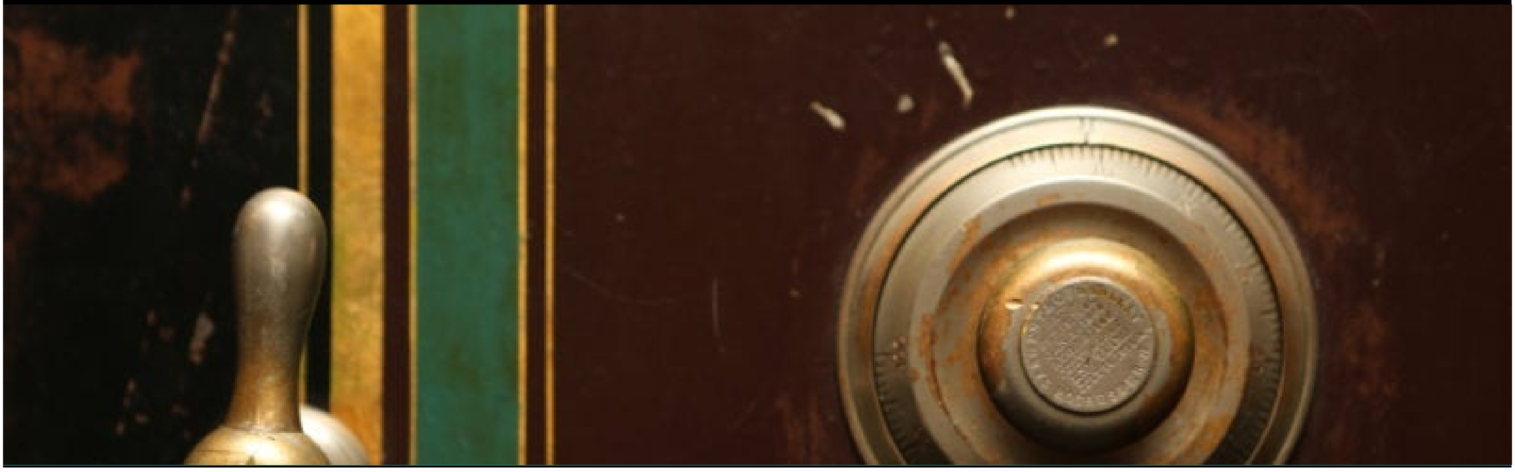
blink



By

Nika Smith

Social networking and content sharing web sites like Facebook and Flickr make it easy for users to connect and share details of their lives with others. Unfortunately, it is all too common to hear stories of users unknowingly sharing embarrassing status updates or photos with their professional colleagues, due to misunderstanding or ignoring available privacy settings in these sites.

Preventing usability issues with such popular web destinations is critical not just to minimize general frustration or inefficiency in use, but also to protect users' privacy.

There are a lot of professionals– lawyers, politicians, software developers and program managers to name a few – who "own" various aspects of online privacy in social applications. We believe that usability professionals are well suited to take a more active role to protect users and set standards for online privacy protection, addressing critical questions such as:

- What level of privacy should be set by default?
- How should users be notified about privacy settings and changes to them?
- When is it okay to share private information with others? How should this be supported?
- What tools are needed to allow users to control their private information and the audience who has access to it?

Why are usability professionals well-prepared to take on this role?

1. We are champions of developing and using reliable user research methods

When developing applications that allow users to manage, organize, or share private information, it is essential to understand users' expectations and needs for these applications. Willingness to share, for instance, may vary significantly from one application to another based on how the shared information will be used or who may have access to it.

Usability professionals are prepared to use our experience with user research methods to learn about unique needs and expectations and to make recommendations based on more than just a hunch. User research enables us to understand privacy implications before designing applications and lets us answer questions such as:

- What level of control and amount of privacy do users expect to have?
- What do users already do to maintain their privacy, both online and offline?
- What words do intended users use to describe privacy options?
- What do users NOT do to maintain their privacy?

Further, we are in a unique position to develop new research methods to address opportunities that aren't fully supported by our traditional toolkit. For example, there is a growing need to create privacy-specific sets of heuristics or guidelines (much like Jakob Nielsen and Rolf Molich's often-used Usability Heuristics) for efficiently evaluating potential privacy issues in existing interfaces.

2. One of our roles is to advocate for the user

Organizations that develop applications with privacy considerations are bound to have a number of people involved in the development process. For example:

- Project managers make business decisions about the intended goals of the application.
- Lawyers ensure that the privacy policies are comprehensive and that business decisions are safe.
- Software developers turn business decisions into a reality.

These professionals provide necessary areas of expertise to the table, but they may not have direct contact with the users they intend to serve. Based on the research and studies that we conduct as usability professionals, we provide an unbiased source of knowledge about users' needs and habits for all collaborators during product development. When developing a potentially privacy-invading application, a product team that employs the skills of a usability professional can access users' points of view and behavioral habits to:

- Verify that the type of content being shared is what users are actually interested in sharing.
- Identify the types of privacy settings and the level of control that users want or need to efficiently manage their content and audiences.
- Validate that users can effectively use privacy-controlling features and settings.

Further, usability practitioners are able to ensure that potentially privacy-invading applications literally speak the users' language. Our knowledge about users prepares us to check that terminology used in settings and instructions is consistent with users' own vocabulary. Further, we can advocate for usability improvements to necessary documents that are typically daunting for users to read, such as privacy policies.

3. We can protect users from harm, even when they do not notice a privacy risk

The Pew Internet & American Life Project has reported that 60% of Internet users are not worried about the information that is available about them online. Even more disconcerting, only a small subset of concerned users actively does something to protect their privacy. A few reasons may account for this lack of action:

- Many people assume the information out there is not that personal or that no one important will be able to find it.
- Users do not like to read lengthy privacy policies, instructions, or help documents that tell them exactly what aspects of their privacy are at risk.
- Users often do not know how to protect themselves and find the available privacy settings or protocols cumbersome or irrelevant to their needs.

It is not necessarily our job to convince users that their privacy is at risk, nor is it our job to train them to become privacy experts. It is our responsibility, however, to ensure that applications limit or prevent errors and minimize risk. There are many things we can do behind-the-scenes to help prevent users from accidentally putting their privacy at risk. For example:

- Ensure that the application uses reasonable default settings.
- Advocate for potential privacy-invading settings to be opt-in rather than opt-out.
- Refrain from offering any seriously harmful or destructive options.

Further, applying basic usability principles to the privacy domain will go a long way in subtly making users aware of their privacy risk and helping them make informed decisions without expertise or cognitive overload. Some examples:

- Use clear and consistent language around concepts relating to privacy, personal information, and sharing.
- Prominently display the status of privacy settings ("you are sharing your health information with the world") throughout the application.
- Give users complete control over the private data they previously shared by letting them undo, unshare, or revoke access from others.

Recommended reading:

- End-User Privacy in Human-Computer Interaction by Giovanni Iachello and Jason Hong
- Digital Footprints: Online Identity Management and Search in the Age of Transparency by Mary Madden, Susannah Fox, Aaron Smith, and Jessica Vitak
- 10 Privacy Settings Every Facebook User Should Know by Nick O'Neill