

Are You Looking At Me? - Social Media and Privacy Literacy

Dana Rotman

drotman@umd.edu

College of Information Studies

University of Maryland

College Park, MD 20742

ABSTRACT

Information privacy has received significant attention in past years. The shift from physical to online interaction entails a change in privacy paradigms. Yet, most of the attention has been directed at forms of self-identifying information (e.g. health records and financial information); less attention has been given to privacy concerns resulting from the information provided voluntarily by users during online social interaction. This paper suggests *privacy literacy* - an educational framework that will be used to enhance users' awareness to privacy issues that are intertwined in online exposure.

Categories and Subject Descriptors

K.3.2 Computer and Information Science
Education/Literacy

General Terms

Human Factors

Keywords

Social media, Online communities, Privacy literacy, Self-disclosure

1. INTRODUCTION

Social media are extremely popular, and draw large numbers of users. Online communities, social networks media-sharing sites and blogs are all based on the premise of information exchange, creating a sense of intimacy, based on the relative anonymity and lack of prior acquaintance with other users [1]. This intimacy causes people to open themselves up to a dialog with unfamiliar and undefined audience. The information shared in this dialog shapes the way a user's identity is created, recreated and refined [2, 3]. This information can be divided to 3 facets:

(1) **Self-identifying information** (e.g. health and financial records, SSN);

(2) **Access-enabling information** (passwords, location); and

(3) **Expressive information** (opinions, views and lifestyle choices)[4]. The fragmented pieces of information present facets of the online self, and may lead to an almost-complete portrayal of the user [5, 6]. The ability of users to consciously select which information to disclose and which will be kept private is the basis for their self-governance and autonomy [6]. Yet, in many online social media this autonomy is inadvertently mitigated during social interactions.

2. SOCIAL MEDIA AND PRIVACY CONCERNS

Many social media tools are supported by technology that enables the collection and retention of large bodies of information for indefinite periods of time. Websites employ repositories, archives and wikis, in which user-generated-content, including personal information, is collected and stored indefinitely, in a manner that enables search and retrieval or harvesting by commercial applications and private queries. The combination of an extreme sense of intimacy and mass data storage, with little or no user-control, is a valid reason for concern.

Table 1. Level of privacy concerns arising from different online social interactions

Media type	Identifying information	Access enabling information	Expressive information
Online communities	✓✓	✓	✓✓✓
Blogs / Vlogs	✓✓	✓	✓✓✓
Photos	✓	✓	✓✓✓
Social tagging	✓		
Social networking sites	✓✓✓	✓✓	✓✓
Video sharing	✓✓	✓	✓✓

However, prior studies [7-13] have shown that few users are aware of the fact that the social information they willingly provide can be stored indefinitely, or misused in a wide range of unwarranted activities, from identity theft [14] to online bullying [15].

Solutions to privacy concerns related to social media stem from several sources – policy, design and social settings [16]. We suggest *privacy literacy*: an educational framework that will complement the two other sources of privacy protection, and aid in creating proactive and aware users.

3. PRIVACY LITERACY

Privacy literacy may be viewed as a sub-category of digital literacy [17], or as a complementing literacy. Prior research stressed education as a literacy promoting tool [7, 18]. Thus, a privacy-literate user should be educated to distinguish between different facets of personal information; familiar with the settings in which he/she will readily relinquish personal information and those in which information should not be disclosed; understand the limitations of online anonymity; aware of the threats – immediate and prospective – that may stem from information disclosure, and take precautions against over-exposure.

A privacy literacy framework should include 5 elements that iteratively complement and enhance one another. These are:

1. *Understanding* - the different contexts of privacy in the personal information spectrum, and their place in online interaction: self-identifying information differs from access-enabling information, and this, in turn, differs from expressive information. Each has a different role in social interactions, and their interplay should be known and understood.

2. *Recognizing* – various online places in which personal information is shared. Most users are familiar with circumstances in which identifying information is disclosed. They are less familiar with the outcome of online social interactions, and readily reveal themselves visually and emotionally on different social media. Comprehending that almost every online social interaction entails a certain level of exposure will lead to greater awareness of the implications of such exposure.

3. *Realizing* - the implications of sharing private information in social circumstances. Even computer-savvy users can be confounded by the endless possibilities for privacy infringements that may occur during online social interaction - photos of a user partying during college can reach a potential employer; a personal message on an online community or a blog can be read by unwarranted audience. The realization of how far-reaching and how long-lasting social information is, should direct users when interacting online.

4. *Evaluating* – possible threats to privacy in a given interaction. This is possible when the user is knowledgeable enough and is able to assess the benefit and cost that he/she will incur from specific disclosure. It is also a matter of personal choice, based on the user's specific privacy and exposure preferences.

5. *Deciding* – the last element of privacy literacy is deciding consciously which information to share, in which circumstances. This is a proactive step, taken by the educated user, based on his/her knowledge and understanding of the range of privacy issues.

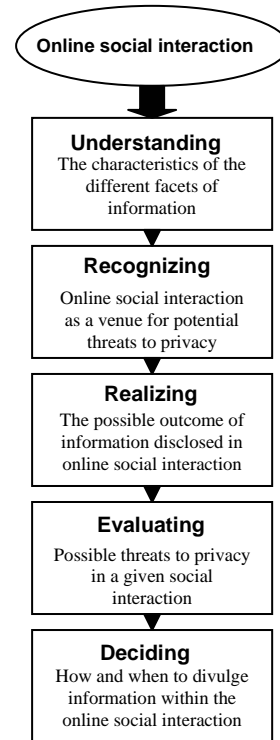


Figure 1. Privacy literacy framework.

4. CONCLUSIONS AND FUTURE RESEARCH

Protecting privacy, and especially social privacy, is not an easy feat. It is a delicate and continuous task. The variety of social media applications that are available today, and the heterogeneous nature of social media consumers, lessen the ability to suggest one solution to fit all.

Educating users to be privacy literate is not merely making them realize that online personal privacy encompasses much more than formal record protection; nor that information which is shared during social interaction may harm privacy. It is creating the essential understanding of what may become of this information online; the fact that loose boundaries exist as to the retention and use of the data, and the proactive choice of a desired level of privacy. Privacy literacy will have to be re-evaluated against users' perception of online information sharing, and refined with time and changes in online social interaction, especially where locative services are used. Behavior patterns that could not have been foreseen a decade ago, such as voluntary exposure of personal images and locative information, are now prevalent and necessitate different privacy literacy skills. Future research would address the issue of shifting privacy

literacy paradigms within social media, and especially mobile-social-media, as well as examine specific educational programs that will help make users privacy literate.

5. REFERENCES

- [1] Preece, J., Abras, C. and Maloney-Krichmar, D. 2004. Designing and evaluating online communities: research speaks to emerging practice. *International Journal of Web Based Communities*, 1(1), 2-18.
- [2] Donath, J. 1998. *Identity and deception in the virtual community*. Routledge, London.
- [3] Turkle, S. 1997. Multiple Subjectivity and Virtual Community at the End of the Freudian Century. *Sociological Inquiry*, 67, 1, 72-84.
- [4] DeCew, W. J. 1997. In *Pursuit of Privacy: Law, Ethics & the Rise of Technology*. Cornell University Press, Ithaca.
- [5] Burkhalter, B. 1999. *Reading Race Online: Discovering Racial Identity in Usenet Discussions*. Routledge, London.
- [6] Floridi, L. 2006. Four Challenges for a Theory of Informational Privacy. *Ethics and Information Technology*, 8, (3), 109-119.
- [7] Goldie, J. L. 2006. Virtual Communities and the Social Dimension of Privacy. *University of Ottawa Law & Technology Journal*, 3(1), 133-167.
- [8] Miyazaki, A. D. and Fernandez, A. 2001. Consumer Perceptions of Privacy and Security Risks for Online Shopping. *Journal of Consumer Affairs*, 35, 1, 27-44.
- [9] Dinev, T. and Hart, P. 2006. Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce*, 10(2), 7-29.
- [10] Qian, H. and Scott, C. R. Anonymity and self-disclosure on weblogs. *Journal of Computer-Mediated Communication*, 12, 4), 14.
- [11] Romanosky, S., Acquisti, A., Hong, J., Cranor, L. F. and Friedman, B. 2006. Privacy patterns for online interactions. In *Proceedings of the 2006 conference on Pattern languages of programs* Portland, Oregon, October 21 - 23, 2006). PLoP '06. ACM, New York, NY, 1-9.
- [12] Madden, M., Fox, S., Smith, A. and Vitak, J. 2007. *Digital Footprints - Online identity management and search in the age of transparency*. Pew Internet & American Life Project, Washington, DC.
- [13] Ahern, S., Eckles, D., Good, N. S., King, S., Naaman, M. and Nair, R. 2007. *Over-exposed?: privacy patterns and considerations in online and mobile photo sharing*. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (San Jose, California, USA, April 28 - May 03, 2007). CHI '07. ACM, New York, NY, 357-366.
- [14] Spiekermann, S., Grossklags, J. and Berendt, B. 2001. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM Conference on Electronic Commerce* (Tampa, Florida, USA, October 14 - 17, 2001). EC '01. ACM, New York, NY, 38-47.
- [15] Gross, R. and Acquisti, A. 2005. *Information revelation and privacy in online social networks*. In *Proceedings of the ACM Workshop on Privacy in the Electronic Society*, November 2005
- [16] Ackerman, M., Darrell, T. and Weitzner, D. J. 2001. Privacy in Context. *Human-Computer Interaction*, 16 (2), 167 - 176.
- [17] Gilster, P. 1997. *Digital Literacy*. John Wiley and Sons, New York, NY.
- [18] Sheehan, K. B. 2002. Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, 18 (1), 21 - 32.