Privacy in Context: Critically Engaging with Theory to Guide Privacy Research and Design

Karla Badillo-Urquiola
University of Central Florida
Orlando, FL, USA
Kcurquiola10@knights.ucf.edu

Yaxing Yao
Syracuse University
Syracuse, NY, USA
yyao08@syr.edu

Oshrat Ayalon
Tel Aviv University
Tel Aviv, Israel
oshratra@post.tau.ac.il

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

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

Eran Toch
Tel Aviv University
Tel Aviv, Israel
erant@post.tau.ac.il

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

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

CSCW '18 Companion, November 3–7, 2018, Jersey City, NJ, USA
© 2018 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-6018-0/18/11.
https://doi.org/10.1145/3272973.3273012

Abstract

Privacy has been a key research theme in the CSCW and HCI communities, but the term is often used in an ad hoc and fragmented way. This is likely due to the fact that privacy is a complex and multi-faceted concept. This one-day workshop will facilitate discourse around key privacy theories and frameworks that can inform privacy research with the goal of producing guidelines for privacy researchers on how and when to incorporate which theories into various aspects of their empirical privacy research. This will lay the groundwork to move the privacy field forward.

Author Keywords

Privacy, Theory, Frameworks, Contextual Integrity.

Introduction

The networked privacy research community [4,11,13,24,26,28] is growing quickly as the discourse about and around privacy is becoming increasingly prominent in academia and in the public. One consensus among this research community is that the term "privacy" is complex, misunderstood, and often misused in empirical HCI research [6]. One way to solve the problem of the often fragmented and erratic use of the term privacy in HCI is for our community to converge on a subset of core privacy theories and

Keynote by Helen Nissenbaum:

- Helen Nissenbaum is a Professor of Information Science, Cornell Tech. Her research focuses on ethical and political dimensions of digital technologies including issues surrounding privacy, accountability, bias in computer systems, security, and values in design. She received the 2014 Barwise Prize of the American Philosophical Association and has earned grants from the US National Science Foundation and Defense Advanced Research Projects Agency.

frameworks that can meaningfully inform our scholarly work and provide a common foundation in which to move our field forward. This is the primary goal for our one-day CSCW "Privacy in Context" workshop.

There are a wide range of privacy theories and frameworks that approach privacy in different ways. Some classify information type by sensitivity [1,18], others focus on privacy as awareness and control of information [14], and still others approach it from a state-based perspective where there are different privacy states (e.g., anonymity, intimacy) [22]. More recently, norm-based approaches have been used to frame privacy as appropriate information sharing [6] such as Nissenbaum's (keynote speaker; see side bar) framework of Contextual Integrity (CI) [15]. Such work shows the value of integrating privacy theories and frameworks into empirically driven privacy research.

However, how to use these privacy theories to inform empirical research is an open question. For instance, Badillo-Urquiola et al.'s [5] initial review of the recent HCI literature that invoked CI as a privacy framework found that most of these studies did not deeply engage with CI beyond mentioning it in the background or discussion sections either to motivate or explain their findings. Few studies used CI to inform the design of their study, system, or even their codebooks, when CI was presented as a theoretical lens for qualitative work.

The gap between theory and empirical HCI research on privacy motivates our **workshop themes**:

1) *What privacy theories and frameworks have or could more meaningfully inform empirical HCI and social computing research?*

2) *How can we ensure that we are critically engaging with these theories and frameworks in a way that improves the quality of our scholarship?*

3) *How can we use these theories and frameworks to inform the design of collaborative technologies?*

The first theme will focus on facilitating discourse around relevant privacy theories and frameworks that are available to inform networked privacy research, while the second and third themes emphasize best practices for integrative methods that leverage and build upon these theories. Therefore, the outcomes of this workshop will include: 1) a descriptive taxonomy of theoretical frameworks that can be used in networked privacy research, and 2) a set of prescriptive heuristics for how to methodologically incorporate these theories into different aspects of empirical privacy research, including the design of collaborative systems.

Privacy Theories and Frameworks

In this section, we provide an overview of some of the most commonly referenced privacy frameworks in the HCI networked privacy literature. A number of studies frame privacy as a form **of interpersonal boundary regulation** [10,20,29], where individuals or groups must negotiate appropriate boundaries with others. This work often references the work of social psychologist Irwin Altman, who defined privacy as, "an interpersonal boundary process by which a person or group regulates interaction with others," by altering the degree of openness of the self to others [3]. According to Altman, boundary mechanisms are behaviors employed in combination and adjusted over time to achieve one's desired level of privacy. Individuals have different mechanisms for erecting boundaries, and they adjust these mechanisms as their needs change.

Wisniewski et al. [30] built upon Altman's theory to empirically show how different users have different privacy management profiles on Facebook, which are related to their awareness of the privacy settings and features available to manage one's privacy desires.

Building on Altman's conceptualization of privacy, Petronio's **Communication Privacy Management Theory** (CPM) [21] outlined five suppositions related to disclosure boundaries and delineated between two different interpersonal boundaries: personal and collective. Personal boundaries deal with how one shares private information about one's self, while collective boundaries involve private information shared with others. A number of researchers have extended Petronio's CPM theory by trying to design interfaces and create models to help users understand and alleviate collective privacy concerns [8,9]. For example, Jia and Xu developed the SNS collective privacy concerns (SNSCPC) scale to measure an individual's collective privacy concerns across three dimensions: collective information control, access, and diffusion [9].

Prior literature also highlights that people sometimes undergo a cost-benefit analysis when they make privacy decisions. For instance, they consider and make a tradeoff between the cost and gain of disclosing their personal information, a phenomenon known as "**privacy calculus**" [12]. There are various types of activities that can pose threats to one's privacy. Solove proposed a **taxonomy of privacy threats** which includes four categories of "socially recognized privacy violations:" information collection, information processing, information dissemination, and invasions [23]. In practice, people are likely to differ in terms of what kinds of privacy benefits and violations that they consider important for themselves. For instance, Page et al. found that collecting one's location data might unsettle some people but not others [19].

Studies that try to predict information disclosure or technology usage have produced mixed results, often showing behavior that does not reflect people's stated concerns [2,7,25]. This mismatch between stated concerns and actual behavior has been defined as a "**privacy paradox**" [7,17]. This research suggests that users may not always weigh costs and benefits in what researchers might consider a rational way. Therefore, a number of researchers have started to move towards more nuanced approaches for conceptualizing and measuring privacy that focus on context and norms [6].

The privacy framework at the forefront of this research is Nissenbaum's **Contextual Integrity** (CI), which is based on two principles: 1) individuals interact within a "plurality of realms" (or contexts), and 2) each context has its own norms. Therefore, privacy is a negotiation, reliant on norms and assumptions, between two or more individuals [15]. The CI framework provides researchers with a systematic approach, by means of heuristics, for designing technologies that take into consideration privacy. Three of the key dimensions of CI include: 1) contexts (e.g., social contexts), 2) contextual informational norms (privacy norms), and 3) contextual ends, purposes, and values (what embodies the context) [16]. Empirical research has shown that people's contextual privacy concerns align well with CI theory. Wang et al.'s study on drone bystanders' privacy shows that people's privacy concerns about drone usage are highly dependent on context and purpose (e.g., using a drone in a friend's party for personal recording use causes less concerns) [27]. In

Program Committee:

- **Louise Barkhuus**, University of Copenhagen
- **Marshini Chetty**, Princeton University
- **Shion Guha**, Marquette University
- **Roberto Hoyle**, Oberlin College
- **Jen King**, Stanford Law School
- **Lorraine Kisselburgh**, Purdue University
- **Priya Kumar**, University of Maryland
- **Airi Lampinen**, Stockholm University
- **Yifang Li**, Clemson University
- **Heather Lipford**, UNC Charlotte
- **Florian Schaub**, University of Michigan
- **Irina Shklovski**, University of Copenhagen
- **Luke Stark**, Microsoft Research Montreal
- **Janice Tsai**, Mozilla
- **Jessica Vitak**, University of Maryland
- **Michael Zimmer**, University of Wisconsin-Milwaukee

another example, Ayalon and Toch concluded that users were less willing to share older content on online social networks as a result of norm changes [4]**.**

Since privacy is a complex, multi-faceted concept, it is unlikely that a single theory can provide the theoretical foundation for privacy research. Yet, a comprehensive understanding of the main privacy theories can lead to better connections between research and design works. By consolidating this knowledge and providing guidelines on how to apply these theories, we will be able to help researches decide which theories to use when conducting empirical social computing research.

Participants

We propose a one-day workshop with 30 to 40 participants from academia and industry. Participants will be recruited from the CSCW community, previous privacy workshop attendees, the extended research networks of the workshop organizers, and privacy researchers in multiple disciplines. We will also recruit participants from industry who are concerned about privacy issues and are interested in improving the implementation of privacy theories in empirical research and systems design. This will allow us to understand a broad range of privacy perspectives as well as make for a suitable pool of collaborators with which to engage during the workshop and beyond.

Call for Participation

We will solicit a 2-4 page position paper (SigCHI extended abstract format), describing the participant's experience and research related to privacy theories in HCI. At least 2 members from our program committee (see side bar) will peer-review each position paper and evaluate participants based on their potential to contribute to the workshop goals.

Workshop Activities

We plan the following activities for the workshop:

- **Welcome/Introduction**: Lightning talk presentations of position papers.
- **Keynote Speaker:** To inspire participants and spark discussion, we will have Dr. Helen Nissenbaum, Professor of Information Science at Cornell Tech, engage with the audience about her renowned Contextual Integrity framework. Helen will discuss applications of the CI framework. There will also be a Q&A with the workshop participants.
- **Coffee Break**
- **Large-group Discussion:** Identify relevant privacy theories or frameworks and discuss their strengths and limitations. Brainstorm key areas of needs and goals in the current research landscape.
- **Lunch**
- **Break-out Activity:** Individuals will form small groups based on different privacy theories or frameworks. Each group will discuss the contexts in which these frameworks can be applied and brainstorm on how to best engage with the theory.
- **Coffee Break**
- **Report/Synthesize:** Present results to the full group, with time for full group discussion.
- **Next Steps:** Draft a roadmap on how to engage theories in future privacy research.

Equipment and Supplies

Workshop organizers will provide laptops for running individual presentation slides and for group note taking during large group discussion. We will also create our own website for advertising the workshop and

Timeline:

- **August 31, 2018**: Position Papers Due (Late submissions will be accepted through September 24th, 2018)
- **September 9, 2018**: Notification of Acceptance
- **September 28th**: Camera-ready Papers Due
- **November 3, 2018**: Workshop

managing submissions. We will need one projector to project the slides and notes. We will also need large paper pads and markers for small group breakout sessions, brainstorming, and presentations.

Contributions

The workshop will draw upon participants' knowledge and understanding of privacy theories and frameworks. This workshop brings together privacy researchers across disciplines to develop a descriptive taxonomy of theoretical frameworks that can be used in networked privacy research and set of prescriptive heuristics for how to methodologically incorporate these theories into different aspects of empirical HCI privacy research.

Workshop Organizers

Karla Badillo-Urquiola is a McKnight Doctoral Fellow pursuing her Ph.D. in Modeling and Simulation at the University of Central Florida. She plans to leverage her interdisciplinary background to develop better training and intervention strategies for the online safety of teens, especially those who are underrepresented.

Yaxing Yao is a fourth year Ph.D. student in the School of Information Studies at Syracuse University. His research interests are privacy online and in the Internet of Things. His dissertation work focuses on designing privacy-enhancing mechanisms for smart home users considering the different power dynamics (e.g., contexts, relationships) inside the home.

Oshrat Ayalon is a Ph.D. student in Engineering at Tel-Aviv University. Her research focuses on usable privacy, in areas such as online social networks and privacy engineering. Her dissertation work aims to facilitate decisions makers with tools for helping them design privacy-respectful information systems.

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.

Xinru Page is an Assistant Professor of Computer Information Systems at Bentley University. Her research explores technology adoption and non-use, social media, individual differences, and privacy.

Eran Toch is an Assistant Professor in the Department of Industrial Engineering, The Iby and Aladar Fleischman Faculty of Engineering at Tel Aviv University. His research focuses on usable privacy and security, human-computer interaction and data mining.

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 current research focuses on inclusive privacy, which aims to design effective privacy mechanisms for under-served populations: http://inclusiveprivacy.org/

Pamela Wisniewski is an Assistant Professor in the College of Engineering and Computer Science at the University of Central Florida and director of the Socio-Technical Interaction Research (STIR) Lab. Her research interests are situated at the juxtaposition of Social Computing and Privacy.

References

1. Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle. 1999. Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences.

Proceedings of the 1st ACM Conference on Electronic Commerce, ACM, 1–8.

2. Alessandro Acquisti and Ralph Gross. 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy enhancing technologies*. 36–58.
3. Irwin Altman. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey, CA.
4. Oshrat Ayalon and Eran Toch. 2017. Not Even Past: Information Aging and Temporal Privacy in Online Social Networks. *Human-Computer Interaction* 32, 2: 73–102.
5. Karla Badillo-Urquiola, Xinru Page, and Pamela Wisniewski. 2018. Literature Review: Examining Contextual Integrity within Human-Computer Interaction. .
6. Louise Barkhuus. 2012. The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 367–376.
7. Susan B. Barnes. 2006. A privacy paradox: Social networking in the United States. *First Monday* 11, 9.
8. Paul Dourish and Ken Anderson. 2006. Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human–Computer Interaction* 21, 3: 319–342.
9. Haiyan Jia and Heng Xu. 2016. Measuring individuals' concerns over collective privacy on social networking sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10, 1.
10. Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in It Together: Interpersonal Management of Disclosure in Social Network Services. *SIGCHI Conference on Human Factors in Computing Systems*, 3217–3226.
11. Airi Lampinen, Fred Stutzman, and Markus Bylund. 2011. "Privacy for a Networked World": Bridging Theory and Design. *SIGCHI Conference on Human Factors in Computing Systems*.
12. Robert S. Laufer and Maxine Wolfe. 2010. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues* 33, 3: 22–42.
13. Heather Richter Lipford, Pamela J. Wisniewski, Cliff Lampe, Lorraine Kisselburgh, and Kelly Caine. 2012. Reconciling privacy with social media. *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work Companion*, ACM, 19–20.
14. Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15, 4: 336–355.
15. Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79, 119.
16. Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
17. Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs* 41, 1: 100–126.
18. Judith S. Olson, Jonathan Grudin, and Eric Horvitz. 2005. A Study of Preferences for Sharing and Privacy. *CHI '05 Extended Abstracts on Human Factors in Computing Systems*, ACM, 1985–1988.
19. Xinru Page, Alfred Kobsa, and Bart P. Knijnenburg. 2012. Don't Disturb My Circles! Boundary Preservation Is at the Center of Location-Sharing Concerns. *Sixth International AAAI Conference on Weblogs and Social Media*.

20. Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. *Proceedings of the conference on Human factors in computing systems - CHI '03*: 129.
21. Sandra Sporbert Petronio. 2002. *Boundaries of Privacy: Dialects of Disclosure*. SUNY Press.
22. Osborne M. Reynolds. 1969. Review of Privacy and Freedom. *Administrative Law Review* 22, 1: 101–106.
23. Daniel J Solove. 2006. A taxonomy of privacy. *University of Pennsylvania Law Review* 154, 3: 477–560.
24. Luke Stark, Jen King, Xinru Page, et al. 2016. Bridging the Gap Between Privacy by Design and Privacy in Practice. *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, ACM, 3415–3422.
25. Zeynep Tufekci. 2008. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society* 28, 1: 20–36.
26. Jessica Vitak, Pamela Wisniewski, Xinru Page, et al. 2015. The Future of Networked Privacy: Challenges and Opportunities. *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing*, ACM, 267–272.
27. Yang Wang, Huichuan Xia, Yaxing Yao, and Yun Huang. 2016. Flying Eyes and Hidden Controllers: A Qualitative Study of People's Privacy Perceptions of Civilian Drones in The US. *Proceedings on Privacy Enhancing Technologies* 2016, 3: 172–190.
28. Daricia Wilkinson, Moses Namara, Karla Badillo-Urquiola, et al. 2018. Moving Beyond a "One-size Fits All": Exploring Individual Differences in Privacy. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, ACM, W16:1–W16:8.
29. Pamela Wisniewski, A.K.M. Najmul Islam, Bart P. Knijnenburg, and Sameer Patil. 2015. Give Social Network Users the Privacy They Want. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, ACM, 1427–1441.
30. Pamela J. Wisniewski, Bart P. Knijnenburg, and Heather Richter Lipford. 2017. Making Privacy Personal. *Int. J. Hum.-Comput. Stud.* 98, C: 95–108.