Social Networks and Privacy—Threats and Protection

“Broadcast yourself!” YouTube’s slogan alone could summarize the spirit of the social revolution caused by the tidal wave of social networks. These have emerged as one of the main channels of communication on the web: links of all kinds are being forged, developed and broken almost instantly.

According to a study¹ published in France by the French Institute of Public Opinion (IFOP) on social networks, carried out using a sample of 1,002 people aged 18 years and over, 77 percent of Internet users say they are a member of at least one of the online social networks included in the study. These social networks’ notoriety is not simply the result of a mere fad. They allow their members to connect in a useful and enjoyable way by offering a variety of applications and benefits tailored to their target audience. LinkedIn has a huge employment market; for example, Jeff Epstein, chief financial officer of Oracle, was allegedly recruited thanks to his profile on this network.²

However, it would be unrealistic to think that the exponential growth of social networks has only positive effects. Indeed, publication and sharing of personal information exposes Internet users to all types of abuse and violation of their privacy. In 2009, a worker was fired for using Facebook during her sick leave from work due to migraines when using computers. Her boss said that if she could use Facebook, she was capable of working on a computer. This incident launched the issue of spying using Facebook.³

The aim of this article is twofold: to identify, based on the motivations of Internet users visiting social networks, the risk of violating users’ privacy, and to analyze and evaluate the effectiveness of the control methods used. MEG.ACTIVATION OF INTERNET USERS

A study published by Deloitte⁴ in April 2011 states that “continuous connection to the maximum number of friends is the main function for most people” connected to social networks. This statement does not mean that this function is unanimous among all users of social networking sites. Indeed, members of social networks are far from forming a uniform population. Depending on age and socio-professional background, there are several groups, each with different areas of interest. Figure 1 provides a brief overview of the major user groups and their motivations for using social networks.

<table>
<thead>
<tr>
<th>Group</th>
<th>Motivations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals</td>
<td>Interaction with family and friends, research, and professional opportunities</td>
</tr>
<tr>
<td>Employers and recruiters</td>
<td>Psychological and social profiling of applicants</td>
</tr>
<tr>
<td>Criminals</td>
<td>Spam, scams and sexual crimes</td>
</tr>
<tr>
<td>Police, army, secret services and government agencies</td>
<td>Staff profiling, criminal investigations and quick communication with the public, particularly via Twitter</td>
</tr>
<tr>
<td>Politicians and activists</td>
<td>Ideological propaganda, research and gauge of popularity</td>
</tr>
<tr>
<td>Businesses</td>
<td>Profiling and targeting potential markets, deepening customer relationships, online promotion and sales, and online surveys and studies</td>
</tr>
</tbody>
</table>

Figure 1 shows that the most vulnerable group is individuals, who make up the majority of social network users. In fact, the other groups freely make use of the information published by individuals for a variety of purposes.

So, what are the types of risk facing the hundreds of millions of people connected to Facebook, LinkedIn, Twitter and Myspace?
RISK
Each Internet user connected to social networks has a digital identity. It is made up of everything users publish on their various accounts and allows a sketch to be drawn of their personalities. “On each login, sending of e-mail and search on a search engine, there are private conversations, IP addresses and addresses of sites visited that are archived and possibly exploited for commercial purposes.”5

The financial or strategic stakes of access to this identity by various interest groups are obvious. As a result, there are many types of risk for social network users and the security of the information shared on social networks:

- **Identity theft**—Access to basic information constituting the identity of the Internet user (i.e., name, surname, date of birth, place of birth, photo) opens the door to the risk of identity theft. In France, for example, this risk has been recognized and has led to a change in legislation. Thus, a new section 226-4-1 of the Law of Orientation and Programming for the Performance of Internal Security (LOPPSI 2) was adopted by the French legislature on 8 February 2011.6

- **Pedophilia and sexual crimes**—Teenagers, who are more numerous and more active on social networks, are exposed to sexual predators. Predators have time to make contact with their victims, most of the time under a false identity, and locate them geographically. The risk is even greater as teenagers are less likely than adults to be careful on these networks. A survey carried out in 2006 in the US, as part of research conducted by Princeton University, found that of 935 teenagers:7
  - Four out of five teenagers put their first name in their profile.
  - Four out of five teenagers post their photo and two out of three teenagers post photos of their friends. When they are reminded of the public nature of the publication of photos, most of them say they are not concerned about the risk to their privacy. They think that the photos, even combined with the other information in the profile, do not give enough details to compromise their safety.
  - Six out of 10 teenagers put the name of the town where they live.
  - One half of teenagers post the name of their school.
  - Four out of 10 teenagers post their messaging nicknames (e.g., MSN address).
  - Three out of 10 teenagers include their surnames in their profiles.

  – One in 10 teenagers put their first name and surname in their public profile.
  – One in 20 teenagers include their full name, their photo, the name of their school and the name of their town in their public profile.
  – Two thirds of teenagers restrict access to their profile (e.g., by making it private, protecting it with a password, completely hiding it from the view of others)

The results of this survey show the vulnerability of younger people, and their obvious lack of information on the risk of pedophile attacks through social networks. It is also worth noting the risk of teenagers developing trauma or dependencies with regard to some pornographic and obscene content published on these sites.

- **Dismissal/disqualification/serious misconduct**—Some social networks, such as Viadeo or LinkedIn, allow their users to post their curriculum vitae (CV) and provide opportunities to find career prospects. In contrast, people’s publications on a general social network, such as Twitter or Facebook, can strike a blow to their career aspirations. An employer may find that obscene photos or foul language may undermine the image of the company, and dismiss the offending employee. In the US, 45 percent of employers search through social networks when they want to recruit.8

While the debate on the involvement of companies in controlling content published by their current (or potential) employees is quite complex, the risk for businesses is real. For example, hackers could use information left on a social network by the employees of a particular company to try to gain access to the information systems of the company; information such as date of birth or the first and last names of children may in fact enable hackers to figure out passwords. Even worse, clumsy system administrators could, for example, by asking their peers for help on a web site, post information on the configuration of the
operating system, which would be very beneficial to any hackers. Thus, there must always be a compromise made by employees between their behavior and the interests of the companies that employ them.

• Advertising harassment/spam—In 2011, Facebook achieved advertising revenues of US $4 billion, according to its chief operating officer, Sheryl Sandberg.9 Of course, companies display commercial advertisements on the site, but they also, and above all, use the private information that is published to better target their communication. This is also the case with Twitter, which, through its “sponsored tweet” concept, provides advertisers with detailed statistics on user profiles. This system allows them to find out more about potential customers and to obtain substantial revenue sources. Spam is a real nuisance, and the worst is that the operators of these sites are just as much victim to it as the public. For example, in mid-November 2011, Facebook was victim to a campaign of pornographic spam that appeared in users’ news feeds.10

There are yet further dangers associated with the protection of privacy on networks: phishing facilitated by information left on social networks, spying by government agencies and ideological manipulation (e.g., terrorism, racism). The risk is exacerbated by the business model of social networks, which is an obstacle to the development of a serious private information security policy.

BUSINESS MODEL AND PRIVACY POLICY

Business Model
The business model of social networks is based primarily on building huge databases of Internet users’ information on which companies and government agencies are willing to pay an awful lot of money. In this context, it goes without saying that respect for privacy is not the main concern of the operators of these sites.

They are constantly creating more applications that are a potential threat to protection of privacy, and sometimes installed by default on each profile. Such is the case with “Places,”11 a geolocation system, or “Timeline,”12 a kind of biography of users generated with all their publications on their Facebook profiles. These facts prompt us to look more closely at the conditions of use and privacy of social networks.

Terms of Use and Privacy of Social Networks

“The era of privacy is over.” This statement is not that of a hacker on the lookout for accounts to hijack, but that of Mark Zuckerberg, founder and chief executive of Facebook. And, although it provoked a public outcry, it does reflect what little importance social networks grant to user privacy.

Thus, although the Facebook conditions of use make a point of respecting and protecting the information of site members, a clause further specifies: “We do everything we can to make Facebook a safe service, but cannot guarantee its absolute security. To do this, we need your help, which includes the following obligations… .” A series of recommendations then follows.

In short, social networks’ conditions of use are in no way capable of guaranteeing the safety of Internet users and are purposely written in such a way that will discourage users from browsing them properly. Sites basically have no interest in users finding certain clauses that give them full control over all the information published. Thus, in 2009, Facebook was claiming lifetime ownership of all user information even after users unsubscribed from the site. The site was then forced to abandon this quietly introduced clause, faced with the veritable outcry provoked by this decision.

Due to the ambiguous behavior of operators of the sites, each consumer must be informed about current legislation and then act responsibly to protect themselves.

LEGISLATION
In February 2009, Alex Turk, president of France’s National Commission for Information Technology and Civil Liberties (CNIL), pointed the finger at a crucial issue. “The American companies that dominate the Internet do not feel bound by European regulations… .”13 In fact, it is virtually impossible at this time to establish binding global legislation on the regulation of social networks. As the majority of servers for these networks are located in the US, American law applies and, unfortunately, it is relatively deficient with regard to security of Internet users’ private information.

Failing a more effective means of pressuring network administrators, the European Commission has adopted two strategies for the moment:14

• Awareness, through advertising campaigns aimed particularly at minors
• Self-regulation, relying on voluntary action by social networks
However, it must be noted that in light of the facts mentioned previously, these networks are reluctant to assume social responsibility for obvious reasons of financial and strategic interests. This is evidenced by the recent reprimand of Facebook in the US by the Federal Trade Commission (FTC), concerning the violation of users’ privacy rights. The FTC’s criticisms are as follows: “The social network Facebook has accepted the criticisms of the FTC in the sense that it has disappointed users by telling them that they could protect the privacy of their personal information, and then on the other hand regularly sharing and making public this same information.” Of course Mark Zuckerberg says that he is working to ensure that these “mistakes” do not happen again. However, it is clear that, at the moment, users are extremely vulnerable to all sorts of abuse and to violation of their fundamental right to respect for their privacy, but that public authorities have no real means of enforcement.

This inability of governments to implement coercive global legislation led a coalition of experts in privacy protection in 40 countries to publish a statement in 2009. It requires governments to implement and enforce effective legislation on privacy.

HOW TO PROTECT YOURSELF?
Privacy protection on the Internet in general and on social networks in particular is becoming increasingly necessary. Vigilance continues to spearhead the security and, thus, the privacy of the information. It can be broken down into a few techniques that are simple but could make all the difference:

• **Choice of “friends” and contacts**—Users should be extremely careful in their choice of friends on these networks. It is common practice to accept contact from friends of friends, who are frequently complete strangers. This can lead to one’s private life being exposed to potentially harmful individuals.

• **Restricting private content to close friends and family only**—Social networking sites are increasingly allowing their users to configure restrictions on access to their information. It is, therefore, important to use these restrictions and to ensure that they are properly configured, given that our information is public by default.

• **Careful choice of information to be broadcast**—The key to the protection of privacy is in fact what information one broadcasts. Name, surname, date of birth, place of birth, photos, videos, comments and opinions should be carefully screened prior to being posted. Keep in mind that information posted on a network may one day be used against its author.

• **Awareness**—Every sector of the population should be made aware of the need to protect themselves against the risk that the use of social networks may entail. In the business world, this awareness must form part of the IT security program.

CONCLUSION
Social networks are a great way to express oneself and share with others. They help users lift the barriers of space and time and communicate with the whole world. However, there is another side associated with the proven dangers of user privacy violation. These dangers are even more of a threat now thanks to the increasingly widespread trend of registering on several sites using a single user account. In response to this situation, each Internet user must remain vigilant and governments must put more pressure on the operators of these sites in order to safeguard the security of Internet users.

ENDNOTES
1  Creative Commons, 2011, http://controverses.ensmp.fr/wordpress/promo10g20/importance-des-reseaux-sociaux/
5  Le Monde Newspaper, 28 May 2010, p.16
8 Balague, Christine; David Fayon; “Facebook, Twitter et les Autres...” (“Facebook, Twitter and the Rest”), Pearson Village Mondial Edition, 26 February 2010
Manjoo, Farhad; “De Plus en Plus Difficile de Mentir à ses Proches sur Facebook” (“Harder and Harder to Lie to Friends and Family on Facebook”), 4 October 2010, www.slate.fr/story/26401/mentir-facebook-places
11 Le Bourlout, Eric; “Comment Obtenir Timeline, le Nouveau Profil Facebook” (“How to Get Timeline, the New Facebook Profile”), 23 September 2011, www.01net.com/editorial/541884/comment-obtenir-timeline-le-nouveau-profil-facebook/