Designing for Data Awareness: Addressing Privacy and Security Concerns About "Smart" Technologies

JESSICA VITAK, College of Information Studies, University of Maryland, College Park, USA, jvitak@umd.edu

MICHAEL ZIMMER, Department of Computer Science, Marquette University, USA
michael.zimmer@marquette.edu

ANNA LENHART, College of Information Studies, University of Maryland, College Park,
alenhart@terpmail.umd.edu

SUNYUP PARK, College of Information Studies, University of Maryland, College Park, sypark@umd.edu

RICHMOND Y. WONG, Center for Long Term Cybersecurity, University of California Berkeley,
ryw9@berkeley.edu

YAXING YAO, Department of Information Systems, University of Maryland, Baltimore County,
yaxingyao@umbc.edu

The internet of things (IoT) and smart home technologies are pervasive in the U.S. and abroad. Devices like smart speakers, cameras, thermostats, and vacuums promise to save consumers time and energy and to make tasks easier. Many devices also provide significant benefits through accessibility features that offer hands-free options, voice commands, and management through smartphone apps. At the same time, however, researchers and the media have documented a number of vulnerabilities in these devices, which raises concerns about what and how much data is being collected, how that data is used, and who has access to the data. In this one-day workshop, participants will work together to brainstorm potential solutions for making smart device data more visible and interpretable for consumers. Through rotating breakout sessions and full-group discussions, participants will identify data-based threats in popular smart home technologies, select data flows that are most concerning, and generate design ideas for tools or other artifacts that can help consumers make more informed decisions about using these devices. Opportunities for networking and future collaborations will also be incorporated.

CCS CONCEPTS • **Security and privacy**→Human and societal aspects of security and privacy→Privacy protections

Additional Keywords and Phrases: privacy, internet of things, IoT, smart homes, design

ACM Reference Format: Jessica Vitak, Michael Zimmer, Anna Lenhart, Sunyup Park, Richmond Y. Wong, and Yaxing Yao. 2021. Designing for Data Awareness: Addressing Privacy and Security Concerns About "Smart" Technologies. In CSCW '21, ACM, New York, NY, USA.

1 INTRODUCTION TO WORKSHOP THEME

The Internet of Things (IoT) refers to technologies that embed sensors or software in everyday objects to collect, analyze, respond to, and disseminate data [Xia et al 2012]. IoT sensors may be used to collect audio, visual, movement, and other data types, and they are used in nearly all major industries, ranging from healthcare to retail to the military. Norton has estimated that by 2025, there will be more than 21 billion IoT devices in use [9].

An increasingly popular application of IoT is in consumer technologies and especially the area of "smart home" technologies. In a smart home, appliances and furniture use sensors to complete tasks, typically collecting and sharing data through a home network connection. Smart home devices may operate alone or as part of a wider ecosystem where devices share data with each other and can be controlled by a hub device or mobile app. Smart speakers like Amazon Alexa and Google Home are among the most popular smart home devices and often serve as central hubs for controlling other smart devices, while other popular smart home technologies include cameras (e.g., Ring), thermostats (e.g., Nest), lighting (e.g., Philips Hue), and vacuums (e.g., Roomba). According to Statista [8], there are 258.5 million smart homes worldwide, representing 12.2% penetration. The global smart home market is expected to grow to US$135.3 billion by 2025, up from US$78.3 billion in 2020 [6].

IoT raises a number of privacy and security concerns, and smart home devices are of particular interest because one's home is traditionally considered a private sphere. Within CSCW and the wider HCI/social computing research communities, researchers have begun exploring how consumers think about and use smart home devices [1, 4, 5, 10, 14, 15]. Researchers have identified a tension between the convenience provided by smart home devices and considerations for data privacy [15], as well as between different types of users (e.g., primary, secondary, incidental/bystander) [4, 14].

That said, we still lack clarity on users' understanding of what data flows from their smart technologies and how to make information about such data flows more useful to consumers. Currently, smart home devices typically provide data visibility via apps and dashboards where users can review their interactions with a device, but these tools provide limited and often highly curated data streams. While Yao and colleagues [14] made several design recommendations for enhancing privacy when using smart technologies—including increasing transparency and offering multiple modes that constrain data collection depending on the context—few studies have translated their findings about privacy risks and concerns into designs to increase user awareness. Notable exceptions include the IoT Inspector tool [3] and Song and colleagues' work [7] evaluating designs for locating IoT devices.

In light of this, we argue that the sheer quantity and diversity of data collected by IoT devices—and their tremendous popularity in the home—requires additional research to identify best practices for helping consumers understand what data is being collected and used by their smart home devices, and to help them make more informed decisions about whether and how to use these devices.

2 WORKSHOP GOALS

The goal of this workshop is to identify potential solutions to privacy and security concerns raised in prior research examining smart home devices. Specifically, we're interested in responding to findings that consumers make assumptions about data collected by devices, as well as variations in privacy risks across different types of users and contexts. For example, Zheng and colleagues [15] note that "users trust IoT device manufacturers

to protect their privacy but do not verify that these protections are in place" (p. 1). Likewise, Yao and colleagues [14] have explored how bystanders are often caught up in data collection but lack control over the device.

To accomplish this goal, we'll engage workshop participants in a series of design thinking activities to identify challenges related to data collection by these devices and generate design ideas to make IoT data more visible and/or interactive. Depending on the number of participants, we will have between 3-6 groups, each assigned a different type of IoT technology (e.g., smart speakers, cameras, toys) or a different space in the home (e.g., bedroom, shared space, playroom). Throughout the workshop, participants will move between these groups, iterating on others' design ideas.

An additional goal of this workshop is to foster the network of privacy, technology, and design scholars who are interested in the unique challenges new technologies like IoT pose to consumers. The organizers plan to use design ideas developed during the workshop in focus groups with smart home device users to further refine the ideas and develop the most promising ideas for testing in people's homes. The organizers will invite workshop participants to join this larger project if interested. Opportunities for networking will also be included in the workshop schedule.

A final goal is to encourage researchers to think creatively about design challenges like the one being explored during the workshop. Traditional approaches to addressing privacy (e.g., requirements engineering, legal compliance, usable privacy) may not fully protect privacy in this emerging context due to new technologies, stakeholders, and data practices. We expect that many participants will not have a background in design, and we will use the workshop to think creatively about design solutions, including through a speculative design activity and through the use of participatory design methods. We believe this is an important skill for privacy and security scholars to develop when trying to balance the convenience of these technologies against their potential harms.

3 WORKSHOP STRUCTURE

We will hold a one-day workshop on Zoom, with full-group and breakout activities and regular breaks to minimize fatigue. Prior to the workshop, we will share a Google Drive and Slack workspace with all participants. The Drive will include position papers to allow participants to provide feedback on others' work. The Slack is for the broader community of people doing research on networked privacy topics but will also have a channel specifically for this workshop. We will also use Miro boards for the design activities. Below we provide an outline of the full workshop schedule:

- **Introductions & Lightning Talks (30-45 minutes):** We'll open the workshop with introductions from the organizers and an overview of our plans for the day. We'll share brief participant introductions, then let participants who submitted a position paper give a lightning talk (3-4 minutes, two slides max) about the research idea or project they want feedback on. We'll provide opportunities for both written feedback and casual conversations with presenters throughout the day.

- **Panel discussion (45 minutes)**: Following lightning talks, we will hold a discussion with invited panelists to share their experiences and challenges in doing design work at the intersection of privacy and IoT. We will reserve significant time for Q&A with participants.

- **Bio Break / Networking**

- **Design Fiction & Speculative Design Activity (60-90 minutes):** The primary goal of the workshop is to have participants identify creative design solutions to the privacy challenges raised by smart home technologies. To encourage participants to start thinking creatively about design, Richmond Wong will facilitate a design fiction activity to help the group explore and define this problem space. Design fiction and related design futuring practices (e.g., speculative and critical design) create speculative worlds through conceptual artifacts or design proposals [11, 12]. These speculative worlds help designers and researchers surface discussions of values, critique social issues, or present alternative visions of the future. With privacy specifically, these practices can help ask: "What does privacy look like from different perspectives?" and "What conceptions of privacy are at play?"

  Participants will break into groups and be tasked with creating fictional stories and objects that capture some of the major privacy challenges raised by smart home technology. Each group will have a set of virtual card decks for brainstorming and providing ideas for different categories such as different stakeholders, contexts, technologies, and harms. Each group will craft the outline of a short story and develop some associated fictional artifacts (e.g., social media post by a character, text message chain between two characters) depicting a series of privacy-related events in the smart home.

  This activity will help participants craft a shared understanding of the problem space by depicting the situated everyday privacy experiences from the perspective of diverse stakeholders. While the stories may depict near-future scenarios, a concluding discussion will help participants identify what issues and problems are already occurring in smart homes today, and which ones may need to be most urgently addressed. These design fiction stories and artifacts can be referred back to by participants throughout the workshop in order to ground conversations about potential design solutions, and with consent, may be shared afterward to help communicate the workshop findings with a broader audience.

- **Bio Break / Networking**

- **Designing for Visibility (2 hours)**: We'll begin our primary design activity with a short, full-group activity to brainstorm challenges related to smart speakers, which are especially important because they often serve as a hub for smart home ecosystems. We'll ask participants to spend two minutes each brainstorming responses to two prompts: first, we'll ask them to list all the types of data that smart speakers might generate; second, we'll ask them to list all the potential concerns or challenges these data types raise. We'll use Miro Boards so participants can quickly add post-it notes and see others' notes, and so organizers can cluster notes into themes.

  Following this, we will break participants into groups based on areas of the home: (1) private spaces like bedrooms, (2) public spaces like the kitchen and family room, (3) child-focused spaces like playrooms, and (4) spaces that surround a home (e.g., driveway, yard, hallway outside apartment).

Each group will be given a set of prompts that ask them to expand on the smart speaker discussion by identifying additional technologies that are specific to their assigned space, the potential data flows generated by those technologies, and potential privacy risks of those technologies. While considering the effect of each technology, participants will be invited to use the design thinking framework *Layers of Effect* [16], which encourages designers to begin by thinking about primary effects, those that are "intended and known"; secondary effects, which are not core to the product but still impact key stakeholders; and tertiary effects—often unintended and unforeseen consequences on a societal/macro level. This approach will highlight the data governance and privacy concerns inside and outside the home.

Once they have identified those risks, they will begin brainstorming potential design solutions that could respond to those risks. Each group will have its own Miro board for brainstorming and note-taking and will be encouraged to use additional online tools they find appropriate.

After 30-45 minutes, we will mix up the groups using the World Cafe model [2], where 1-2 people will remain in each group while others rotate to other groups. After rotating, we will ask the groups to spend a few minutes catching up on progress, then to continue working on design ideas. We will add an additional design challenge by asking them to consider how their design ideas might vary based on different types of users (e.g., people with disabilities, parents, children, older adults, bystanders).

After 20-30 minutes, we will ask participants to rotate one more time. Again, after reviewing prior work by the group, we will ask groups to continue working on design ideas and commenting on prior ideas, and we will introduce a final prompt for them to consider. This time, participants will be asked to consider how their design ideas are influenced by different types of user relationships (e.g., parents and children, roommates).

- **Bio Break / Networking**

- **Design Debrief / Next Steps / Wrap-up (60-75 minutes):** Back as one group, we will ask each group to provide a short report on the design ideas generated during their session. During this reporting, organizers will map out the different ideas and themes connecting them on a shared whiteboard. Following this, we'll discuss next steps for this research, opportunities for participants to get involved, and networking opportunities to keep connected with workshop participants and the broader community of privacy researchers. We'll also invite participants to contribute to a post-workshop write-up to be shared more widely.

4 SUBMITTING TO AND ATTENDING THE WORKSHOP

We will begin recruiting participants for the workshop in mid-summer and launch a website with information about the workshop and how to submit and will share this through our various networks. Vitak is an active contributor to the Networked Privacy Workshop Series (https://networkedprivacy.com/workshops), which has run 14 workshops at CSCW, CHI, SOUPS, and other venues over the last decade and has built up a large

network of researchers working in this space. We will access this network and share the call more widely on social media platforms and in relevant groups (e.g., CSCW Meta, CHI Meta).

Those interested in attending the workshop will have two ways to participate. Those who are actively conducting research in this space and looking for feedback can submit a 2-4 page position paper that outlines their ongoing or proposed research idea or makes an argument for an approach, theory, or method to studying privacy in the context of IoT and smart homes. If accepted, we will share their position paper with all attendees prior to the workshop via Google Drive and allow participants to comment on the work. They will also be given 3-4 minutes to give a lightning talk about their position paper. This will provide a useful networking opportunity, especially for participants looking for collaborators or specific feedback.

Those interested in attending who do not have current work they want to share can submit a 1-page statement of interest that provides a brief background on their research and their interest in the workshop's focus. These statements will also be shared in the Google Drive, but participants will not give a lightning talk.

All submissions will be reviewed by 2-3 members of the program committee, which includes the organizers and other community members. While Zoom enables larger workshops than conducted in person, we plan to keep this workshop relatively small, limiting it to 20-30 participants. If we receive more applications than that, our main criteria for selection will be the person's fit with the workshop theme. We will also give preference to junior scholars, including students who are studying technology and privacy.

When we notify workshop participants of their acceptance, we will ask them to complete a short survey to identify preferred times (to account for multiple time zones) and accessibility-related requests (e.g., live captioning).

Timeline for workshop:

- **July 23, 2021:** Begin promoting workshop widely
- **September 1, 2021:** Position papers / statements of interest due
- **September 15, 2021:** Workshop acceptance notifications sent
- **October 4, 2021:** Google Drive shared with workshop attendees
- **October 23 or 24, 2021:** Date of workshop
- **November 15, 2021:** Publish write-up/blog based on workshop outcomes

5 ABOUT THE ORGANIZERS

Jessica Vitak is an Associate Professor in the College of Information Studies at the University of Maryland. Her research evaluates the privacy and ethical implications of big data and "smart" technologies. She seeks to understand how privacy concerns play a role in technology adoption and use, and she develops tools and resources to help children and adults make more informed decisions when using technology and sharing sensitive data. She has organized six prior workshops on this topic.

Michael Zimmer is an Associate Professor in the Department of Computer Science at Marquette University. His work focuses on digital privacy & surveillance, data ethics, and the broader social & ethical dimensions of emerging technologies. Recent projects have included both quantitative and qualitative investigations into the privacy and ethical dimensions of big data and computational social science research, wearable fitness trackers, smart home devices, the development of suicide risk prediction algorithms based on social data, and the

increased surveillance practices during the COVID-19 pandemic. He has organized numerous workshops/symposia on this and related topics.

Anna Lenhart is a PhD student in the College of Information Studies at the University of Maryland. Her research focuses on participatory design and lay citizen engagement in technology policy. She has worked in industry as a data ethicist and data system developer. She received her MPP from the University of Michigan and her BA in Engineering at Carnegie Mellon University.

Sunyup Park is a PhD student in the College of Information Studies at the University of Maryland. Her research interest lies in privacy, the Internet of Things, and Human-Computer Interaction. She received her MFA in Communication Design 2020 and her BA in Economics in 2016, both from Yonsei University.

Richmond Wong is a postdoctoral researcher in the Center for Long-Term Cybersecurity at the University of California Berkeley. His research studies the relationships between design and social values by developing design-centered methods to proactively surface ethical issues related to technology (particularly those surrounding privacy and surveillance). He also studies how technology professionals address privacy and ethical issues in their work. He has co-organized multiple prior workshops on this and related topics.

Yaxing Yao is an Assistant Professor in the Department of Information Systems at the University of Maryland, Baltimore County. His research focuses on understanding and addressing the privacy needs in the context of the Internet of Things, smart homes, and online. In particular, his research touches on the needs of those who are not the primary users and seek to balance the conflicting interests and needs of multiple stakeholders. He has organized multiple workshops related to privacy, design, and the Internet of Things.

REFERENCES

[1] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2, 2 (July 2018), 59:1–59:23. DOI: https://doi.org/10.1145/3214262

[2] Juanita Brown. 2010. *The World Café: Shaping Our Futures Through Conversations That Matter*. ReadHowYouWant.com.

[3] Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. 2020. IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 4, 2 (June 2020), 46:1–46:21. DOI: https://doi.org/10.1145/3397333

[4] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. Proc. ACM Hum.-Comput. Interact. 2, CSCW (November 2018), 102:1–102:31. DOI: https://doi.org/10.1145/3274371

[5] Yuting Liao, Jessica Vitak, Priya Kumar, Michael Zimmer, and Katherine Kritikos. 2019. Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption. In *Information in Contemporary Society* (Lecture Notes in Computer Science), Springer International Publishing, Cham, 102–113. DOI: https://doi.org/10.1007/978-3-030-15742-5_9

[6] Markets and Markets. 2020. Smart Home Market worth $135.3 billion by 2025. Available: https://www.marketsandmarkets.com/PressReleases/global-smart-homes-market.asp

[7] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. 2020. I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20), Association for Computing Machinery, New York, NY, USA, 1–13. DOI: https://doi.org/10.1145/3313831.3376585

[8] Statista. 2021. Smart home. Statista. Available: https://www.statista.com/topics/2430/smart-homes/

[9] Steve Symanovich. 2019. The Future of IoT: 10 Predictions about the Internet of Things | Norton. *NortonLifeLock*. Available: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html

[10] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. "I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, USENIX Association, 435–

450.

[11] Richmond Y. Wong, Vera Khovanskaya, Sarah E. Fox, Nick Merrill, and Phoebe Sengers. 2020. Infrastructural Speculations: Tactics for Designing and Interrogating Lifeworlds. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (CHI '20), Association for Computing Machinery, New York, NY, USA, 1–15. DOI:https://doi.org/10.1145/3313831.3376515

[12] Richmond Y. Wong and Deirdre K. Mulligan. 2019. Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Association for Computing Machinery, New York, NY, USA, 1–17. Retrieved June 8, 2021 from https://doi.org/10.1145/3290605.3300492

[13] Feng Xia, Laurence T. Yang, Lizhe Wang, and Alexey Vinel. 2012. Internet of Things. International Journal of Communication Systems 25, 9 (2012), 1101–1102.

[14] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. Proc. ACM Hum.-Comput. Interact. 3, CSCW (November 2019), 59:1–59:24. DOI:https://doi.org/10.1145/3359161

[15] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. Proc. ACM Hum.-Comput. Interact. 2, CSCW (November 2018), 200:1–200:20. DOI:https://doi.org/10.1145/3274469

[16] Kat Zhou. 2021. Design Ethically Toolkit. Available: https://www.designethically.com/toolkit