The Future of Networked Privacy: Challenges and Opportunities

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

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

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

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

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

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

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

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

CSCW '15 Companion, Mar 14-18 2015, Vancouver, BC, Canada
ACM 978-1-4503-2946-0/15/03.
http://dx.doi.org/10.1145/2685553.2685554

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

[1] Ackerman, M.S.The intellectual challenge of CSCW: the gap between social requirements and technical feasibility. *Human-Computer Interaction 15,* 2(2000), 179-203.

[2] Albergotti, R. Furor erupts over facebook's experiment on users. *The Wall Street Journal* (June 30, 2014). Retrieved August 1, 2014 from http://online.wsj.com/articles/furor-erupts-over-facebook-experiment-on-users-1404085840

[3] Acquisti, A. and Gross, R. Imagined communities: Awareness, information sharing, and privacy on Facebook. In *Proc. PET* (2006)*,* Robinson College, Cambridge, UK, 36–58.

[4] Barkhuus, L. The mismeasurement of privacy: Using contextual integrity to reconsider privacy in HCI. In *Proc CH*I (2012), ACM Press, 367-376.

[5] Bernstein, M.S., Bakshy, E., Burke, M. and Karrer, B. Quantifying the invisible audience in social networks. In *Proc. CHI* (2013), ACM Press, 21-30.

[6] boyd, d. Networked privacy. *Surveillance & Society 10*, 3 (2012), 348–350.

[7] Boyle, M. and Greenberg, S. The language of privacy: Learning from video media space analysis and design. *ACM Transactions on Computer-Human Interaction 12,* 5 (2005), 328-370.

[8] Das, S. and Kramer, A. Self-censorship on Facebook. *International Conference on Weblogs and Social Media*, *Proc. ICWSM*, AAAI Press (2013), 120-127.

[9] Data & Society. (2014). Available: http://www.datasociety.net/

[10] De Wolf, R., Willaert, K. and Pierson, J. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior 35* (2014), 444-454.

[11] Executive Office of the President. *Big data: Seizing opportunities, preserving values*. Washington DC: The White House (2014).

[12] Fox, S. and L. Rainie *The Web at 25 in the U.S*. Washington DC, Pew Internet Project (2014)..

[13] Gould, T.A. Can privacy survive social networking? *InformationWeek* (July 14, 2014). Retrieved August 3, 2014 from http://www.informationweek.com/software/social/can-privacy-survive-social-networking/a/d-id/1297267

[14] Heggestuen, J. One in every 5 people in the world own a smartphone, one in every 17 own a tablet (December 15, 20130. Retrieved August 4, 2014 from http://www.businessinsider.com/smartphone-and-tablet-penetration-2013-10

[15] Iachello, G. and J.I. Hong. End-User Privacy in Human-Computer Interaction. *Foundations and Trends in HCI 1*, 1 (2007, 1-137.

[16] Jayson, S. Social media research raises privacy and ethics issues. *USA TODAY* (March 12, 2014). Retrieved August 1, 2014 from http://www.usatoday.com/story/news/nation/2014/03/08/data-online-behavior-research/5781447/

[17] Lampinen, A., Lehtinen, V., Lehmuskallio, A. and Tamminen, S. We're in it together: Interpersonal management of disclosure in social network services. In *Proc. CHI*, ACM Press (2011), 3217–3226.

[18] Lampinen, A., Stutzman, F. and Bylund, M. Privacy for a networked world: Bridging theory and design [workshop]. In *Proc CHI* (2011), 2441-2444.

[19] Lipford, H. R., Wisniewski, P., Lampe, C., Kisselburgh, L. and Caine, K. Reconciling privacy with social media [workshop]. In *Proc CSCW,* ACM Press, 19-20.

[20] Litt, E. Knock, knock. Who's there? The imagined audience. *Journal of Broadcasting & Electronic Media*, *56*, 3 (2012), 330-345.

[21] Litt, E. Understanding social network site users' privacy tool use. *Computers in Human Behavior, 29* (2013), 1649-1656.

[22] Litt, E., E. Spottswood, Birnholtz, J., Hancock, J.T., Smith, M.E. and Reynolds, L.Awkward encounters of an "other" kind: collective self-presentation and face threat on Facebook. In *Proc CSCW,* ACM Press (2012), 449-460.

[23] Madden, M. *Privacy management on social media sites.* Washington DC: Pew Internet Project (2012).

[24] Marwick, A.E. and boyd, d. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society, 13* (2011), 114–133.

[25] Marwick, A.E. and boyd, d. Networked privacy: How teenagers negotiate context in social media. *New Media & Society* (in press).

[26] Nissenbaum H.F. *Privacy in Context: technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, CA, 2010.

[27] Oremus, W. Facebook's privacy dinosaur wants to make sure you're not oversharing. *Slate* (March 25, 2014. Retrieved June 20, 2014 from http://www.slate.com/blogs/future_tense/2014/03/25/facebook_privacy_dinosaur_privacy_checkups_take_aim_at_oversharing.html

[28] Page, X., Kobsa, A. and Knijnenburg, B.P. Don't disturb my circles! Boundary preservation is at the center of location-sharing concerns. In *Proc ICWSM*, AAAI (2012), 266-273.

[29] Page, X., Tang, K., Stutzman, F. and Lampinen, A. Measuring networked social privacy [workshop]. In *Proc CSCW,* ACM Press (2013), 315-320.

[30] Palen, L. and Dourish, P. Unpacking "privacy" for a networked world. In *Proc CHI,* ACM Press (2003), 129-136.

[31] Petronio, S. *Boundaries of Privacy.* State University of New York Press, Albany, NY, 2002.

[32] Stutzman, F., Gross, R. and Acquisti, A. Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality 4*, 2 (2012), 7-41.

[33] Symposium On Usable Privacy and Security (SOUPS). (2014). Retrieved August 1, 2014 from http://cups.cs.cmu.edu/soups/2014/

[34] Thelwall, M. Privacy and gender in the social web. In S. Trepte and L. Reinecke, eds., *Privacy Online: Perspectives On Privacy And Self-Disclosure In The Social Web*. Springer, Heidelberg and New York, 2011, 251–266.

[35] Vitak, J. The impact of context collapse and privacy on social network site disclosures." *Journal of Broadcasting and Electronic Media 56,* 4 (2012), 451-470.

[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.

[37] Vitak, J. and Kim, J. "You can't block people offline": Examining how Facebook's affordances shape users' disclosure process. In *Proc. CSCW,* ACM Press (2014), 461-474.

[38] Wang, Y., Norcie, G., Komanduri, S., Leon, P. G., Cranor, L. F. and Acquisti, A. (2011). "I regretted the minute I pressed share": A qualitative study of regrets on Facebook. In *Proc. SOUPS,* ACM Press, n.p.

[39] Wisniewski, P., Xu, H. Lipford, H.R. and Bello-Ogunu, E. Facebook Apps and tagging: The trade-off between personal privacy and engaging with friends. *Journal of the Association of Information Science and Technology* (in press).

[40] Wood, M. OKCupid Plays with love in user experiments. *The New York Times* (July 28, 2014). Retrieved July 30, 2014 from http://www.nytimes.com/2014/07/29/technology/okcupid-publishes-findings-of-user-experiments.html

[41] Xu, H., Dinev, T., Smith, J. and Hart, P. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems 12,* 12 (2011), 798-824.

[42] Xu, H., Zhang, X. and Reddy, M. Collaborative privacy practices in social media. In *Proc. CSCW*, ACM Press (2011), n.p.