Research Statement

Imtiaz Ahmad (imtahmad@iu.edu)

My research interests are at the intersection of usable privacy, security, and human-computer interaction. I aim to minimize the privacy/security risks of existing and emerging technologies, while preserving their utility and ensuring equal-benefits for all types of end-users (e.g., owners, bystanders). My research motivation, philosophy, and methodology are centered around studying and designing user-centered privacy enhancing technologies for smart internet connected devices that conform to existing social norms. With the swelling number of internet connected devices (e.g., security cameras, voice assistants, AR/VR technology) around us, the need to protect end users' privacy is greater than ever before. The ubiquitous presence of such networked cameras and microphones 'peeking' into one's personal spaces has given rise to unprecedented privacy concerns. Through my interdisciplinary research spanning the fields of privacy and security, human-computer interaction, psychology, social science, and prototype design, I (i) Explore the privacy perceptions and concerns of end-users, and (ii) Design, implement, and evaluate privacy enhancing solutions to address their concerns. My work has been published in **CSCW '20, '22**[1] [1,2] which is a top HCI venue.

Completed & Current Research

The key theme of my research is to investigate end-users' privacy perceptions and design privacy enhancing technologies for them. Next, I elaborate my completed researches.

Understanding Privacy Perceptions of Incidental Users of Smart Devices. Smart devices such as home security cameras and voice assistants are increasingly becoming pervasive in our physical environment. With the embedded cameras and microphones in these devices, this 'invasion' of our everyday spaces can pose significant threats to the privacy of end-users especially bystanders – who are not the primary user of these devices. To understand how bystanders manage their privacy with these devices, we conducted an interview study about bystanders' perceptions of and privacy enhancing behaviors around smart devices. We find that current designs lead to an uncertainty about device states (on/off/stand-by) and create confusion about features such as the meaning of different colors displayed using LEDs. This uncertainty, along with the mistrust of software controls, lead people to improvise their own tangible privacy mechanisms such as covering cameras with other objects and even attempting to muffle microphones. Our findings highlighted the need for 'tangible privacy' where control and feedback mechanisms can provide a more assured sense of privacy to end-users. [Accepted at CSCW'20]

Design Considerations for Addressing Incidental Users' Privacy Concerns. For protecting end-users' privacy unlike cameras in smart devices (where people can be assured of their privacy by covering or obscuring cameras), microphones need special attention because their current embedded designs do not seem to offer any easy ways of being obscured. To address this gap in the design of smart devices with embedded microphones, based on the findings of the previous study, and with the help of virtual prototyping we developed various design combinations of smart assistants offering hardware vs. software controls and different feedback approaches (privacy notices) about the microphone's state (on/off). Using a between-subjects online experiment (N=261) we compared user's perceptions of risk, trust, reliability, usability, and control for these designs. In general, we found that the use of software applications (for control and feedback) is

[1] accepted and to appear

perceived as unreliable and untrustworthy by our participants. Users considered devices with tangible, built-in physical controls for microphones to be more trustworthy and usable than non-tangible mechanisms. We also found quantitative evidence regarding the effectiveness of tangible privacy mechanisms in protecting *both* user privacy and enhancing usability in the context of smart voice assistants with embedded microphones – suggesting that *tangible privacy mechanisms do* not *represent a usability-privacy trade-off* in the context of smart voice assistants. [Accepted and will be presented at CSCW'22]

Reducing Privacy Tensions Between Visitors and Owners of Smart Assistants. Our studies established that bystanders want to exert some controls over the data collection of smart devices and providing them with tangible control mechanisms have a positive effect on their privacy perceptions. However, from the owners' point of view, providing visitors with certain controlling mechanisms (e.g., to physically turn off devices) may bring about some level of discomfort and may contradict established social norms; thus creating tensions and conflicts regarding privacy management between the two parties [3]. To address this gap, we are conducting a user study where we have developed two prototypical voice assistants incorporating tangible control mechanisms and currently conducting semi-structured interviews with participants to evaluate these designs. Our goal is to find whether tangible designs can provide the desired control for bystanders and at the same time increase owners comfort in sharing their device with other users – thus reducing the existing privacy tensions between the two stakeholders. [This is an ongoing work]

Evaluating Users' Online Photo Sharing Preferences: Privacy vs Viewer Satisfaction. With the rising popularity of online photo sharing, privacy violations have become an increasing concern for users. While the existing privacy enhancing tools (e.g., instant obfuscation) has been shown to be useful in terms of improving privacy, they often come with the price of reduced viewer satisfaction. Finding the perfect balance between user privacy and viewer satisfaction has been a tricky problem. To bridge this, we conducted a user study (N=385) to investigate how temporal photo redaction technique (applying redactions on selected regions of the photos) influences users photo sharing behavior. We also compared sharing preferences when participants share photos with viewers whose devices include (or do not include) trusted hardware (e.g., Intel SGX) to provide higher security and privacy assurances. Our findings suggest that while users in general are comfortable with the existing privacy enhancing photo sharing methods, the proposed temporal redaction mechanisms are often preferred in some contexts. However, whether the viewing platform comes with trusted platform (or not) does not influence users sharing behavior. [This work is currently under review]

Understanding Younger Adults Perceptions of Voice Privacy. Understanding privacy perceptions of end-users of different age groups is an important step in designing fine-grained privacy enhancing technologies. Given that younger people are considered as smart device early adopters and more tech-savvy [6], we want to explore their understanding of voice privacy in the two different contexts of video-conferencing and the daily use of voice assistants. We are currently exploring details regarding younger adults' daily usage of these technologies and their perception of voice privacy by conducting semi-structured interviews. [This is an ongoing work]

Future Research Plan

In the long term, my research goal is to keep exploring and designing privacy enhancing solutions for privacy challenges faced by the end users of smart devices. Over the next half-decade, I envi-

sion a research program with the following thrusts:

T1: Towards Privacy Oriented, Social, and Reliable Smart Assistants. Smart voice assistants with their newly added ability to 'speak and converse' with people [4,7], pose a new security and privacy threat vector. Thus, in addition to the ongoing privacy research on the 'listening' side of these devices, we need to focus on the 'speaking' side as well; particularly, given that these conversational artificial intelligence based smart devices are becoming more human-like. In particular, I want to explore the following sub-thrusts going forward:

- **T1a: Privacy preserving ways to communicate sensitive information.** Apart from the non-private queries (e.g., weather and traffic update) users often make private queries, for example, asking about the next event in daily routine or the side-effect of a medication etc. With the shared nature of voice assistants, often there might be other people present in the shared space and speaking out sensitive private information can be at the same time socially awkward and risky for the person asking. On top of that, responses made by the built-in AI-agents of voice assistants at times can be manipulative and lead users to engage in physically harmful activities [5]. Hence, to this end, I aim to conduct studies that (i) Enable voice assistants to learn about specific contexts and identify sensitive information, (ii) Design privacy preserving ways to communicate sensitive information, and (iii) Explore users perception of trustworthiness and reliability of the 'responses' made by the AI-agents of voice assistants. To achieve these goals, I plan to use statistical and machine learning models to train the voice assistants (identify specific contexts and sensitive information) and empirically validate the prototypical designs using cross-cultural studies, both observational and experimental.
- **T1b: Embodiment of social cues in voice assistants.** With the newly added capability of AI-backed smart assistants to engage in conversation with its users, it is important to make such interactions privacy preserving, reliable, and socially engaging. Prior works in the context of human-robot interaction have shown that the embodiment of anthropomorphic features and non-verbal social cues results in higher levels of social presence, thus evoking more engagement from users. However, very few works have been done in the context of interaction with voice assistants. To bridge this gap in literature, I aim to explore (i) How non-verbal social cues can be embodied in voice assistants to increase their social presence, and (ii) How such embodiment influences users privacy perception and their privacy management in shared spaces. As an extension to my current work, I plan to leverage tangible privacy mechanisms for embodying such non-verbal social cues (e.g., visually perceivable body movement) and assess users' privacy perception and their privacy management using established privacy theories such as Communication Privacy Management, Privacy Calculus etc.

T2: Designing Privacy Oriented, Accessible Smart Devices. Privacy notices in current systems mostly rely on visual and audio cues, for example, the security lock icon in browser windows, green led light for web cameras or audio feedback from voice assistants. Therefore, these systems fail to assist end-users with special needs (e.g., visually-impaired, Deaf and Hard of Hearing) in protecting and managing their privacy, security, and safety. To this end, based on my current research, my future works for addressing the accessibility issues in privacy management will be focused on designing *(i) Accessible Authentication Mechanisms* and *(ii) Privacy Enhancing Assistive Features* for smart devices that are *tangible* in nature. Prototyping such accessible systems would require a deeper understanding of the privacy needs of end-users (with certain disabilities) of smart assistants, their concerns, and then designing and validating sensor platforms embodying 'tangible privacy'.

References

[1] Imtiaz Ahmad, Taslima Akter, Zachary Buher, Rosta Farzan, Apu Kapadia, and Adam J. Lee. Tangible privacy for smart voice assistants: Measuring users' attitudes towards user-centric sensor designs [to appear]. *Proc. ACM Hum.-Comput. Interact.*, (CSCW2), October 2022.

[2] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW2), October 2020.

[3] Christine Geeng and Franziska Roesner. Who's in control? interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019.

[4] *Have a conversation with your speaker or display*, (accessed Feb 2, 2022). `https://support.google.com/googlenest/answer/7685981?hl=en&co=GENIE.Platform%3DAndroid`.

[5] *Alexa told a child to do potentially lethal challenge*, (accessed Mar 7, 2022). `https://www.theverge.com/2021/12/28/22856832/amazon-alexa-challenge-child-dangerous-electricity-algorithm`.

[6] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies*, 2019(4):250–271, 2019.

[7] *New technology lets you talk to Alexa on the Echo Show 10 without repeating the wake word*, (accessed Feb 2, 2022). `https://www.aboutamazon.com/news/devices/conversation-mode-helps-interactions-with-alexa-feel-more-natural`.