the extent to which the PII has spread. One reason for this confusion is the way social networks enable the settings for the account. If sharing privileges were made available by default as opt in, as opposed to opt out, it would greatly facilitate user control for PII. Another reason is the fact that social networks are still emerging. Until they reach a mature state, privacy concerns will continue to pose problems. For example, consumers still trust their friends more than any other source when it comes to researching a product, service or a topic.

When looking at the rapid growth of social networks, it is worth noting that the three most popular social networks were launched less than a decade ago. Their millions of users point to the public’s desire to keep connected to their friends and coworkers. Therefore, some of the privacy issues can be attributed to the growing pains of the rapidly changing technological landscape.

Another viewpoint to consider in this regard is the perceptions of the majority of users who are on social networks. Even though social networks have pervaded every demographic, they are still widely used by people in the 17–24 age group. People in this age group tend to trust systems more and do not have concerns about their personal information getting misused. Also, they might unwittingly provide their information and do not see reasons to be cautious in social networks. According to a 2007 research survey, nearly 90 percent of teenagers post a video and expect feedback from their friends. This attitude lends itself to keeping some privacy settings open to a larger group of people. These kinds of benefits of social networks, especially Facebook, are further reinforced by the study of M. D. Roblyer. The main benefits to note from Roblyer’s study are summarized in figure 1.

An innate problem that many Facebook users seem to overlook is the possibility that personal information could be released to unintended people. Many users perceive that when they add a friend, their friend will be judicious in passing on the privilege to view their information to others. However, many users are not that discriminating when it comes to setting the privileges. The Technology Acceptance Model (TAM) was used in analyzing this aspect of user perceptions (see figure 2). Two of the three main components of the TAM are “perceived ease of use” and “perceived usefulness.” Facebook users clearly experience the ease of use aspect in connecting with their friends. They value such interactions with their friends and find Facebook useful in facilitating those interactions, thus validating the second aspect of TAM concerning perceived usefulness. The overwhelming numbers of Facebook users demonstrate that their use of Facebook clearly validates the third and final piece of TAM, namely the “behavioral intention to use.”

Moreover, the analysis shows that users perceive ease of use as an overwhelming factor in overlooking the trust aspects when it comes to befriending new persons on a social network. Furthermore, Catherine Dwyer also studied the trust aspects in social networks and found that users overwhelmingly feel comfortable sharing personal information on the network for the benefit of their friends. This observation is validated by a 2011 Pew Internet and American Life Project research survey, which showed that 91 percent of all social networking teens use the sites to stay in touch with friends, while 82 percent use the sites to stay in touch with friends they do not see in person often.

---

**Figure 1—Summary of Student Responses on Reasons for Using Facebook**

<table>
<thead>
<tr>
<th>Criteria for use</th>
<th>Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep in touch with friends</td>
<td>92.5 percent</td>
</tr>
<tr>
<td>Let others know what is happening in my life</td>
<td>48 percent</td>
</tr>
<tr>
<td>Connect with people I have lost touch with</td>
<td>72 percent</td>
</tr>
</tbody>
</table>

Source: Davis, Fred

---

**Figure 2—Technology Acceptance Model**

- Perceived Usefulness
- Perceived Ease of Use
- Behavioral Intention to Use

Source: Davis, Fred
PRIVACY AND SECURITY

The concept of privacy in general dictates that no one should be able to observe things about a person without that person’s knowledge. In social networks, privacy is greatly ignored unwittingly. Many people perceive that rejecting a request to be your friend based on one of your other friends’ recommendations might be considered rude.20 It is important to recognize that friendships are dynamic. A typical scenario in Facebook could be that a friend posts “Five Things About Me” and encourages the recipient to do the same. In response to this suggestion from a friend, the posting by the recipient states, “I attended Valley High,” and, “My cat’s name is Myra.” It is likely that the user has chosen these two answers as his/her challenge response for an online bank account. This simple scenario points to the vulnerability of exposing personal information unwittingly.21

One type of serious privacy violation that occurs in social networks involves photos. A conscientious user might have placed appropriate controls on his/her settings concerning the ability to view photos posted on his/her wall. When a friend posts a photo on his/her wall without putting it in context and invites all mutual friends to view the photos, it could jeopardize the carefully crafted privacy settings of the first user. This kind of privacy violation is all too common in social networks. A similar experience was also discussed by Dwyer about a teacher feeling awkward after her students befriended her and posted some pictures.22 Another source of privacy violations on Facebook involves third-party applications. Users constantly subscribe to new and popular applications. Such applications find acceptance because they are referred by friends. Consider the following scenario in which the user has violated his/her own carefully crafted privacy settings: User downloads a phone app which finds the answer to the question, “Which 1970s movie reflects you?” Before this app is launched, the user is informed that in order to find the answer to the question the app needs access to the user’s profile and that of his/her friends. A whole host of privacy settings have been violated by the simple use of this one app. In the world of social networks, such apps are prevalent. Aaron Beach, Mike Gartrell and Richard Han have studied the role of applications in violating user privacy,23 thereby reinforcing the statement that applications have a way of bypassing some of the security controls.

The ease of use in social networks significantly contributes to many privacy violations. For example, two users participating in the update-and-reply feature of a Twitter conversation are unwittingly sharing their conversations with their friends unless they took specific steps to block the feeds.24 Twitter feeds are brief but contribute to some major privacy violations. A large corporation that allows the use of Twitter by employees could face a serious threat. An employee might tweet to one of his close confidants that a new system developed by the organization has a serious bug. Unfortunately, Twitter feeds are followed by many, and so a confidential organizational problem is now exposed. This example shows that privacy violations need not be at the individual level.

According to a 2011 research survey, social networks provide “a concentrated posse of easily contactable friends.”25 Given the large number of friends to communicate with on social networks, many use the networks in a variety of ways. The research survey results appear in figure 3.

These statistics show how information gets posted and communicated among friends through social networks without much filtering. Potential users must be aware that what is posted on social networks will find its way to a very large audience quickly, so any information that could expose one’s privacy should be guarded.

<table>
<thead>
<tr>
<th>Figure 3—Uses of Social Networks for Communication With Friends</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of Use</strong></td>
</tr>
<tr>
<td>Post messages to a friend’s page or wall.</td>
</tr>
<tr>
<td>Send private messages to a friend through the social network system.</td>
</tr>
<tr>
<td>Post comments to a friend’s blog.</td>
</tr>
<tr>
<td>Send a group message to all friends.</td>
</tr>
<tr>
<td>Give e-props or kudos to friends.</td>
</tr>
</tbody>
</table>

Source: Pew Internet and American Life Project research survey

The benefits of social networks extend not only to individuals, but also businesses. In a survey of 72 business managers conducted at Texas A&M International University regarding the perception of the use of social networks in business, the respondents were skeptical of new technologies. However, they recognized that the introduction of both the Internet and email had significant benefits to business. With this experience, the analysis of the data shows that managers perceived that the use of social networks in business builds:

• Employee morale
• Satisfaction
• Commitment
• Enhanced performance
The survey showed that some managers perceived that allowing the use of social networks at work is essential because their competition allows it. This line of reasoning should be tempered by the fact that every business should assess its business goals in light of what technology has to offer.

Social networks realize the importance of security and provide some tools to protect the information. However, the overwhelming goal is ease of use and rapid dissemination of information. It is clear from various statistics on the use of social networks that younger people use it extensively. The prior comment concerning the goals of social networks comes as a result of this observation as well as the fact that older adults also use social networks for ease of use and rapid communication capabilities. These aspects pose an inherent security problem in social networks.

A typical Facebook user’s preferred device of choice is the cell phone. Even though setting a user ID and password are options from a cell phone, virtually all users ignore this aspect for the sake of convenience. Given this fact, if the cell phone is misplaced or lost, then anyone obtaining the device will have access to the Facebook account of the user. Someone with a criminal intent could post a damaging or misleading message.

A new security threat is emerging in social networks because of location tracking. Facebook has a feature called “check-in,” which lets friends know one’s GPS location. Since one’s circle of friends sometimes gets very large simply by transference of friends, one must monitor one’s privacy settings closely.

The login notification on Facebook is similar to Skype. Friends are notified when a user logs into their Facebook account. Facebook and other social networks let members link up to their account in other popular sites such as YouTube. Even though this feature allows for the setting up of user ID and password, many users simply ignore this security feature. Thus, a user logged into one social network potentially exposes all their other accounts as well.

On Facebook, the update feature is a major security vulnerability. An innocuous message such as, “I am looking forward to my vacation in Europe next month,” gets forwarded to a large circle of friends. Since some of the friends are basically acquaintances, the user has essentially broadcast a message that they are not going to be home, thereby creating an opportunity for someone to rob them.

These simple instances illustrate the security threats widely prevalent in social networks.

**BEST PRACTICES**

This article highlights some of the widely practiced usage patterns in social networks that may lead to privacy and security vulnerabilities of one’s confidential information and personal safety. In this section, some best practices are provided for users to protect their privacy.

First, users should not feel obligated to accept invitations from friends because they show a referral from another friend. This preventive action alone could significantly enhance privacy and security because the people whom a user accepts as friends should indeed be people known to the user.

Second, in social networks URL shortening or obfuscation is widespread. Since trust among friends is widespread, people with criminal intent befriend people to post obfuscated web links to questionable sites. To protect against such an intrusion into their circle of friends, users should choose to copy and paste the web link rather than navigate from it directly. If a web link appears questionable, there are web sites such as www.longurl.org or www.longurlplease.com that can verify the authenticity of web links.

Finally, attachments are another source of potential threat in social networks, and users should remain vigilant. The vulnerable aspect of attachments is that even if they appear to emanate from known friends, they could be potential attacks originated by hijacking users’ address books.

**CONCLUSION**

Social networks have revolutionized communication among an extended circle of friends. This technology has many benefits to offer society. Millions of people around the world are benefiting from the use of social networks. An analysis of this new technology shows that it has many positive aspects, but at the same time it has significant problems with respect to privacy of information and security. Social networks themselves are evolving and, as such, some of the settings that could offer the necessary security and privacy are still emerging. The ease of use aspect of the major social networks, such as Facebook, Twitter and LinkedIn, undermines their privacy and security features. The discussion established in this article also sheds light on some of the steps users can take to protect both privacy and security.
ENDNOTES

1 Kirkpatrick, David; *The Facebook Effect*, Simon and Schuster, USA, 2010


3 LinkedIn Press Center, [http://press.linkedin.com/about](http://press.linkedin.com/about)


5 *Op cit*, Kirkpatrick


7 Crunch Base, [www.crunchbase.com/company/facebook](http://www.crunchbase.com/company/facebook)


10 Jeff Fox, May 2012, [http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm](http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm)

11 Dwyer, Catherine; Starr Roxanne Hiltz; Katia Passerini; *Trust and Privacy Concern With Social Networking Sites: A Comparison of Facebook and MySpace*, Proceedings of 13th Americas Conference on Information Systems (AMCIS), USA, August, 2007


13 Beck, Timo; *User Perception of Targeted Ads in Online Social Networks*, University of St. Andrews, School of Management, Scotland, UK, 2010


16 Davis, Fred; *A Technology Acceptance Model for Empirically Testing New End-user Information Systems: Theory and Results*, Thesis (Ph.D.), Massachusetts Institute of Technology (MIT), Sloan School of Management, 1986


18 *Op cit*, Dwyer


20 Tokunga, Robert S.; “Friend Me or You’ll Strain Us: Understanding Negative Events that Occur Over Social Networking Sites,” *Cyberpsychology, Behavior and Social Networking*, vol. 14, issue 7–8, p. 425–432


22 *Op cit*, Dwyer

23 Beach, Aaron; Mike Gartrell; Richard Han; “Solutions to Security and Privacy Issues in Mobile Social Networking,” International Conference on Computational Science and Engineering, vol. 4, p. 1036–1042


25 *Op cit*, Pew Internet


27 Obfuscation means that the full web site information is shortened, so that it may not be apparent what the web site is by just looking at the text displayed.