# Leveraging Tangible Mechanisms for Providing a True Sense of Privacy to Bystanders of Smart Devices

IMTIAZ AHMAD, Indiana University Bloomington, USA

The current design space of internet connected smart devices has given rise to various privacy concerns for all stakeholders. While there have been attempts to empower users of these devices to better manage their privacy, most of them are either policy based or require software-based implementation. On one hand, these solutions are mainly focused on helping the primary users; thus rarely addressing the privacy needs of bystanders. On the other hand, because of being software-based procedures, they can not provide strong privacy assurances to any stakeholders, especially bystanders. Thus, it is essential to understand the privacy needs and behaviors of people who are bystanders of smart devices to design effective privacy interventions. Moreover, as an alternative to software-based procedures, hardware-based tangible design solutions need to be explored to provide bystanders with an actual sense of their privacy.

CCS Concepts: • **Security and privacy** → *Usability in security and privacy*; • **Human-centered computing** → *Empirical studies in ubiquitous and mobile computing*.

Additional Key Words and Phrases: IoT devices, tangible design, privacy assurance, smart voice assistant

**ACM Reference Format:**
Imtiaz Ahmad. 2018. Leveraging Tangible Mechanisms for Providing a True Sense of Privacy to Bystanders of Smart Devices. In *Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY*. ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/1122445.1122456

## 1 INTRODUCTION

Internet of things (IoT) devices have revolutionized the use of technology in our day-to-day lives. Slowly but surely, these high-fidelity and often privacy-invasive sensor-enabled, internet connected devices are becoming pervasive in our everyday environments. Security cameras such as the Nest Cam and intelligent voice assistants such as Amazon's Echo and Echo Look occupy the same physical space as us and they continuously interact with us. Cameras equipped with high quality sensors constantly lookout for unusual activities and voice assistants equipped with high quality microphones allow users to complete everyday tasks using their voice. Typical uses of such devices include video surveillance for preventing fraud, theft, improving safeguards, and setting reminders for appointments or alarms, playing music, finding answers to miscellaneous questions. The popularity and the number of users of these devices are always increasing. For example, it is estimated that the number of people using voice assistants is projected to reach 1.8 billion by 2021[7]. Although these devices help make our lives more easier and convenient, the ubiquitous presence of such networked cameras and microphones has given rise to a wide range of privacy concerns [5, 12]. Casual conversations and activities may now be captured and disseminated without the knowledge of the user, and at worst, can be used for malicious purposes. In addition to unauthorized recordings made in the cloud, users are particularly vulnerable to inadvertent recordings [3]. Few years back, there was an incident where a couple found out that their Amazon device secretly recorded their



*Woodstock '18, June 03–05, 2018, Woodstock, NY*



ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

conversation and sent it to one of their colleagues without their knowledge[1]. Another incident involved a family finding out a hidden camera live streaming from their Airbnb [4]. Such privacy risks are exacerbated by the recent advancement in sensor designs. Smart devices are now equipped with multiple sensors and these sensors can collect information from users without their knowledge. With the proliferation of such smart devices, casual conversations and encounters once thought to be private and ephemeral now maybe captured and disseminated or archived digitally, and, at worst, can be used for malicious purposes, often without the knowledge of the user. Despite the various documented privacy concerns, designing these devices in a way that enhances privacy, especially for all stakeholders such as guests, visitors, and passersby who are not the owners of these devices, remains a challenge [8]. We refer to this group of people in the vicinity as 'bystanders' of such devices, who are potentially affected by these devices but do not own or directly use them (i.e., they are 'indirect stakeholders'[2]). Although device owners may have some understanding of how and when these devices collect information, bystanders are particularly vulnerable and concerned about their privacy given their potential unfamiliarity with these devices and limited insight into the current configuration of nearby devices [11]. We posit that it is imperative that the smart devices be designed in a way that assures the privacy of bystanders. Thus, an important goal of our research is to explore sensor designs that provide bystanders of smart devices with adequate understanding and a true sense of their privacy through adequate and acceptable feedback (from) and control mechanisms over these devices.

## 2 COMPLETED AND CURRENT WORK

To address this problem space, in our initial work [1], our goal was to understand bystanders' privacy perceptions, their privacy needs, and their current privacy enhancing behaviors around smart devices. We conducted a semi-structured interview study with 19 participants to uncover their perceptions of privacy and their privacy enhancing behaviors. Participants were shown and allowed to interact with two smart devices equipped with both audio and video recording sensors: the Nest indoor camera and the Amazon Echo Show. The findings uncover the needs for unambiguous privacy notices and hardware-based control mechanisms in smart devices. Based on our qualitative findings, we identify and define 'tangible privacy' mechanisms as those privacy control and feedback mechanisms that are 'tangible', i.e., manipulated or perceived by touch, and of 'high assurance', i.e., they provide clear confidence and certainty of privacy to observers. Camera lens caps and the common use of stickers on laptop cameras are examples of tangible privacy mechanisms. On the other hand, an LED indicator is not (since it lacks the certainty provided by a lens cap: users may worry the camera could still be recording with the LED off). We also proposed several design recommendations for smart devices' sensors (e.g., camera, microphone) that align with the properties of our proposed tangible privacy mechanisms. Further, our findings showed that people do not trust software-based control mechanisms mainly because these can be easily compromised by adversaries and these mechanisms do not provide them with a sense of empowerment and control over the device. Our study showed how peoples' privacy enhancing behaviors around smart devices closely follow controlling mechanisms that people apply to regulate their boundary in interaction with real people in a social setting as outlined by Altman's theory of Privacy Regulation [2] and privacy theories like Nissenbaum's Contextual Integrity [9] can play important roles in designing sensors that can assure users of their privacy. To sum up, our study provided strong evidence that people prefer hardware based controlling mechanisms that are

[1] https://www.wnyc.org/story/amazon-echo-recorded-and-sent-couples-conversation-all-without-their-knowledge
[2] Friedman et al. define 'indirect stakeholders' as "parties who are affected by the use of the system" as opposed to 'direct stakeholders' who "interact directly with the computer system or its output" [6, p. 239]

integrated on the device itself and are tangible in nature. They also want privacy notices that are easy to interpret and clearly communicate the device's actual state to everyone in the vicinity of the device.

The previous study revealed that bystanders show a clear preference towards privacy control and feedback mechanisms that can be manipulated physically. Moreover, they want privacy notices that enable them to perceive their action and the system's output simultaneously. Our first study also showed that though participants considered both camera and microphone sensors to be similarly privacy invasive, they found it comparatively harder to maintain their privacy around microphones than cameras. Thus, as a next step, in our current study, we have designed six prototypical voice assistants by varying the types of control mechanism (physical control, software control) and feedback mechanism (physical feedback, software feedback, LED-based feedback) and evaluated participants' perceived reliability, perceived risk, propensity to trust, and perceived control on these prototypes. We also evaluated their perceived usability of these prototypes. The different types of control and feedback mechanisms were designed based on the property of 'tangibility'– as identified in our first study and a property sought out for providing better control and assurance in other contexts [10]. We conducted a between-subject online survey with participants who had prior experience of using smart voice assistants. We presented them with scenarios where they need to consider themselves as visitors. We have conducted quantitative analysis to understand how different combinations of control and feedback mechanisms influence participants' ratings of the above mentioned variables. Overall, currently, our findings show that users prefer on-device hardware-based control, they find hardware-based controls more reliable and usable compared to software based control mechanisms. Moreover, for privacy notices, they mostly prefer LED based notifications compared to both hardware based and software based notifications. Thus, more researches need to be done to explore reliable, on-device, hardware-based disconnects that also gives usable and reliable hardware based notifications to bystanders of smart voice assistants.

## 3 ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under grants CNS-1252697, CNS-1814513, and CNS-181486.

## REFERENCES

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J Lee. 2020. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–28.

[2] Irwin Altman. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.* Brooks/Cole Pub. Co.

[3] Nigel Davies, Nina Taft, Mahadev Satyanarayanan, Sarah Clinch, and Brandon Amos. 2016. Privacy mediators: Helping IoT cross the chasm. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications.* ACM, 39–44.

[4] Emily Dixon. 2019. Family finds hidden camera livestreaming from their Airbnb in Ireland. https://www.cnn.com/2019/04/05/europe/ireland-airbnb-hidden-camera-scli-intl/index.html.

[5] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS'17)*. USENIX Association, Berkeley, CA, USA, 399–412.

[6] Batya Friedman, Peter H. Kahn, Jr., Jennifer Hagman, Rachel L. Severson, and Brian Gill. 2008. The Watcher and the Watched: Social Judgments About Privacy in a Public Place. *Hum.-Comput. Interact.* 21, 2 (May 2008), 235–272.

[7] Go-Gulf. 2018. The Rise of Virtual Digital Assistants Usage – Statistics and Trends. http://www.go-gulf.com/virtual-digital-assistants/.

[8] Adam J. Lee, Rosta Farzan, Apu Kapadia, and Imtiaz Ahmad. 2020. Making sense of risk in an increasingly cyber-physical world. *Critical Quarterly* 62, 1 (2020), 40–48.

[9] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[10] Brygg Ullmer and Hiroshi Ishii. 2000. Emerging frameworks for tangible user interfaces. *IBM systems journal* 39, 3.4 (2000), 915–931.

[11] 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, Article 59 (Nov. 2019), 24 pages.

[12] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 65–80.