Social Networks and Privacy

by Maria Dailey & M. E. Kabay, PhD, CISSP-ISSMP
School of Business & Management
Norwich University, Northfield VT

Maria Dailey is a senior in the Bachelor of Science in Computer Security and Information Assurance (BSCSIA) in the School of Business at Norwich University. She recently submitted an interesting essay in the IS455 Strategic Applications of Information Technology< http://www.mekabay.com/courses/academic/norwich/is455/index.htm *> course, and I suggested to her that we work together to edit and expand it for publication. The following is the result of a close collaboration between us and continues last week's column about changing conceptions of privacy.*

* * *

Social Network Sites and Privacy

Harvey Jones and José Hiram Soltren published an interesting early study of privacy practices on Facebook in 2005.[1] They wrote in their abstract, "Privacy on Facebook is undermined by three principal factors: users disclose too much, Facebook does not take adequate steps to protect user privacy, and third parties are actively seeking out end-user information using Facebook." Key findings of the study (page 13) include the following (quoting, with bullets added):

- Users put real time and effort into their profiles.
- Students tend to join as soon as possible, often before arriving on campus.
- Users share lots of information but do not guard it.
- Users give imperfect explicit consent to the distribution and sharing of their information.
- Privacy concerns differ across genders.

For adolescents regularly using social networking sites (SNSs), reactions to their postings are emotionally significant. In a study of 881 teenagers in the Netherlands by Valkenburg, Peter and Schouten, the authors explored "…the consequences of friend networking sites (e.g., Friendster, MySpace) for adolescents' self-esteem and well-being." The young people spent an average of half an hour online every few days; the most important factor correlated with the participants' self-esteem was the tone of the comments on their postings. "Positive feedback enhanced adolescents' self-esteem, and negative feedback decreased their self-esteem. Most adolescents (78%) always or predominantly received positive feedback on their profiles. For these adolescents, the use of friend networking sites may be an effective vehicle for enhancing their self-esteem."[2]

On the other hand, sometimes users of SNSs may go too far in posting intimate details of their lives. Linda Roeder summarized some of the issues[3] to consider before posting information online in personal Web pages (or SNSs), including the following:

- How much identifying detail (full name, address, phone number…) should parents post about their children?
- How much intimate detail should users post about their inner thoughts and feelings?
- Should you avoid hyperlinks to your personal Web pages to prevent web-crawlers from indexing material you want to keep to a limited circle of friends?

The *Who's Watching* Website warns, "Sharing too much information on social networking sites can be problematic in two ways: first, it can reveal something about you that you'd rather your current or future employer or school administrator not know, and second, it can put your personal safety at risk."[4]

SNSs such as Facebook, Twitter, and MySpace all have privacy features that users can implement to protect their information against indiscriminate access. In the United States, these sites must meet requirements set by the Federal Trade Commission (FTC). However, SNSs have not always abided by regulations.

In December 2009, the Electronic Privacy Information Center (EPIC) and nine other privacy organizations filed a complaint with the FTC alleging privacy violations by Facebook. The introduction included this description:

> "This complaint concerns material changes to privacy settings made by Facebook, the largest social network service in the United States, which adversely impact users of the Facebook service. Facebook's changes to users' privacy settings disclose personal information to the public that was previously restricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available. These changes violate user expectations, diminish user privacy, and contradict Facebook's own representations. These business practices are Unfair and Deceptive Trade Practices…."[5]

FTC Commissioners found that Facebook misled members into believing that clicking on strict privacy settings in the "Central Privacy Page" and the "Profile Privacy Page" would allow them to close access to their information for everyone but "friends" or "friends of friends" if they so wished. However, wrote the Commissioners,

> "None of the pages described in Paragraphs 10-13 have disclosed that a user's choice to restrict profile information to 'Only Friends' or 'Friends of Friends' would be ineffective as to certain third parties. Despite this fact, in many instances, Facebook has made profile information that a user chose to restrict to 'Only Friends' or 'Friends of Friends' accessible to any Platform Applications that the user's Friends have used (hereinafter 'Friends' Apps'). Information shared with such Friends' Apps has included, among other things, a user's birthday, hometown, activities, interests, status updates, marital status, education (e.g., schools attended), and place of employment, photos, and videos."[6]

In addition, the Commissioner found that the privacy provisions against applications were misleadingly labelled (quoting directly):

> "However, in many instances, the links to 'Applications,' 'Apps,' or 'Applications and Websites' have failed to disclose that a user's choices made through Profile Privacy Settings have been ineffective against Friends' Apps. For example, the language alongside the Applications link, depicted in Paragraph 10, has stated, '[c]ontrol what information is available to applications you use on Facebook.' …. Thus, users who did not themselves use applications would have had no reason to click on this link, and would have concluded that their choices to restrict profile information through their Profile Privacy Settings were complete and effective."[6]

The proposed settlement [7] between the FTC and Facebook was summarized by the EPIC as follows:

> "Specifically, under the proposed settlement, Facebook is:
>
> - barred from making misrepresentations about the privacy or security of consumers' personal information;
> - required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;
> - required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;
> - required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers' information; and
> - required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected."[8]

Lessons

Users of Internet-mediated information-gathering services must remain on guard to prevent abuse of their privacy. Users should monitor changes in terms of service for Websites – including especially SNSs.

Corporate officers may be attracted to increasing revenue through deceptive practices; government and law enforcement officials may be interested in snooping illegally into the behaviour of individuals. Knowing that the public is keeping a watchful eye on their behaviour may serve to keep them honest.

Supporting tracking of privacy issues through organizations such as EPIC< https://npo.networkforgood.org/Donate/Donate.aspx?npoSubscriptionId=8252 > in the United

States and Privacy International< https://www.privacyinternational.org/article/about-donating-pi > in Britain and Europe can help maintain a culture of strong privacy.

References

[1] Jones and Soltren 2005
[2] Valkenburg, Peter and Schouten 2006
[3] Roeder 2011
[4] Who's Watching? 2011
[5] Rotenberg, et al. 2009
[6] Leibowitz, et al. 2011, p 6
[7] Beringer, et al. 2011
[8] EPIC 2011

Works Cited

Beringer, S. Ashlie, M. Sean Royall, Theodore W. Ullyot, Laura D. Berger, Cora Tung Han, and Manas Mohapatra. “In the Matter of Facebook, Inc.: Agreement Containing Consent Order.” Federal Trade Commission. 29 11 2011. http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf (accessed 12 23, 2011).

EPIC. “Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises.” Electronic Privacy Information Center. 29 11 2011. http://ftc.gov/opa/2011/11/privacysettlement.shtm (accessed 12 23, 2011).

Jones, Harvey, and Jose Hiram Soltren. Facebook: Threats to Privacy. 14 December 2005. http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf (accessed November 30 2011).

Leibowitz, Jon, J. Thomas Rosch, Edith Ramirez, and Julie Brill. “In the Matter of FACEBOOK, Inc.: FTC Ruling.” Federal Trade Commission. 29 11 2011. http://ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf (accessed 12 23, 2011).

Roeder, Linda. “How Much Information Is Too Much? Be Safe Online.” about.com Social Media. 2011. http://personalweb.about.com/cs/securityprivacy/a/311toomuchinfo.htm (accessed 12 31, 2011).

Rotenberg, Marc, John Verdi, Kimberly Nguyen, Jared Kaprove, Matthew Phillips, and Ginger McCall. “In the Matter of Facebook, Inc.: Complaint, Request for Investigation, Injunction, and Other Relief.” Electronic Privacy Information Center. 17 12 2009. http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf (accessed 12 23, 2011).

Valkenburg, Patti M., Jochen Peter, and Alexander P. Schouten. “Friend Networking Sites and Their Relationship to Adolescents' Well-Being and Social Self-Esteem.” *CyberPsychology & Behavior* 9, no. 5 (10 2006): 584-590. (Accessed 12 31 2011 through Norwich University Kreitzberg Library online databases.)

Who's Watching? “Too Much Information: On social networking sites, you may be giving away more than you think.” Who's Watching. 2011. http://whoswatchingcharlottesville.org/social.html (accessed 12 24, 2011).

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *