The Future of Networked Privacy: Challenges and Opportunities

Jessica Vitak  
College of Information Studies  
University of Maryland  
College Park, MD 20742  
jvitak@umd.edu

Pamela Wisniewski  
College of Info Sciences & Technology  
Pennsylvania State University  
State College, PA 16801  
pamwis@ist.psu.edu

Xinru Page  
School of Information and Computer Sciences, University of California  
Irvine, Irvine, CA, 92697  
xcpage@uci.edu

Airi Lampinen  
Mobile Life Centre, Stockholm  
University, Kista, Sweden  
airi.lampinen@iki.fi

Eden Litt  
Media, Technology, & Society  
Northwestern University  
Evanston, IL 60208  
eden.litt@u.northwestern.edu

Ralf De Wolf  
Media & Communication Studies, iMinds-SMIT-VUB  
Brussels, Belgium  
ralf.de.wolf@vub.ac.be

Patrick Gage Kelley  
Computer Science Department  
University of New Mexico  
Albuquerque, NM 87131  
pgk@unm.edu

Manya Sleeper  
School of Computer Science  
Carnegie Mellon University  
Pittsburgh, PA 15213  
msleeper@cmu.edu

Abstract
Building on recent work in privacy management and disclosure in networked spaces, this two-day workshop examines networked privacy challenges from a broader perspective by (1) identifying the most important issues researchers will need to address in the next decade and (2) working to create actionable solutions for these privacy issues. This workshop comes at a critical time for organizations, researchers, and consumers, as content-sharing applications soar in popularity and more privacy and security vulnerabilities emerge. Workshop participants and organizers will work together to develop a guiding framework for the community that highlights the future challenges and opportunities of networked privacy.

Keywords
Networked privacy; information disclosure; social media

ACM Classification Keywords
H.m. Information Systems: Miscellaneous.

Introduction
Research within the CSCW community has identified a fundamental gap between personal information management in everyday situations and its occurrence
via technologically mediated settings [1]. Networked systems do not provide the flexibility, nuance, or ambiguity inherent in normal social situations, instead requiring users to make intentional and complex disclosure decisions [1]. That said, users’ data—and subsequently, their privacy—is increasingly networked [6], requiring an “ongoing negotiation of contexts in a networked eco-system in which contexts regularly blur and collapse” (p.13) [25].

In the last decade, information and communication technologies (ICTs) have revolutionized how people interact with organizations, institutions, friends, and even strangers. Nearly 90% of Americans now use the Internet or email for personal or professional interactions [12]. Smartphone ownership is steadily increasing in the U.S. [12] and around the world [14]. Social media are thriving, with Facebook alone reporting 1 billion active users.

When considering questions of privacy management in a networked world, one must remember that every interaction made through these channels involves one or more parties disclosing information to known and/or unknown audiences. Many interactions are banal in nature; others involve highly sensitive information such as financial or health data. As ICTs have become more ubiquitous, research in both academia and industry has increasingly focused on the relationship between people’s privacy attitudes and behaviors [3, 7, 15, 30, 32, 41], new and adapted theories of privacy [26, 31], and user strategies to manage both their own disclosures and what others share [10, 17, 22, 28, 35].

It is important that those researching networked privacy take time to consider how systems, norms, and behaviors may evolve in the future. However, platforms are constantly emerging, restructuring, and disappearing. Users flock from one site to the next, interact across platforms, and may develop distinct or overlapping networks and identities based on their primary goals. The increasingly blurry distinction between public and private spheres further complicates privacy management, with platforms only now beginning to consider solutions to make privacy and disclosure easier to manage (e.g., [27]).

While difficult, it is extremely important for privacy researchers and practitioners to critically evaluate the potential challenges and opportunities presented by these new technologies. Thus, this workshop focuses on unpacking future directions for networked privacy research.

**Background**

The process of managing personal information becomes more complex in a networked world. Discrepancies in individuals’ media literacy, as well as their use of privacy tools, exist across age [21, 23], gender [21, 23, 34], network composition [35, 36], social norms [4, 26], and previous experiences [21, 23, 38].

Furthermore, the very structure of these technologies, which pushes public disclosure and interaction, makes it nearly impossible to recognize the full audience for a given piece of shared content. People typically imagine an audience when making a disclosure; however, discrepancies may exist between that imagined audience and those who view it [5, 20, 24]. Context collapse—the flattening of several distinct relational contexts into a homogeneous unit (e.g., “Friends,” “Followers,” “Connections”)—may lead to more proactive management of privacy features, self-
censorship or, particularly if skills or comprehension are lacking, posts later regretted [8, 24, 35, 37, 38].

Within the past year, numerous privacy challenges have surfaced as the public has expressed outrage upon learning of NSA’s surveillance, the Heartbleed security bug, and the manipulation of users’ experiences for research purposes (e.g., [2, 41]). The importance of finding practical solutions to these privacy challenges can be seen in mass media coverage [13, 17], White House policy [11], research initiatives [9], symposia [34], and a number of recent workshops in the CSCW and CHI communities [19, 20, 30, 43].

Building on this foundation, the current workshop looks to the future of networked privacy. It seeks to shed light on the various challenges individuals, groups, societies, and organizations will face when balancing online disclosure with a desire for privacy. We stand at a critical point in history, with new communication technologies rapidly spreading through both developed and developing nations. As people adopt these technologies, they often do so without significant thought to how their data are collected, stored, and transferred; furthermore, many people lack sufficient skills to successfully navigate these sites [22]. Researchers must consider future implications of these developments and address the challenges they create.

**Theme**

This workshop extends previous related workshops by identifying the major theories, methodological and design considerations, and policy implications researchers and practitioners will need to consider when engaging with users in networked spaces. At the same time that people are sharing more information through the Web and applications, managing privacy is becoming increasingly difficult. It is no surprise that privacy concerns related to personal information are steadily increasing. Therefore, it is essential to identify both the challenges and opportunities that ICTs will present consumers, researchers, and organizations in the coming years. By bringing together some of the leading privacy researchers in academia and industry, this workshop will look to the future and identify the most important challenges and opportunities in creating, maintaining, and enhancing networked privacy.

**Goals**

This workshop has four primary goals. The first goal is to connect academic and industry researchers studying privacy and HCI. This workshop can facilitate in-depth discussions regarding the current and future state of networked privacy. The second goal is to encourage collaborative work across disciplines and consider ways to bridge the gap between social science and computer science research in this area. A third goal of this workshop is to identify the most important topics and challenges related to networked privacy that should be addressed in the next 5-10 years. The final, long-term goal of this workshop is to share with the broader HCI community actionable solutions to identified privacy challenges.

**Call for Participation**

We are holding a two-day workshop for up to 25 participants from academia and industry. Participants will be recruited from the CSCW community, previous workshop attendees, and the extended research networks of the eight organizers, which span multiple continents. We especially encourage a balanced mix of
participants from academia, industry, and the public sector in order to provide participants with broader perspectives on the future challenges of privacy online.

Interested individuals should submit a 2-4 page position paper in CSCW extended abstracts format that addresses the workshop theme and highlighted topics provided in the call. We encourage submission of theoretical, methodological, design-focused, and empirically driven papers. Papers will be peer-reviewed by the workshop program committee (drawn from the existing privacy research community), and submissions will be accepted based on relevance and development of their chosen topic, as well as their potential to contribute to the workshop discussions and goals.

This workshop will focus on the future of networked privacy in a variety of subtopics. Topics of interest include, but are not limited to:

- **Theory**: What theories are most commonly used in privacy research? Which are most productive? How do we adapt privacy frameworks to the ever-changing socio-technical structure of ICTs?

- **Methodology**: What methods have been most useful or helpful while engaging in privacy research? Which methods should we be training privacy researchers in and employing in the future?

- **Design**: How can design account for evolving norms and values of users? How do we design technologies that meet user needs while ensuring the highest level of privacy protection? What design solutions can we import into existing technologies to reduce users’ privacy concerns?

- **Policy**: How, if at all, should individual privacy be regulated in the future? What are the biggest challenges to developing a comprehensive policy on protecting consumers’ personal information?

- **Privacy Perceptions**: How are privacy attitudes and norms evolving with changes in landscape and user base? How will these changes affect users’ ability to manage their networks?

- **Big Data**: What challenges will arise with big data collection as it becomes more common? How can big data analysis be conducted while protecting users’ privacy?

- **Ethics/Responsible Conduct of Research**: Should all research employing user data require an opt-in process? How can researchers conduct ethical studies without compromising the quality of data?

- **Mobile**: What privacy challenges will emerge as mobile becomes the dominant method globally for connecting to the Web? Can we ensure mobile communication is secure?

**Contributions**

This workshop contributes to the growing interest in networked privacy by considering, evaluating, and compiling key issues to be addressed in coming years. It has implications for theory and design, academia and industry. The workshop will share data and research through a public website and will contribute an article summarizing the outcomes of workshop discussions as well as develop a call for a special issue on the topic. With ICTs constantly evolving, it is essential that we look to the future, and this workshop provides privacy researchers with a foundation for future research.
Works Cited
[36] Vitak, J. and Ellison, N.B. 'There’s a network out there you might as well tap': Exploring the benefits of and barriers to exchanging informational and support-based resources on Facebook. New Media & Society 15 (2013), 243–259.