Privacy Norms within the Internet of Things Using Contextual Integrity

Denielle Abaquita
University of Central Florida
Orlando, FL 32816, USA
dabaquita@knights.ucf.edu

Karla A. Badillo-Urquiola
University of Central Florida
Orlando, FL 32816, USA
kcurquiola10@knights.ucf.edu

Paritosh Bahirat
Clemson University
Clemson, SC 29631, USA
pbahira@clemson.edu

Pamela Wisniewski
University of Central Florida
Orlando, FL 32816, USA
pamwis@ucf.edu

Abstract
The collection of devices networked via the internet, also referred to as the Internet of Things, is poised to grow in adoption. With this rise has come equally increasing concerns for security and privacy. Considering Nissenbaum's framework of Contextual Integrity, we examined users' perceptions of IoT environmental and wearable devices to investigate acceptable norms surrounding privacy perceptions. We present results from a qualitative analysis of an interview study of 19 parent-young adult dyads to give insights on how privacy norms in context of two IoT environments were varying across two generations. We strongly believe understanding these variations can inform IoT system designs and government policies concerning the privacy and management of IoT devices.

GROUP '20 Companion, January 6–8, 2020, Sanibel Island, FL, USA

ACM ISBN 978-1-4503-6767-7/20/01.
https://doi.org/10.1145/3323994.3369891

Author Keywords
Internet of Things; Contextual Integrity; Smart Home Devices; Wearable Devices; Privacy; Security

CCS Concepts
• **Human-centered computing~Ubiquitous and mobile computing** • Human-centered computing~HCI theory, concepts and models

Introduction
The Internet of Things (IoT) is the term used to refer to the collection of devices connected via internet. IoT devices can range from wearables, like smart watches, to everyday kitchen appliances, like refrigerators. IoT devices are rapidly growing. Gartner has predicted that there will be a 42% increase in the number of IoT building automation devices between 2019 to 2020 [6]. The growing popularity of IoT can be attributed to the experience it gives its users. For example, a smart

Side bar 1

Research Questions

RQ1: Are *there any generational differences between perceptions on appropriateness of norms in IoT environments?*

RQ2: *Do norms differ across different IoT contexts*?

Interview Questions Examples

1. What is the appropriate information?
2. Appropriate duration of storing collected information
3. Actors: Entities receiving and distributing information

home IoT can conveniently use automation to carry out routine chores. However, this convenience comes at the cost of privacy concerns associated with data, which is used to offer such experiences.

Privacy choices and perceptions in IoT are heavily dependent on contextual factors [3]. For IoT, context plays an even more crucial role primarily due to the numerous different factors at play. For example, who is collecting and receiving the data, the type of data itself, the purpose for which collection happens and so on [1,2]. While context significantly affects privacy perceptions of IoT users, it is also possible that non contextual factors like generational differences, conceptual models, and interpersonal relationships can also have an impact [4]. IoT household devices are destined for shared experiences (e.g., a smart assistant like Google Home can be shared by different people in a household). Therefore, it is important to understand how such shared resources shape privacy perceptions. Therefore, our study investigates the perceptions and norms of parents and young adults on IoT devices.

Contextual Integrity Framework

In this paper, we present observations of data collected from a qualitative study which leverages Nissenbaum's Contextual Integrity (CI) framework [3]. According to Nissenbaum, contextual integrity is based on two principles: 1) individuals interacting within a context, and 2) each context has its own norms. This means privacy is a negotiation, reliant on norms and assumptions, between two or more individuals [3]. We leverage the \contextual integrity framework to answer two key research questions mentioned in the side bar.

Methodology

Our data comprised of 38 semi-structured interviews from 19 student-parent dyads. This included 10 Research Experience for Undergraduates (REU) students, 9 non-STEM students, and their 19 parents. Eleven students were male and eight were female. Fourteen parents were female and five were male. The students were Millennials between the ages of 18-26-years-old. All parents were from Generation X (born between 1965-1980), except one Baby Boomer (born between 1946-1964) [5]. The interview questions probed to understand opinions about the norms of IoT devices (see side bar 1). We performed an iterative thematic content analysis to identify themes within our interview responses.

Results

In this section, we discuss the results from our qualitative analysis.

Norms of Appropriate Data Collection

Overall, different contextual factors, such as the type and quantity of information, influenced the privacy perceptions of our participants. They wanted the system to collect just the "right amount" of information, the bare minimum needed for a device to function. It was easy for the participants to identify (in)appropriate information when they had a clearer understanding of benefits/threats. This was specifically in the case of wearable devices; in the case of environmental IoT, it was slightly difficult for them to ideate what should be deemed (in)appropriate. For example, in case of wearable devices 19P said it depends on who has access (see side bar 2).

Side bar 2

Norms of Appropriate Data Collection

Wearable device: "Well that depends on who is going to have access to the information, but location certainly. I think that it's appropriate for people to know where you are, certain health information like with the FitBit. You know, counting the number of steps that you take or calories." - 19P, Female

Environmental devices: *"Anything and everything that doesn't violate someone else's privacy or right."* -19P, Female

However, for environmental devices, 19P had less clarity about what norm should be for (see side bar 2). It was also easier for individuals to conceptualize what information was appropriate to be collected if they owned smart home devices. For example, 14Y owned a Nest Thermostat (Environmental IoT) and said, *"I would say day-to-day lifestyle, you know, like...the temperature you're used to or you know things along those lines*." – 14Y, Male

Norms of Data Storage Duration

The norm surrounding appropriate amount of time personal information should be stored varied a lot across our participants as well as technology types. For some, the appropriate amount of time data was stored was a day or a week. Whereas for others, it was as long as a year or even forever. On the contrary, when participants were asked how long they thought information was being stored, they believed it was much longer than what they expected. For example, 1P expected data to be stored "a week or so," but they believed data is actually stored longer: *"It can store more and more information on smaller devices, so I would think, the sky is the limit." – 1P, Female*

While describing their perspectives on the appropriate duration for information storage, a few participants accounted for additional contextual factors (e.g., what is the purpose for storing different types of information, how the data is being collected, and who is getting the data). On the other hand, some wanted the user to have the control over how long the information is stored, 9P said: *"As long as it is needed by the user, required by the user."* There was similar variation across the different IoT types as well.

Actor Related Norms

Our participants varied greatly in their opinions about who they considered appropriate for accessing the data collected by the devices. Half of the participants felt that the authority of the person accessing the information was important (e.g., authority granted by device owner, device manufacturer, or a government entity). For example, 3P said: *"People with high clearance, like military... not military but some type of status like the corporate or whatever company is making these devices." -3P, Female*

However, six participants mentioned that only the users of the devices should have access to the collected data. In the case of young adults, there was variation within the group; while some wanted to be the "only ones" to have access to their information, others acknowledged the use of data for appropriate purposes like improving products and so on. This points toward a potential difference between the two participant groups about acceptable norms for actors.

Discussion

Context plays a crucial role in terms of privacy choices. Rapidly evolving dynamics of privacy choices in IoT environments make it harder to establish common norms about what is acceptable and what is not. This research attempts to show that norms surrounding privacy may vary to a far greater extent than we might imagine. For a parent, the norm for who receives information may be decided by means of authorization, while for young adults it might be more restrictive as they may want to have all the control of the data for themselves. However, our results also showed that young adults felt their data would stay on the internet forever, while parents felt their data could be deleted at

any time. This shows the valley of differing norms across generations (RQ1).

Norms varied across different types of environments, too (RQ2). For example, it was easier for 14Y to conceptualize what was appropriate for wearable devices, but not for environmental IoT. Additionally, we also believe a gap exists in expectations and perceptions of appropriateness of norms. This was evident in 1P who wanted her information to be stored by the manufacturer for only a week but suspected that it was being stored longer than that. Arguably, a reason why users of IoT devices feel their privacy is being violated is because of this gap between what norms they expect and their devices not meeting these set norms. While the devices themselves can be shared by multiple entities in a closed environment, like a Smart Home, the data can also be treated as a shared entity, where it is owned by the user but is being used by manufacturers to enhance services. Hence, there is a dire need for creating specific guidelines which can help inform acceptable norms for data transactions in IoT and more importantly help create better mental models for end users, so they can make more informed choices. Based on our preliminary results, we found variations across what different generations of users consider to be acceptable norms. It is important to investigate these variations further to inform IoT system designs and government policies concerning the privacy and management of IoT devices.

Acknowledgement

We would like to thank the REU students who participated in this research. This work was supported in part by the National Science Foundation Research Experience for Undergraduates program under Award No. 1560302 and by the National Science Foundation award CNS-1640664. Any opinions, findings, and conclusions and recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. We also thank Mozilla for their support.

References

[1] Yangyang He, Paritosh Bahirat, Bart P. Knijnenburg, and Abhilash Menon. 2019. A Data-Driven Approach to Designing for Privacy in Household IoT. *ACM Trans. Interact. Intell. Syst.* 10, 1: 10:1–10:47.

[2] H. Lee and A. Kobsa. 2016. Understanding user privacy in Internet of Things environments. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 407–412.

[3] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79, 119.

[4] 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.

[5] Richard Fry, Suite 800 Washington, and DC 20036 USA202-419-4300 | Main202-419-4349 | Fax202-419-4372 | Media Inquiries. 2018. *Millennials are the largest generation in the U.S. labor force*. Pew Research Center.

[6] Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020. *Gartner*. Retrieved September 26, 2019 from https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io.