In Whose Best Interest? Exploring the Real, Potential, and Imagined Ethical Concerns in Privacy-Focused Agenda

Pamela Wisniewski
University of Central Florida
Orlando, FL 32816 USA
pamwis@ucf.edu

Bart Knijnenburg
Clemson University
Clemson, SC 29634
bartk@clemson.edu

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

Yang Wang
Syracuse University
Syracuse, NY 13244
ywang@syr.edu

Xinru Page
Bentley University
Waltham, MA 02452
xpage@bentley.edu

Casey Fiesler
University of Colorado Boulder
Boulder, CO 80309
Casey.Fiesler@colorado.edu

CSCW '17 Companion, February 25 - March 01, 2017, Portland, OR, USA
ACM 978-1-4503-4688-7/17/02.
http://dx.doi.org/10.1145/3022198.3022660

Abstract
Through a series of ACM SIGCHI workshops, we have built a research community of individuals dedicated to networked privacy—from identifying the key challenges to designing privacy solutions and setting a privacy-focused agenda for the future. In this workshop, we take an intentional pause to unpack the potential ethical questions and concerns this agenda might raise. Rather than strictly focusing on privacy as a state that is always desired—where more privacy is viewed unequivocally as "better"—we consider situations where privacy may not be optimal for researchers, end users, or society. We discuss the current research landscape, including the recent updates to the ACM's Code of Ethics, and how researchers and designers can make more informed decisions regarding ethics, privacy, and other competing values in privacy-related research and designs. Our workshop includes group discussions, breakout activities, and a panel of experts with diverse insights discussing topics related to privacy and ethics.

Author Keywords
Ethics; privacy; security; information disclosure; research design; usability

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous

Important Dates:

- **Nov. 5, 2016:** Call for proposals
- **Dec. 14, 2016:** Position paper deadline
- **Jan. 10, 2017:** Notifications sent to authors
- **Jan. 31, 2017:** Camera-ready due and will be linked on website
- **Feb. 25, 2017:** Workshop

Expert Panelists:

- **Sara Kiesler,** *National Science Foundation*
- **Lorraine Kisselburgh,** *Purdue University*
- **Poul Petersen,** *BigML*
- **Elaine Raybourn,** *Sandia National Labs*
- **Jen Romano-Bergstrom,** *Facebook*

Introduction

Since Irwin Altman's research on privacy as control first appeared in the 1970s [3], a number of prominent scholars have examined privacy—both on- and offline—as *a boundary regulation* process—that is, the process of disclosing more/less information or being more/less accessible to others. As networked privacy researchers, we tend to emphasize how sharing too much can expose individuals to undesired audiences or outcomes, or leave users vulnerable to interactional or physical privacy harms. As such, we often assume that helping individuals be more private is to their direct benefit.

That said, being *too private* can also lead to negative outcomes, such as isolation and loneliness, or being unable to obtain needed social, informational, and tangible resources [8]. For instance, machine learning research shows how personal information can be leveraged to create powerful personalized experiences [1], and health IT studies have shown that patients often need others to be aware of personal health information in order to provide beneficial care in life-threatening situations [16]. On the political stage, there is a renewed focus on balancing an individual's right to privacy versus national security [7].

Consequently, privacy-focused research has been criticized for ignoring other values that may be equally or even more important [19]. As such, privacy might *not* always be in people's best interest or in the best interest of society. While this assertion may seem obvious, a large portion of the empirical, theoretical, and design-based research on networked privacy continues to focus solely on how to protect individuals from unwanted access and over-sharing. Given this emphasis on trying to increase privacy protection for end users – from designing better privacy defaults to raising privacy awareness to more algorithmic approaches that nudge users toward being more private – the primary goal of this workshop is to initiate a discussion on the real, potential, and imagined ethical concerns associated with such privacy-focused agendas. This workshop shifts the current discussion to more deeply evaluate how multiple competing values—and especially values around privacy and ethics—shape research and design processes. We will bring together researchers and practitioners from the broader CSCW and ACM community to develop heuristics to guide privacy and ethical decision-making in regard to both research design and designs for privacy protection.

Workshop Themes

This workshop merges two streams of research that have received increased attention within the social computing community: (1) ethical concerns around collecting and analyzing user data (e.g., "Big Data"), and (2) balancing privacy and disclosure in networked spaces.

In addressing both themes, the workshop will bring together two CSCW research communities to address common problems related to user research and networked privacy research and design.

Ethics and Privacy in User Research

Discussions of both research ethics and networked privacy have become increasingly common in the social computing research community, but the discussions around these two inter-related topics have often occurred separately. Though, a common ethical metric for collecting online data without consent is that the data is "public" and viewable to anyone [20], thereby

Past ACM SIGCHI Privacy/Ethics Workshops:

- **CHI 2011:** Privacy for a Networked World: Bridging Theory and Design
- **CSCW 2012:** Reconciling Privacy with Social Media
- **CSCW 2013:** Measuring Networked Social Privacy
- **CSCW 2015:** The Future of Networked Privacy: Challenges and Opportunities
- **CHI 2016:** Bridging the Gap Between Privacy by Design and Privacy in Practice
- **GROUP 2016:** Ethics and Obligations for Studying Digital Communities

protecting users through upholding their privacy – illustrating how research ethics and privacy can overlap. Yet, there are still concerns that this practice violates privacy expectations—particularly since social media users may not have an accurate idea of their audience [11], and information leaks can occur accidentally by the individual or by third parties [14].

Such nuanced relationships between ethics and privacy shows how the two research communities could benefit from a joint discussion of these types of issues. Characterizations of the ethical complexities introduced by Internet research focus on privacy, e.g., with respect to anonymity and confidentiality, or with expectations of privacy that might be violated by a lack of informed consent [10]. However, the traditional notion of participant anonymity as paramount is not always the ethical choice; different levels of identity disguise may be appropriate in some situations, or even the use of real names [6].

The question of whether *more privacy* is always better, therefore, applies not only to systems design but also to research design. This discussion should also not be limited to the academic community; for example, members of Facebook's public policy team published a law review article highlighting how the ethics review process must evolve in light of changing research methods [9]. They note, "a flexible process is key: The ever-changing nature of the questions and data involved in industry (and academic) research requires that any processes must be able to adapt efficiently to new internal challenges and external feedback so they can improve over time" (p. 444). These discussions highlight the contextual nature of expectations of privacy [15] that could impact our research practices.

Ethical Considerations for Privacy Research

The current tradition in privacy research for embedding ethics in privacy-sensitive designs is to either give users ample transparency/control or to apply privacy nudges in order to help users make better privacy choices. While the intention is to protect users, a key assumption is that transparency and control are always beneficial to users, and that when nudges are applied, designers know which way is the "best" way to nudge users toward particular actions. Yet, promoting transparency and control are problematic in that they assume that users are able and willing to take control over their privacy.

Given the complexity of the digital privacy landscape, this is often an unrealistic assumption [13]. Additionally, while privacy nudges have been shown to help people make privacy decisions (e.g., [21]), a key limitation of nudging is that it is unclear what "beneficial behavior" entails: should we nudge users to always protect their privacy at all costs, or is there a subtler trade-off to be made? Scholars have warned that nudging can be subject to abuse or shift the responsibility of decision making from the people themselves to relying on nudges. As a result, people can become less capable of making their own decisions [5].

The positive and negative potential of these types of privacy-focused solutions raise important ethical questions. For instance, why are designers in a better position to know what is good for the users, more so than users themselves? The integral ethical dilemma with well-intentioned, privacy-sensitive designs is that privacy is a highly normative construct [2], and social norms around privacy vary drastically from individual to individual, as well as change over time and context

CSCW 2017 Workshop Activities:

- **Welcome and Introductions:** Lightning talk presentations
- **Large-group Discussion:** Ethical issues related to networked privacy
- **Coffee Break**
- **Panel Discussion:** Privacy, social computing, and ethics experts from both academia and industry.
- **Lunch**
- **Break-out Activities:** Balancing privacy with other values (e.g., Apple vs. FBI legal case).
- **Report/Synthesize:** Summarizing break out session outcomes
- **Next Steps:** Workshop participants draft a future roadmap on balancing ethics and privacy values in research and design.

[15]. Thus, designing privacy features to optimally meet the needs of a varied user population is tricky at best, and some design patterns have been deemed outright unethical, at their worst [4].

Some more recent research has focused on applying more user-centered principles to privacy research and design, such as helping users achieve a level of privacy *relative to* their own desires [22], as opposed to trying to sway them one way or another, and a number of researchers have attempted more intelligent privacy designs to meet diverse privacy needs [12, 18]. For instance, some research has worked to profile users' privacy behaviors and information disclosure decisions in order to inform the best approach for educating and nudging users in a way that is consistent with their own desires [23]. Such adaptive approaches circumvent the "direction problem" in nudging research by following users' own desires [18]. Yet, the ethical considerations of such approaches have yet to be unpacked, which motivate this workshop.

Workshop Goals

The main goal of this workshop is to bring together researchers currently studying questions around ethics and privacy in research and design to identify the most pressing questions and concerns. By the end of the workshop, the organizers and participants should have developed a set of heuristics on ethical privacy by design work, e.g., a more nuanced framework to help researchers make decisions around data (collecting, analyzing, storing, deleting). This work could also help move towards ethical norm setting, which is a goal articulated by the SIGCHI Ethics Committee. Beyond this goal, we want to use this workshop to encourage collaborative work across disciplines and consider ways to bridge the gap between social science and computer science research, as we strongly believe that the challenges around privacy work require buy-in from all stakeholders. Finally, we hope to share actionable solutions resulting from our workshop discussions with the broader HCI community through the networkedprivacy.com website, as well as other informal and formal channels.

Call for Participation

We will hold a one-day workshop for about 25 participants from industry, academia, and the non-profit/policy sector. Participants will be recruited from the CSCW community, previous workshop attendees, and the extended research networks of the six organizers, which span multiple continents as well as academia and industry. We will invite and encourage participants from academia and industry 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 the CSCW extended abstracts format that addresses the workshop themes and highlighted topics provided in the call. Papers will be peer-reviewed by the workshop program committee (drawn from the existing privacy research community; see sidebar for PC members), and submissions will be accepted based on the relevance and development of their chosen topic, as well as their potential to contribute to the workshop discussions and goals. Topics of interest include, but are not limited to:

- Ethical considerations of privacy (e.g., is privacy inherently good?)
- Trade-offs between privacy and beneficial outcomes (e.g., social support)

Program Committee:

- **Norah Abokhodair**, University of Washington
- **Seda Gürses**, Princeton University
- **Roberto Hoyle**, Indiana University
- **Luke Hutton**, The Open University
- **Patrick Kelley**, University of New Mexico
- **Lorraine Kisselburgh**, Purdue University
- **Kevin Koidl**, Trinity College
- **Hanna Krasnova**, University of Bern
- **Priya Kumar**, University of Maryland
- **Airi Lampinen**, Mobile Life Centre, Stockholm
- **Heather R. Lipford**, UNC Charlotte
- **Chris Norval**, University of St. Andrews
- **Sameer Patil**, Indiana University
- **Nicholas Proferes**, University of Maryland
- **Elaine Raybourn**, Sandia National Labs
- **Vance Ricks**, Guilford College
- **Jessica Staddon**, NC State
- **Luke Stark**, Dartmouth College
- **Jose Such**, Kings College London
- **Eran Toch**, Tel Aviv University
- **Michael Zimmer**, University of Wisconsin-Milwaukee

- Balancing privacy and security concerns
- Ethics of default settings: Are there "right" privacy defaults? Who decides?
- Awareness, transparency, and consent: Is more always better?
- Ethical questions for privacy nudging research
- Algorithmic authority and the subjective nature of algorithms as it pertains to privacy
- Empirical studies of social norms regarding privacy and their effects
- Methodological considerations around ethics in research/study design

About the Organizers

Pamela Wisniewski is an assistant professor in the Department of Computer Science at the University of Central Florida and the director of the Sociotechnical Interaction Research (STIR) Lab. Her research lies at the intersection of social computing and privacy.

Jessica Vitak is an assistant professor in the College of Information Studies at the University of Maryland and Associate Director of the Human-Computer Interaction Lab (HCIL). Her research evaluates issues around networked privacy as well as questions of ethics in social computing research.

Xinru Page is an assistant professor in the Department of Computer Information Systems at Bentley University. Her research focuses on social media adoption and non-use, networked privacy, and the role of individual differences in mediated communications.

Bart Knijnenburg is an assistant professor in the School of Computing at Clemson University and co-director of the Humans And Technology (HAT) Lab. His research focuses on privacy decision-making, user-tailored privacy, and the user-centric aspects of recommender systems.

Yang Wang is an assistant professor in the School of Information Studies at Syracuse University and co-director of the Social Computing Systems (SALT) Lab. His research focuses on inclusive privacy, which aims to design effective privacy mechanisms for people with disabilities and other underserved populations.

Casey Fiesler is an assistant professor in the Department of Information Science at the University of Colorado Boulder. Her research is at the intersection of law, ethics, and social norms in online communities, as well as research practices around them.

References

1. Elizabeth Aguirre, Anne L. Roggeveen, Dhruv Grewal, and Martin Wetzels. 2016. The personalization-privacy paradox: implications for new media. *Journal of Consumer Marketing* 33, 2: 98–110.
2. Anita L. Allen. 2012. Privacy Law: Positive Theory and Normative Practice. *Harvard Law Review Forum* 126: 241.
3. Irwin Altman. 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. Retrieved October 18, 2016 from http://eric.ed.gov/?id=ED131515
4. Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proc. on PETS* 2016, 4.
5. Luc Bovens. 2009. The Ethics of Nudge. In *Preference Change*, Till Grüne-Yanoff and Sven Ove Hansson (eds.). Springer Netherlands, 207–219.

6. Amy Bruckman, Kurt Luther, and Casey Fiesler. 2015. When Should We Use Real Names in Published Accounts of Internet Research? In *Digital Research Confidential: The Secrets of Studying Behavior Online*, Eszter Hargittai and Christian Sandvig (eds.). MIT Press, 449–468.
7. Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire. 2014. *The NSA Report: Liberty and Security in a Changing World*. Princeton University Press.
8. Nicole B. Ellison and Jessica Vitak. 2015. Social network site affordances and their relationship to social capital processes. In *The Handbook of the Psychology of Communication Technology*, S. Shyam Sundar (ed.). John Wiley & Sons.
9. Molly Jackman and Lauri Kanerva. 2015. Evolving the IRB: Building Robust Review for Industry Research. *Washington and Lee Law Review Online* 72: 445.
10. Heidi E. Keller and Sandra Lee. 2003. Ethical Issues Surrounding Human Participants Research Using the Internet. *Ethics & Behavior* 13, 3: 211–219.
11. Eden Litt. 2012. Knock, Knock. Who's There? The Imagined Audience. *Journal of Broadcasting & Electronic Media* 56, 3: 330–345.
12. Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Zhang, Norman Sadeh, Alessandro Acquisti, and Yuvraj Agarwal. 2016. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In *SOUPS*, 27–41.
13. Michelle Madejski, Maritza Johnson, and Steven M. Bellovin. 2012. A study of privacy settings errors in an online social network. In *2012 IEEE PERCOM Workshop*, 340–345.
14. Huina Mao, Xin Shuai, and Apu Kapadia. 2011. Loose Tweets: An Analysis of Privacy Leaks on Twitter. In *Proc. of the 10th ACM WPES*, 1–12.
15. Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79: 119.
16. Aarathi Prasad. 2012. Exposing Privacy Concerns in mHealth Data Sharing. Retrieved October 18, 2016 from http://www.cs.dartmouth.edu/reports/TR2012-711.pdf
17. Ramprasad Ravichandran, Michael Benisch, Patrick Gage Kelley, and Norman M. Sadeh. 2009. Capturing Social Networking Privacy Preferences: In *Privacy Enhancing Technologies*, Ian Goldberg and Mikhail J. Atallah (eds.). Springer Berlin Heidelberg, 1–18.
18. N. Craig Smith, Daniel G. Goldstein, and Eric J. Johnson. 2013. Choice Without Awareness: Ethical and Policy Implications of Defaults. *Journal of Public Policy & Marketing* 32, 2: 159–172.
19. Sarah Spiekermann. 2012. The Challenges of Privacy by Design. *Commun. ACM* 55, 7: 38–40.
20. Jessica Vitak, Katie Shilton, and Zahra Ashktorab. 2016. Beyond the Belmont Principles: Ethical Challenges, Practices, and Beliefs in the Online Data Research Community. In *Proceedings of the 19th ACM CSCW*, 941–953.
21. Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A Field Trial of Privacy Nudges for Facebook. In *Proceedings of the 32nd Annual ACM CHI*, 2367–2376.
22. Pamela Wisniewski, A.K.M. Najmul Islam, Bart P. Knijnenburg, and Sameer Patil. 2015. Give Social Network Users the Privacy They Want. In *Proceedings of the 18th ACM CSCW*, 1427–1441.
23. Pamela Wisniewski, Bart P. Knijnenburg, and Heather Richter Lipford. 2017. Making Privacy Personal: Profiling Social Network Users to Inform Privacy Education and Nudging. *Intl. Journal of Human-Computer Studies* 98, 2017: 95-108.