Ubiquitous Privacy: Research and Design for Mobile and IoT Platforms

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

Nick Merrill
University of California, Berkley
Berkeley, CA
ffff@berkeley.edu

Pamela Wisniewski
University of Central Florida
Orlando, FL
pamela.wisniewski@ucf.edu

Richmond Wong
University of California, Berkeley
Berkeley, CA
richmond@ischool.berkeley.edu

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

Pardis Emami-Naeini
Carnegie Mellon University
Pittsburgh, PA
pardis@cmu.edu

Yang Wang
University of Illinois at Urbana-Champaign
Champsign, IL
yvw@illinois.edu

CSCW '18 Companion, November 3–7, 2018, Jersey City, NJ, USA

ACM ISBN 978-1-4503-6018-0/18/11.
https://doi.org/10.1145/3272973.3273012

Abstract
This one-day workshop aims to explore ubiquitous privacy research and design in the context of mobile and IoT by facilitating discourse among scholars from the networked privacy and design communities. The complexity in modern socio-technical systems points to the potential of utilizing various design techniques (e.g., speculative design, design fiction, and research through design practices) in surfacing the potential consequences of novel technologies, particularly those that traditional user studies may not reveal. The results will shed light on future privacy designs for mobile and IoT technologies from both empirical and design perspectives.

Author Keywords
Privacy, IoT, Mobile, Research, Design.

Introduction
Privacy research has been a key research theme in the HCI/CSCW community. The research paradigm within the SIGCHI community generally: 1) focuses on user experiences and technical feasibility, and 2) relies heavily on empirical data collected from users. With the increasing popularity of mobile devices and the Internet of Things (IoT), privacy research is facing a new era characterized by a complex and sophisticated eco-system where new threats and challenges are emerging beyond what was previously imaginable. Considering

Program Committee:

- **Norah Abokhodair,** Microsoft Learning
- **Louise Barkhuus**, University of Copenhagen
- **Sanchari Das,** Indiana University
- **Apu Kapadia,** Indiana University
- **Jen King**, Stanford Law School
- **Lorraine Kisselburgh**, Purdue University
- **Bart Knijnenburg,** Clemson University
- **Priya Kumar,** University of Maryland
- **Mainack Mondal,** Cornell University
- **Airi Lampinen**, Stockholm University
- **Weijia He,** University of Chicago
- **James Pierce,** California College of the Arts
- **Florian Schaub,** University of Michigan
- **Irina Shklovski**, University of Copenhagen
- **Eran Toch,** Tel Aviv University Innovation Lab

the multitude of ubiquitous devices and sensors, ever-changing social contexts, power dynamics, and needs of different stakeholders, this revolution is transforming our understandings of privacy in ways that are uniquely relevant and timely for the SIGCHI community.

Research methodologies from the design community provide different perspectives in understanding this complicated eco-system and offer alternative opportunities for privacy designs. For example, speculative design allows researchers to critique the status quo, imagine and experience an alternative future where they are free from the current market and technology limitations, and raise questions for future technology development [6]. More importantly, it helps to surface other potential (often social and political) issues and consequences that are not obvious through traditional user studies. However, such methodology is yet to be widespread in the networked privacy community. Therefore, by bringing the privacy and design communities together, this workshop aims to explore the following **themes** in the context of mobile devices and the Internet of Things:

1) *How does the evolution in IoT and mobile devices transform our expectations of privacy designs?*
2) *What can privacy researchers learn from the various design methodologies to broaden their research and provide alternative privacy designs?*
3) *How can design researchers proactively facilitate and deepen the privacy-related aspects in their design work?*

The first theme focuses on exploring the characteristics of ubiquitous privacy designs in the context of mobile and IoT, while the second and third themes emphasize how privacy researchers and design researchers can learn from one another to enhance their research and come up with alternative privacy designs. The outcomes of this workshop will be: 1) privacy design heuristics considering the evolving landscape of mobile devices and IoT, and 2) an agenda for how privacy researchers and design researchers can collaboratively move forward in a mutually beneficial way.

Privacy in Mobile and IoT

In this section, we review relevant literature related to ubiquitous privacy designs in the context of mobile and IoT devices, as well as some examples in the intersection between privacy and design.

Privacy in Mobile Contexts

Privacy researchers have studied and predicted user behavior, as well as designed and user-tested multiple ways to increase users' awareness about their mobile privacy and security. For instance, Safi et al. [19] found that asking a user to reflect on their comfort level of their past location sharing behavior is one of the strongest predictors of future location sharing privacy behaviors. Privacy Facts, a "just-in-time" privacy display designed by Kelley et al., warns users when sensitive information (e.g., location) is collected by their phones [12]. Almuhimedi et al. designed a system to notify users of the data collection behaviors of the apps on their phones, which nudged users to deny or permit app permission on their phone [2]. Jackson and Wang designed a privacy discrepancy interface to nudge users to make app permission decisions based on the discrepancy between individual users' general privacy preferences of mobile apps and the privacy risks of these apps [10]. Meanwhile, Lin et al.'s study

Timeline:

- **July 26, 2019**: Website and Call for Participation Due
- **August 31, 2019**: Position Papers Due (submissions will be accepted till September 26, 2019)
- **September 30, 2019**: Review Deadline
- **October 7, 2019**: Notification of Acceptance
- **October 20, 2019**: Camera-ready Papers Due
- **November 9, 2019**: Workshop

leveraged the power of "the crowd" to show that users rely on the ratings of other users to understand the degree to which permission violates users' privacy expectations in mobile applications [14].

A common theme among these studies is the focus on the individual's user experience with mobile privacy leading to calculated improvements in design. There is a need to move beyond the user to employ creative design methodologies that generate innovative, and potentially disruptive, tools that can better meet the needs of different types of users, groups of users, and other stakeholders.

Internet of Things (IoT) Privacy

For privacy designs in the IoT context, we observe a similar trend. For example, drawing from drone controllers' and ordinary citizens' privacy perceptions of drones [20,24], Yao et al. proposed a number of technological and policy-oriented privacy mechanisms for drones, arguing that an app that facilitates the communication between drone controllers and ordinary citizens had the potential to be well perceived and accepted by both groups [25]. Emami-Naeini et al. designed privacy labels for IoT devices (i.e., a security camera, a smart toothbrush, and a smart thermostat) to present various privacy and security factors related to IoT devices (e.g., collected data, purposes of data collection) and found the final versions of the labels to be useful in providing necessary privacy-related information to users [7]. Yao et al. adopted a co-design approach in which the researcher worked together with smart home users to come up with privacy designs for smart homes. Their study discovered a number of factors that should be considered in privacy designs for smart homes [23]. Page et al. proposed the use of a hybrid design approach that balances "user-centric" and "agentic view" of different types of IoT users [16].

We argue that the novelty and increasing complexity in mobile and IoT systems points to the potential and need for exploring the design space beyond existing privacy designs. In this workshop, our goal is to take a deeper dive into speculative and interrogative privacy design [6] for mobile and IoT technologies to address the new challenges and opportunities that will present themselves within the next 5-10 years of ubiquitous privacy design. Through our workshop, we aim to develop privacy design heuristics for mobile and IoT systems to guide future research and practices.

Bridging Privacy and Design

Moving beyond user studies and current technical feasibility, Wong and Mulligan discussed multiple ways that design can be used in relation to privacy along three dimensions, including: 1) the purpose of design, 2) the actors who do design work in these settings, and 3) the envisioned beneficiaries of design work [21]. They argued that, in addition to the traditional privacy research paradigm in which researchers create designs to solve privacy issues, privacy research should utilize values- and critically oriented design approaches to surface social values and help define privacy spaces. In this way, research from the design community can complement traditional privacy research. For instance, Briggs and Thomas adopted an inclusive, value sensitive design approach and identified a number of common values of future identity technologies that were commonly recognized by people from different communities (e.g., young people, older adults, etc.) [3]. Wong et al. leveraged a design workbook of

speculative design fictions to elicit values of different stakeholders [22].

In parallel, research through design has explored privacy in mobile and IoT systems through design-led inquiries. For example, Pierce conducted a design study to develop a theoretical framing of types of privacy concerns related to smart home cameras [17]. Lindley and Coulton used a design fiction to surface policy and privacy implications of drone use in public spaces [15]. The IKEA Catalogue project used a design fiction in the form of a catalog to surface questions about data use in relation to instrumented home furniture [4]. Fox et al's speculative menstrual catalog used speculative design to analyze privacy concerns around menstrual tracking mobile apps [8]. The orientations and uses of design work varies: sometimes to help surface and analyze issues of privacy, sometimes to speculate the future of technology development, and sometimes to synthesize or imagine design concepts and solutions [17].

A number of studies have also hinted the privacy needs and expectations of people other than the direct users of a system, such as incidental users (guests and children) of smart speakers [13], and bystanders of lifelogging devices [9] and Augment Reality glasses [5]. Others have stressed the importance of moving beyond individual needs towards a more collaborative approach where design meets the privacy needs of communities, groups and organizations [18]. For instance, Aljallad et al. [1] proposed a community-based approach to help people make informed privacy decisions about their mobile app security. Similarly, in a study on sharing smart-home devices with people outside of one's home, users often wanted to share their smart home security systems with friends and family members in the case of emergencies, but this technical capability is currently not feasible in most smart home systems [11].

Thus, it is critical that we begin to imagine new use cases and re-imagine existing mobile and IoT privacy designs in a way that can move us strides beyond the status quo. We aim to bring together the expertise and varied approaches of privacy researchers, practitioners, and designers to achieve this goal. Additionally, we intend to build an agenda for how these different communities can work together to move forward.

Contributions

This workshop contributes to privacy and design research by developing privacy design heuristics for mobile and IoT contexts. Moreover, it brings researchers and designers together to discuss privacy norms, design methodologies, frameworks in the ever-evolving landscape of IoT and mobile devices and how to incorporate these ideas into HCI for Ubiquitous Privacy Design. This workshop will also provide resources to researchers and designer from various disciplines on how to work collaboratively and broaden their expertise. For more information on the workshop and the workshop co-organizers, go to: https://privacydesigncscw2019.wordpress.com/

Acknowledgments

Dr. Wisniewski was supported by Mozilla Research and the U.S. National Science Foundation under grant CNS-1814439, which are related to the themes of this workshop. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. National Science Foundation.

References

1. Zaina Aljallad, Wentao Guo, Chhaya Chouhan, et al. 2019. Designing a Mobile Application to Support Social Processes for Privacy Decisions. *Proceedings 2019 Workshop on Usable Security*, Internet Society.

2. Hazim Almuhimedi, Florian Schaub, Norman Sadeh, et al. 2015. Your Location has been Shared 5,398 Times!: A Field Study on Mobile App Privacy Nudging. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*, ACM Press, 787–796.

3. Pam Briggs and Lisa Thomas. 2015. An Inclusive, Value Sensitive Design Perspective on Future Identity Technologies. *ACM Trans. Comput.-Hum. Interact.* 22, 5: 23:1–23:28.

4. Barry Brown, Julian Bleecker, Marco D'Adamo, et al. 2016. The IKEA Catalogue: Design Fiction in Academic and Industrial Collaborations. *Proceedings of the 19th International Conference on Supporting Group Work*, ACM, 335–344.

5. Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, ACM, 2377–2386.

6. Anthony Dunne and Fiona Raby. 2013. *Speculative Everything: Design, Fiction, and Social Dreaming*. MIT Press.

7. Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ACM, 534.

8. Sarah Fox, Noura Howell, Richmond Y. Wong, and Franchesca Spektor. 2019. Vivewell: Speculating Near-Future Menstrual Tracking through Current Data Practices.

9. Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras. *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ACM, 571–582.

10. Corey Brian Jackson and Yang Wang. 2018. Addressing The Privacy Paradox Through Personalized Privacy Notifications. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2: 68:1–68:25.

11. Abhiditya Jha, Jess Kropczynski, Heather Richter Lipford, and Pamela Wisniewski. An Exploration on Sharing Smart Home Devices Beyond the Home. *Extended Abstract presented at the Workshop on Page 10 of 29 Intelligent User Interfaces for Internet of Things in the proceedings of the ACM conference on Intelligent User Interfaces (IUI 2019), Los Angeles, CA.*

12. Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy As Part of the App Decision-making Process. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 3393–3402.

13. Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors

with smart speakers. *Pro. ACM Human-Computer Interaction CSCW*, ACM.

14. Jialiu Lin, Norman Sadeh, Shahriyar Amini, Janne Lindqvist, Jason I. Hong, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12*, ACM Press, 501.
15. Joseph Lindley and Paul Coulton. 2015. Game of Drones. *Proceedings of the 2015 Annual Symposium on Computer-Human Interaction in Play*, ACM, 613–618.
16. Xinru Page, Paritosh Bahirat, Muhammad I. Safi, Bart P. Knijnenburg, and Pamela Wisniewski. 2018. The Internet of What?: Understanding Differences in Perceptions and Adoption for the Internet of Things. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4: 183:1–183:22.
17. James Pierce. 2019. Smart Home Security Cameras and Shifting Lines of Creepiness: A Design-Led Inquiry. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ACM, 45:1–45:14.
18. James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong. 2018. Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us About Cybersecurity. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW: 139:1–139:24.
19. Muhammad Irtaza Safi, Abhiditya Jha, Makak Eihab PAly, Xinru Page, Sameer Patil, and Pamela Wisniewski. 2019. Will They Share? Predicting Location Sharing Behaviors of Smartphone Users through Self-Reflection on Past Privacy Behaviors. *Proceedings 2019 Workshop on Usable Security*, Internet Society.
20. 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.
21. Richmond Y Wong and Deirdre K Mulligan. 2019. Bringing Design to the Privacy Table: Broadening. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ACM, 262.
22. Richmond Y Wong, Deirdre K Mulligan, Ellen Van Wyk, James Pierce, and John Chuang. 2017. Eliciting values reflections by engaging privacy futures using design workbooks. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW: 111.
23. Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. ACM Press, 1–12.
24. Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Free to Fly in Public Spaces: Drone Controllers' Privacy Perceptions and Practices. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ACM, 6789–6793.
25. Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders. ACM Press, 6777–6788.