Interdisciplinary Research Agenda on Privacy 2.0

Heng Xu
College of Information Sciences and Technology, Pennsylvania State University, University Park
hxu@ist.psu.edu

Sandra Petronio
Department of Communication Studies, Indiana University-Purdue University Indianapolis
petronio@iupui.edu

Xiaolong (Luke) Zhang
College of Information Sciences and Technology, Pennsylvania State University, University Park
lzhang@ist.psu.edu

Anna C. Squicciarini
College of Information Sciences and Technology, Pennsylvania State University, University Park
asquicciarini@ist.psu.edu

ABSTRACT

Online social networks (OSNs) brought the voluntary disclosure of personal information to the mainstream, rendering the potential intrusion of privacy a critical and acute concern. The main objective of this roundtable is to address the need for a paradigm shift in understanding and addressing users' privacy risks in the Web 2.0 environment with a focus on OSNs. The discussion themes are to: (1) deepen the theoretical understanding of privacy in the context of OSNs, (2) identify privacy intervention strategies for users to prevent privacy threats, and (3) promote privacy awareness.

Categories and Subject Descriptors

J.4 [Social and Behavioral Sciences]: Psychology; K.4.4 [Electronic Commerce]: Security; H.1.2 [User/Machine Systems]: Human factors.

General Terms

Algorithms, Management, Measurement, Security, and Human Factors.

Keywords

Privacy, Online Social Networks (OSNs), Privacy Enhancing Technologies (PETs), Privacy Regulations, and Privacy Awareness

DESCRIPTION

The extensive display of personally information by users of online social networks (OSNs) has made privacy concerns particularly salient. A larger volume of user digital footprints could be potentially accessible to the public [6]. OSNs brought the voluntary disclosure of personal data to the mainstream, thus exposing users' published information with potential abuse by online crooks, stalkers, bullies, and even by their own friends [3, 4]. At the same time, despite the presence of some privacy norms and regulations, there are relatively few well-established institutional rules and contracts governing OSNs, which gives rise to opportunism.

The main objective of this roundtable is to address the need for a paradigm shift in understanding and addressing users' privacy risks in the Web 2.0 environment with a focus on OSNs. This discussion panel aims to establish an interdisciplinary research on Privacy 2.0. The discussion themes are to: (1) deepen the theoretical understanding of privacy in the context of OSNs, (2) identify privacy intervention strategies for users to prevent privacy threats, and (3) promote privacy awareness. In reviewing the extant literature on privacy studies, the following controversial issues become apparent:

- Privacy has been researched for more than 100 years in various fields, e.g., law, economics, management, marketing, psychology, and philosophy. And yet, it is widely recognized that as a concept, privacy "is in disarray [and n]obody can articulate what it means" [8, p.477]. The picture of privacy that emerges is fragmented and usually discipline-specific, with concepts, definitions, and relationships that are inconsistent and neither fully developed nor empirically validated. Facing this challenge and the murky conceptual waters, this roundtable attempts to start an interdisciplinary discussion toward an understanding of information privacy in the context of OSNs.
- This roundtable will also highlight a debate in the privacy practice and research: the relative effectiveness of *technological solutions* versus *regulatory solutions* in ensuring consumer privacy [1, 2]. Skepticism about the effectiveness of privacy-enhancing technologies (PETs) and industry self-regulation in protecting privacy has resulted in privacy advocates and consumers clamoring for strong legislations to curtail rampant abuses of personal information. This roundtable seeks to address to this debate by: 1) discussing how users of OSNs can be protected from privacy threats, and 2) discussing the effects of different privacy intervention strategies on addressing privacy risks.
- Increasingly, many organizations invest considerable resources into the security and privacy awareness and training programs to raise user knowledge about safe computing practices. Unfortunately, despite the fact that considerable resources have been invested to design educational materials to teach users not to fall for security attacks, these materials are often ignored by users [5, 7]. Facing this challenge, this roundtable will discuss how to promote users' collective privacy awareness through facilitating collaborative privacy experiences among users and their peers.

In sum, a multidisciplinary approach will be expected to address above challenges highlighted in the current privacy literature. This roundtable discussion will be build upon ideas from discussion leaders in multiple fields such as information systems (Heng Xu), communication (Sandra Petronio), HCI (Xiaolong Zhang), and computer science (Anna Squicciarini) to explore the conceptual underpinnings of privacy in the context of OSNs, identify privacy intervention strategies, and promote user privacy awareness. During the roundtable, the team will establish the scope of the research, prepare a rough research agenda and plan for future research proposal submissions.

REFERENCES

1. Caudill, M.E., and Murphy, E.P. Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy & Marketing*, 19, 1 (2000), 7-19.

2. Culnan, M.J. Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing*, 19, 1 (2000), 20-26.

3. Gross, R., and Acquisti, A. Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, Alexandria, VA, 2005.

4. Kelly, S. Identity 'at risk' on Facebook. *BBC News*, 2008.

5. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J., and Nunge, E. Protecting people from phishing: the design and evaluation of an embedded training email system. *Proceedings of the Conference on Human Factors in Computing Systems*, San Jose, California, 2007.

6. Madden, M., Fox, S., Smith, A., and Vitak, J. Digital Footprints: Online identity management and search in the age of transparency. *PEW Internet & American Life Project*. 2007, http://pewresearch.org/pubs/663/digital-footprints.

7. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., and Nunge, E. Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. *Proceedings of the 2007 Symposium On Usable Privacy and Security*, Pittsburgh, PA 2007, pp. 88-99.

8. Solove, D.J. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154, 3 (2006), 477-560.