Understanding Perceptions of Smart Devices

Hilda Hadan and Sameer Patil

Luddy School of Informatics, Computing, and Engineering
Indiana University Bloomington
{hhadan,patil}@indiana.edu

Abstract. We explored perceptions regarding the value and sensitivity of the data collected by a variety of everyday smart devices. Via semi-structured interviews, we found that people's conceptualizations of operational details and privacy and security threats of "smart" functions are greatly limited. Our findings point to the need for designs that readily enable users to separate the physical and digital aspects of device operation and call for further exploration of the design space of privacy and security controls and indicators for smart devices.

Keywords: Smart devices · Smart objects · Privacy preferences · Privacy practices · Data value · Data sensitivity · Usable privacy.

1 Introduction

Increasingly, common household devices and objects are made "smart" by augmenting their functions with technical capabilities and Internet connectivity, often referred to as the Internet of Things (IoT). Although such smart capabilities offer a range of personal benefits, the corresponding data handling operations can raise significant concerns due to the potential for impacting personal privacy and enabling surveillance.

Data collection and use by smart devices is often not apparent to users. Therefore, a proliferation of smart devices in everyday environments can exacerbate the problem of understanding and controlling data capture and disclosure by these technologies, thus underscoring the importance and urgency of ensuring that smart devices provide usable privacy. In this regard, researchers have attempted to uncover people's understanding of device operation and data handling, typically focusing on a single device, such as a smart speaker. We build on these efforts via semi-structured interviews that examined these aspects across a variety of smart devices. Specifically, we tackled the following research questions: (i) What are people's understandings of smart device[1] operation and data

[1] In the rest of the paper, we use the term smart devices to refer to any typical household device or object with augmented capabilities and/or Internet connectivity.

Hilda Hadan, Sameer Patil, Understanding Perceptions of Smart Devices, Proceedings of AsiaUSEC'20, Financial Cryptography and Data Security 2019 (FC). February 14, 2020 Kota Kinabalu, Sabah, Malaysia Springer, 2020

handling? (ii) How do people perceive the value and sensitivity of the data collected by smart devices? (iii) What rights and controls do people expect over data collected by smart devices? and (iv) What actions, if any, do people take to control the data collection and manage privacy?

Our findings confirm several aspects pertaining to people's privacy knowledge, preferences, and practices identified in past studies of online privacy and individual smart devices. Additionally, we identify significant gaps in understanding regarding device operation, data handling, and privacy threats and corresponding impact on judgments of data value and sensitivity, expectations regarding rights and controls, and actions pertaining to privacy management.

2 Related Work

Literature related to our research falls under two broad themes: privacy and security of smart devices and data value and sensitivity.

2.1 Privacy and Security of Smart Devices

There has been a substantial amount of work on people's perception of smart technologies such as smart homes [19,22–26], smart speakers/voice assistants [1, 5,15,17], smart TVs [8,9,16], smart thermostats [13], and so on [20]. In general, such studies found that people's concerns regarding privacy and security aspects of smart devices are limited [1,15,19] due to their superficial knowledge regarding the operational aspects of smart technologies [1,5,25,26], limited understanding of data handling [14,18], and incomplete consideration of risks [1,15]. Even those aware of the risks and wishing to prevent third party sharing or secondary use of their data are often willing to trade privacy for the benefits and conveniences of smart devices [16,25].

2.2 Data Value and Sensitivity

Several studies have attempted to study data valuations in monetary terms, finding that people generally prefer money in exchange for data, even when the monetary benefit is small [2,11,12]. However, recent research suggests that individuals are willing to pay for privacy [3]. Yet, when people are not explicitly prompted to consider privacy and security, they rarely do so prior to purchase and tend to become aware of these issues only afterward via media reports and/or unexpected device operation [6]. Moreover, people's limited understanding of how their data is collected and used [14,18] makes it difficult for them to ascribe appropriate monetary valuations to their data.

In contrast, people may find it easier to express valuations in qualitative terms and in relation to sensitivity that is often associated with privacy-related matters. Several studies indicate that smart device users would prefer to take data sensitivity into account, especially when prompted to consider privacy choices and actions [3,17]. While numerous studies of smart devices indicate that people

are willing to trade privacy for convenience and benefits [9, 25], the relationship to data sensitivity has received less research attention.

2.3 Relationship to Research Objectives

Our objective was to uncover perspectives on smart devices without a narrow focus on specific devices or usage contexts typical of previous studies. To that end, our research covered a wide variety of smart devices with the goal of studying the extent to which findings of device-specific studies apply across devices and noting salient commonalities and differences that affect people's operational understanding, privacy preferences, and usage practices related to smart devices in general. Additionally, we investigated whether qualitative descriptions of data value and sensitivity can be useful for bridging the gap between smart device operation and people's privacy expectations.

Unlike most studies that include *users* of a device, we asked people about devices they own and use, as well as those they do not. We believe that it is important to include those who do not currently use a device. First, users of a device are a biased sample and, as such, may not surface the full spectrum of issues, especially about privacy/security concerns (which may presumably be lower for them). Second, smart devices are still in infancy, and their design and features can still be shaped before they become entrenched. To that end, it is important to understand the needs and expectations of non-users/non-adopters so that these could be addressed. Third, novel design ideas often start by gathering requirements from *prospective* users (since the system does not exist yet) and can proceed with their participation (e.g., via participatory design).

3 Method

We conducted semi-structured interviews with 15 individuals (5 Men, 9 Women, and 1 Other) during the spring and summer of 2019 (see Appendix for the interview protocol). Participants were selected based on an online screening questionnaire (see Appendix) advertised locally. All participants were 18 years of age or older (Range: 18–31, Mean = 24) with some experience of using smart devices (see Appendix: Tables 1 and 2). All participants had lived in the United States for at least five years. Participants were compensated $10 cash. We continued collecting data until we reached theoretical saturation, encountering similar responses compared to earlier participants. Overall, our interviews captured perceptions and expectations based on actual as well as imagined usage scenarios regarding a variety of smart devices. All study materials and procedures were reviewed and approved by our university's Institutional Review Board (IRB).

Based on the devices mentioned in the screening questionnaire responses, participants were asked about reasons for purchase, user experience, understanding of operations and data handling. In particular, we inquired about data value, sensitivity, control, and rights. Since the smart devices mentioned by the participants varied, we asked the same set of questions for a list of commonly used

smart devices including Smart TV, Smart Speaker, Smart Toy, Smart Thermostat, Smart Weighing Scale, and Smart Refrigerator. Based on the experience of the first 8 interviews, we slightly modified the interview protocol to ask participants to rank perceived benefits and data sensitivity of 10 smart devices: Smart Speaker, Smart TV, Smart Thermostat, Smart Doorbell, Smart Toy, Smart Refrigerator, Smart Security Camera, Smart Light Bulb, Smart Household Appliance (e.g., Coffee Maker, Toaster), and Smart Car.

Interview transcripts were coded with an iterative inductive approach inspired by grounded theory [10], involving open coding, identification of categories, and aggregation into themes connected to our research objectives.

4 Findings

We organized participant views regarding data and privacy into the various themes that emerged from the interviews.

4.1 Perceptions Regarding Data

Data Types: Participants mentioned a wide variety of data that they think is collected by various smart devices. We categorized the responses into 9 categories: Location (e.g., device location, owner location), Account Information (e.g., demographics, billing information), Voice, Visuals (e.g., video, images), Histories (e.g., browsing history), Health Information, Device Usage Logs, Power Usage, Environmental Data, and Data from Other Devices.

All 15 participants believed that a smart device needs to collect its location for its operation. Three of the participants expressed the belief that a smart thermostat needs to collect the owner's location to adjust the temperature at the perfect time before the owner comes home. Eleven participants further believed that a smart thermostat has the capability of capturing environmental data to adjust temperature accordingly. If a smart device involved logging into accounts, four participants believed that their account information, such as credit card information and basic demographics, is collected by the device. Participants generally expected that only those smart devices that operate via voice, such as a smart speaker, smart toy, and smart TV would collect their voice. Similarly, six participants believed that only devices with visual functions, such as smart refrigerator, security camera, smart doorbell, and smart toy have the capability of capturing visuals, and eight participants thought that only devices with health- or food-related functions, such as smart weighing scale, smart mattress, and smart refrigerator could collect information related to health. One participant expected only devices with energy-saving functions, such as smart thermostat and smart car, to collect power usage. All participants believed that smart TV companies could access the history of their online activities, such as web browsing and purchases, and a smart speaker could grab data from other devices due to its ability to connect to other devices: *"So pretty much anytime that I'm logging in somewhere that is giving them [smart speakers] access [. . .] they're pulling*

information." (P6, Female, 25). Only one participant thought that a smart car would communicate with other devices and systems. All participants suspected that smart devices could log usage information, such as frequency and duration of use. Regarding frequency, participants tended to expect smart speakers, smart TVs, smart refrigerators, smart thermostats, and smart toys to collect data continuously when switched on. On the other hand, smart weighing scales, smart cars, security cameras, smart mattresses, smart doorbells, and smart door locks were expected to collect data only when people interacted with them. Some participants suspected that smart speakers "listen" even when switched off.

Data Flow and Storage: Most participants were aware that their data is sent to the companies which provide them services, such as Google, Amazon, Apple, Samsung, etc. These companies included device manufacturers as well as app developers. Two participants believed that the data collected by smart refrigerators and smart thermostats is sent to third-party contractors because the device makers are too small to maintain databases. Another two participants believed that their data is stored locally within the devices or within the mobile apps, if the devices connected to their phones.

Data Access and Control: Possible parties identified by participants as being able to access the data collected by smart devices included: companies that provide the service (e.g., device manufacturers, app developers), third-parties (e.g., data buyers, advertisers, device retailers), hackers and technical support personnel, and the government. Besides these specific parties, four participants thought that "everyone" could access their information: *"probably the world, the company, whoever they agreed to sell or share the information with"* (P15, Male, 21). P2 believed that her various accounts are somehow all connected online.

Participants expressed mixed opinions about the ability to access and control their own data. For smart devices with no user interfaces (e.g., controlled via mobile apps, web sites, etc.), most participants did not know how to control or access their data because *"there's not really an interface"* (P7, Male, 31). In contrast, P5 assumed she would be able to access the data if she has a login. For smart devices with a user interface on the device, participants generally thought that they have only partial access to the data local to the device but no access to the data sent to the server. Three participants said that they could gain access to server-side data by requesting it from the respective companies. They also believed that the companies are legally obligated to provide the data upon request.

Five participants expected the companies to take responsibility for protecting their data but two of them simultaneously expressed a lack of trust that the companies would do so diligently: *"it's probably encrypted and there's probably network protections going on. I feel like they [the companies] don't do very much. But they do some stuff."* (P1 Male, 24).

Data Value: Participants were aware that their data is used to infer their preferences, facilitate device operation, generate recommendations and advertise-

ments, and improve the devices and future products. Most participants mentioned that their data was sold for a low price online but could not identify the parties to whom the data was sold. Participants generally tended to deem their data as valuable for device manufacturers, service providers, third-party buyers, advertisers, and the government but not for their friends because *"they [friends] already know me pretty well."* (P10, Female, 22). Three participants recognized that their data could potentially be used for malicious purposes such as blackmail. One participant thought that his data does not have monetary value because it is already traded for free services online. Another three participants believed that their smart devices could not possibly hold any valuable data because of limited and infrequent use of the device.

Two participants desired monetary returns for their data: *"If I spent $200 on a TV and they are collecting my data, shouldn't they give me the TV for free?"* (P5, Female, 24). In contrast, another two participants derived value from the customization enabled by the use of their data: *"When things pop up that are so heavily personalized, I can see the value in it."* (P2, Female, 21).

Data Sensitivity: Participants offered mixed opinions about the sensitivity of the data collected by smart devices. Three participants considered the data sensitive because many of these devices are mainly used in private places, such as homes, cars, etc., but with only a vague characterization of the extent of that sensitivity. Two of the three participants mentioned that they enjoyed the benefits of the devices even though that required their data to be visible to other parties. On the contrary, three participants felt that the data collected by their smart devices is not sensitive because they did not provide confidential or personally identifiable information to these devices. For instance, a participant perceived that the data collected by her smart lock is neither sensitive nor valuable: *"Anyone who enters has a passcode that we gave them. So that means they're allowed to enter."* (P10, Female, 22). The possibility of the passcode being stolen did not occur to her.

Surprisingly, some participants showed little concern for privacy because they figured that machines are not "clever" enough to know everything about them: *"I'm not worried that it uses my data, I just use it carefree. What they [the companies] probably want to see is just how normal people live, but that's something that machines can't quantify easily."* (P2, Female, 21). In contrast, others were unconcerned because of the belief that their data is already everywhere and they have little control over its spread: *"I'm personally at the point where I don't care anymore as long as they don't have access to my social security number. Everyone has my cell phone number. I know a few websites have my credit card information, my banking info, and my PayPal account."* (P3, Female, 22).

Data Sensitivity in Relation to Benefit: We asked participants P9 to P15 to rank 10 common smart devices based on 1) benefits of using the devices and 2) the sensitivity of the data collected by these devices (see Appendix: Figure 1). We compared their rankings with their perceptions of data operation to see if their perceived threats corresponded with their reported behavior.

Smart speakers were ranked as the most beneficial. This matched purchasing choices: 10 out of 15 participants either owned or considered getting a smart speaker. Among the devices we covered in the interviews, smart toys and smart thermostats were ranked the lowest on benefit. Again, these rankings align with purchasing decisions: no participants were willing to get a smart toy, and only four out of 15 owned or considered getting a smart thermostat.

Despite ranking the highest on benefits, smart speakers were ranked the highest in terms of sensitivity as well because they *"can hear every single one of your conversations."* (P14, Female, 22). Participants worried about continuous surveillance. Similarly, smart security cameras were ranked as the second most sensitive due to the capability for continuous video monitoring.

Surprisingly, participants ranked smart toys ninth in terms of sensitivity. Five of the seven participants who did the ranking activity did not imagine that smart toys could collect much sensitive information, contradicting the qualitative responses of the first eight participants. A potential reason for the lack of concern could be no prior exposure to such toys and/or no experience with children. Only one of the seven participants ranked a smart toy as highly sensitive: *"I feel like those are pretty interactive and possibly would collect a lot more than you can imagine."* (P14, Female, 22).

Data Rights: At a high level, all participants expressed similar views regarding data rights. They believed that the company that collects the data owns it, not themselves: *"If I bought the device, that's basically granting the company the right to learn all information about me."* (P2, female, 21). However, when it came to specific smart devices, participants' expectations of rights were driven largely by perceptions of data collection and usage, resulting in different opinions regarding different smart devices. For smart devices that could collect visual, voice, demographic, billing, and health-related data, such as smart speakers, smart TVs, smart doorbells, smart security cameras, smart refrigerators, and smart toys, the majority of participants expected significantly more data rights and control. They wanted details, such as what is being collected and who can see it, and desired the ability to stop data collection and minimize secondary use. Two participants expressed hopes of stopping *"unnecessary data collection"* even though *"there is a blurred line between what information is necessary and what isn't"* (P15, Male, 21). In addition, participants wanted the ability to delete their data permanently from servers, with a mechanism to verify the deletion.

A small number of participants were uncertain about data rights because they *"don't know what's being collected and what it's to be used for."* (P5, female, 24). P6 indicated that she would like to have more control over data only if a device collected her personal information. P5 specifically mentioned California Consumer Privacy Act [4] and the European Union's General Data Protection Regulation (GDPR) [7] and believed that she has full rights to her data even though she felt that it is owned by the device manufacturer. For smart toys that could be used by children under the age of 13, P5 asserted that the children and their parents or guardians would have full rights to their data due to Children's Online Privacy Protection Act (COPPA) [21].

4.2 Perceptions Regarding Privacy

Privacy Concerns: Participant responses showed significantly more concerns regarding smart toys and demanded that smart toys include obvious indicators to show when they are on. P4 wanted smart toys to use his own server for data storage instead of relying on the manufacturer's servers. In the case of smart toys, participants specifically highlighted the importance of data transparency and wanted data collection and transmission processes to be *"crystal clear."*: *"The toy around children should be visibly clear on when it's actually collecting information."* (P7, Male, 31).

On the contrary, most participants were less concerned about the data collected by smart devices they deemed comparatively benign, such as smart thermostats, smart door locks, and smart cars. None of the participants were eager to assert rights over this data. Five participants felt that the data collected by these devices is *"not very important."* because these devices do not collect confidential information. Therefore, they did not see the necessity to have control or accessibility for this data. Alternatively, two participants felt that controlling a few devices would not help minimize data exposure because their data is already everywhere.

Privacy Protecting Actions: When asked about specific actions for managing privacy, participants mentioned several crude techniques (with the exception of one technically savvy participant who tinkered with the Domain Name System (DNS) configuration). In the order of most frequent mentions, these included:

(1) Turning the device off (7 participants)
(2) Not caring because no confidential information is involved (4 participants)
(3) Self-regulating (e.g., using the device only for limited purpose, not providing sensitive information, etc.) (3 participants)
(4) Re-configuring home DNS (1 participant)
(5) Going through device privacy settings (1 participant)
(6) Disconnecting from the Internet (1 participant)
(7) Using 'old-style' (i.e., non-smart) devices (1 participant)

Simply turning the device off was the most common strategy to avoid being monitored. While this is a feasible option for devices such as smart speakers and smart TVs, it is not really possible to turn off others, such as smart refrigerators and smart thermostats, as their basic (non-smart) functions require constant operation. Participants reported self-regulating the exposure of sensitive information to smart devices and associated apps and services, especially those used less frequently. As long as participants deemed that sensitive information was not involved, they were unconcerned about privacy and security. Only one participant interacted with privacy settings, and another mentioned temporarily disconnecting the device from the Internet or using a non-smart analog of the smart device. In general, participants claimed general ignorance of privacy management options available for smart devices.

5 Discussion

Our findings serve as replication and validation of several past investigations focused on specific smart devices (see Section 2). In light of the rapidly changing technological landscape (especially in technologies such as smart devices), it is important to verify that past results continue to apply. Moreover, there is increasing recognition of the importance of efforts to replicate and validate prior work and results. Unlike most device-specific prior work mentioned in Section 2, our findings cover a large variety of devices, thus indicating which of the insight gained from single-device studies is generalizable across smart devices. Further, our findings offer a number of major takeaways regarding smart device privacy.

Understanding of data collection and use is limited. Our broad investigation echoes the findings of past studies of privacy in technological contexts, including specific smart devices, in terms of the limited understanding exhibited by participants regarding operational details and policies for data collection, use, and storage. The variety of data types in participant responses suggest that participants had an idea that smart devices use diverse types of data and are likely to send it to the device manufacturer and/or service provider(s) associated with the device. However, specific operational details, such as granularity, collection frequency, storage location, retention periods, etc., were largely unknown. Similarly, it was widely recognized that the data holds value for those who collect it. Yet, participants were not able to ascribe concrete valuations to the data. Moreover, a notable proportion of participants underestimated the inferential powers of large-scale computational data fusion and analyses that can often reveal a surprising amount of private traits.

Threat models are simplistic. Although participants had heard in the media about privacy issues with specific smart devices, they typically did not consider those when evaluating potential risks of smart device capabilities. For instance, the threat of computational inference of private information was ignored. Participants did not take into account that Internet connectivity makes smart devices vulnerable to hacking. In general, malicious acts, such as stolen passcodes, unauthorized access, etc., were overlooked when considering threats posed by smart capabilities of devices, as were security vulnerabilities created by bugs, unpatched software, etc. Limited operational understanding contributed to the simplicity of the threat models and evaluations of the sensitivity of the data captured by smart devices. A lack of full awareness of the threat landscape sometimes led to a false sense of privacy whereby participants did not feel the need to manage data privacy and were even careless when they deemed that no private information was involved.

Expectations are shaped by the primary device function. Notably, participant expectations regarding smart device data collection were driven by the *primary*, i.e., *non-smart*, use for the device. For instance, participants expected a thermostat to collect only the environmental data necessary to achieve its function

of regulating the home temperature and not include unrelated sensors, such as a microphone. As a result, when considering privacy implications, participants often failed to note unexpected sensors, such as cameras in smart toys, microphones in smart TVs, etc. Not taking into account the full spectrum of sensors present within smart devices further contributed to the lack of appreciation for the power of data fusion and computational inferences enabled by smart device data collection.

Privacy practices are rudimentary. The various aspects noted above contributed to lowering privacy concerns which in turn led to rudimentary privacy protection practices, if any. A couple of reasons further contributed to the limited attention to privacy management. First, participants, especially those who owned smart devices, valued the benefits of the devices highly enough to tolerate their data practices even for sensitive data. Second, the physical nature of the devices made it challenging to adjust privacy settings without access to a traditional user interface, especially for devices not associated with apps and/or online services.

6 Limitations

Our sample is composed mostly of young students from the United States. Therefore, applicability to the general population requires verification via studies of samples covering diverse age and cultural ranges. That said, younger individuals are typically more likely to own and use smart devices owing to greater familiarity and comfort with technology. Our findings are derived from self-reports. Complementary studies that examine real-world interaction with smart devices can help ascertain the degree to which self-reports match behavior.

7 Conclusion

Our investigation shows that data practices and privacy threats of smart devices are opaque to users which can lead a false sense of privacy and/or a perceived lack of control. By taking a broad perspective we could surface insight applicable across devices, such as separation of smart and non-smart aspects. Our study covered users as well as non-users. As such, many of the findings are applicable regardless of device ownership and use. Based on our findings, we call for augmenting smart devices with transparent indicators of data handling, enhancing physical interfaces for privacy management, and compartmentalizing smart capabilities and remote data transfer. There is also a need for public policy to catch up with these developments and update and enforce privacy regulations in this rapidly developing domain.

Acknowledgments

We thank the study participants. We are grateful to anonymous reviewers for feedback that helped improve the paper.

References

1. Abdi, N., Ramokapane, K.M., Such, J.M.: More than smart speakers: Security and privacy perceptions of smart home personal assistants. In: Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). USENIX Association, Santa Clara, CA (Aug 2019), https://www.usenix.org/conference/soups2019/presentation/abdi
2. Acquisti, A., John, L.K., Loewenstein, G.: What is privacy worth? The Journal of Legal Studies **42**(2), 249–274 (2013). https://doi.org/10.1086/671754
3. Barbosa, N.M., Park, J.S., Yao, Y., Wang, Y.: "What if?" Predicting individual users' smart home privacy preferences and their changes. Proceedings on Privacy Enhancing Technologies **2019**(4), 211–231 (2019). https://doi.org/10.2478/popets-2019-0066
4. California State Legislature: California consumer privacy act of 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (2018)
5. Chandrasekaran, V., Fawaz, K., Mutlu, B., Banerjee, S.: Characterizing privacy perceptions of voice assistants: A technology probe study. CoRR **abs/1812.00263** (2018), http://arxiv.org/abs/1812.00263
6. Emami-Naeini, P., Dixon, H., Agarwal, Y., Cranor, L.F.: Exploring how privacy and security factor into IoT device purchase behavior. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. CHI '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3290605.3300764
7. European Parliament and Council of the European Union: Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016), http://data.europa.eu/eli/reg/2016/679/oj
8. Ghiglieri, M., Waidner, M.: HbbTV security and privacy: Issues and challenges. IEEE Security Privacy **14**(3), 61–67 (May 2016). https://doi.org/10.1109/MSP.2016.54
9. Ghiglieri, M., Volkamer, M., Renaud, K.: Exploring consumers' attitudes of smart TV related privacy risks. In: Tryfonas, T. (ed.) Human Aspects of Information Security, Privacy and Trust. pp. 656–674. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-58460-7_45
10. Glaser, B.G., Strauss, A.L.: Discovery of grounded theory: Strategies for qualitative research. Routledge (2017)
11. Grossklags, J., Acquisti, A.: When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In: Proceedings of the Sixth Workshop on Economics of Information Security. WEIS 2007 (2007)
12. Hann, I.H., Hui, K.L., Lee, S.Y.T., Png, I.P.: Overcoming online information privacy concerns: An information-processing theory approach. Journal of Management Information Systems **24**(2), 13–42 (2007). https://doi.org/10.2753/MIS0742-1222240202
13. Hernandez, G., Arias, O., Buentello, D., Jin, Y.: Smart Nest thermostat: A smart spy in your home. In: Blackhat USA (2014), https://blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf

14. Kang, R., Dabbish, L., Fruchter, N., Kiesler, S.: "My data just goes everywhere:" User mental models of the Internet and implications for privacy and security. In: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). pp. 39–52. USENIX Association, Ottawa (Jul 2015), https://www.usenix.org/conference/soups2015/proceedings/presentation/kang
15. Lau, J., Zimmerman, B., Schaub, F.: Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. Proc. ACM Hum.-Comput. Interact. **2**(CSCW) (Nov 2018). https://doi.org/10.1145/3274371
16. Malkin, N., Bernd, J., Johnson, M., Egelman, S.: "What can't data be used for?" Privacy expectations about Smart TVs in the US. In: European Workshop on Usable Security (Euro USEC) (2018)
17. Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., Wagner, D.: Privacy attitudes of smart speaker users. Proceedings on Privacy Enhancing Technologies **2019**(4), 250–271 (2019). https://doi.org/10.2478/popets-2019-0068
18. Matsakis, L.: We're all just starting to realize the power of personal data (December 2018), https://www.wired.com/story/2018-power-of-personal-data/
19. Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., Hasu, T., Vainio, N., Myllymäki, P.: Long-term effects of ubiquitous surveillance in the home. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing. pp. 41—50. UbiComp '12, Association for Computing Machinery, New York, NY, USA (2012). https://doi.org/10.1145/2370216.2370224
20. Pierce, J.: Smart home security cameras and shifting lines of creepiness: A design-led inquiry. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. CHI '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3290605.3300275
21. United States Congress: Children's online privacy protection act of 1998. 15 U. S. C. 6501–6505, https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim
22. Worthy, P., Matthews, B., Viller, S.: Trust me: Doubts and concerns living with the Internet of Things. In: Proceedings of the 2016 ACM Conference on Designing Interactive Systems. pp. 427—434. DIS '16, Association for Computing Machinery, New York, NY, USA (2016). https://doi.org/10.1145/2901790.2901890
23. Yao, Y., Basdeo, J.R., Kaushik, S., Wang, Y.: Defending my castle: A co-design study of privacy mechanisms for smart homes. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. CHI '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3290605.3300428
24. Zeng, E., Mare, S., Roesner, F.: End user security and privacy concerns with smart homes. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). pp. 65–80. USENIX Association, Santa Clara, CA (Jul 2017), https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng
25. Zheng, S., Apthorpe, N., Chetty, M., Feamster, N.: User perceptions of smart home IoT privacy. Proc. ACM Hum.-Comput. Interact. **2**(CSCW) (Nov 2018). https://doi.org/10.1145/3274469
26. Zimmermann, V., Bennighof, M., Edel, M., Hofmann, O., Jung, J., von Wick, M.: 'Home, smart home' – Exploring end users' mental models of smart homes. In: Dachselt, R., Weber, G. (eds.) Mensch und Computer 2018 – Workshopband. Gesellschaft für Informatik e.V., Bonn (2018). https://doi.org/10.18420/muc2018-ws08-0539

Appendix

Participant Demographics and Smart Device Ownership

Table 1. Demographics of the Sample

ID	Age	Gender	Affiliation	School/Department/Major
1	24	Male	Undergraduate Student	Liberal Studies
2	21	Female	Undergraduate Student	Marketing
3	22	Female	Undergraduate Student	English
4	27	Male	Graduate Student	Computational Linguistics
5	24	Female	Graduate Student	Cybersecurity
6	25	Female	Staff	Psychological & Brain Sciences
7	31	Male	Graduate Student	Communication & Culture
8	23	Female	Undergraduate Student	Law & Public Policy
9	21	Female	Undergraduate Student	Art Management
10	22	Female	Undergraduate Student	Neuroscience, Spanish
11	29	Male	Graduate Student	Religious Studies
12	22	Other	Undergraduate Student	Psychology
13	21	Female	Undergraduate Student	Game Design
14	22	Female	Undergraduate Student	Management
15	21	Male	Undergraduate Student & Staff	English

Table 2. Smart device ownership or willingness to purchase

Device	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
Smart TV*	O	✔	O	O	✘	✔	✔	O	O	O	O	✔	O	✘	O
Smart Speaker*	O	O	✘	O	✘	✔	✘	✘	O	O	O	✘	O	O	O
Smart Thermostat	✘	✔	✘	✘	✘	✔	✘	✘	–	O	–	✔	✘	–	–
Smart Toy*	✘	✘	✘	✘	✘	✘	✘	✘	–	–	–	–	–	–	–
Smart Weighing Scale*	–	–	–	–	–	–	–	–	✘	✘	✘	✘	O	✘	✘
Smart Refrigerator*	–	–	✔	–	✘	✔	–	O	✘	✘	✔	✘	✘	✘	✘
Smart Car	✘	–	–	✘	O	–	✔	–	–	–	–	–	–	–	–

*: Included in the interview protocol
O: Own the device
✔: Considered getting the device
✘: Not considered getting the device
–: Not mentioned by the participant

Results of the Ranking Exercises

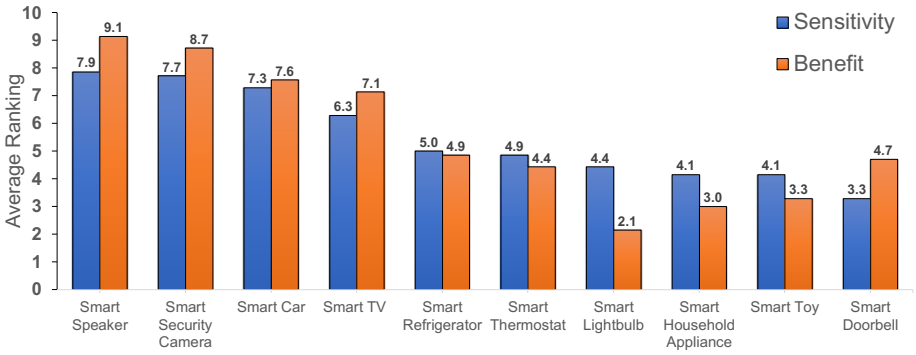

Fig. 1. Ranking of Data Sensitivity and Device Benefit

Screening Questionnaire

Thank you for your interest in participating in our study on Understanding People's Use and Perceptions of Internet-Connected Everyday Objects.

Please fill out this brief 1-minute questionnaire regarding yourself and your experience of using Internet-connected devices. We will use your answers to determine if you are eligible to participate in the study.

If you qualify, we will contact you via email for a 45-60 minute in-person/video conference/telephone interview for which you will receive $10 cash/cash equivalent (for in-person interview) or $10 Amazon gift certificate (for video interview) as a token of our appreciation for your participation. If you do not qualify for participation, your responses will be safely discarded.

1. What is your Year of Birth?
2. What is your Gender?
   (a) Male
   (b) Female
   (c) Something else. Please specify:
   (d) Do not wish to answer
3. How long have you been living in the United States?
   (a) All my life
   (b) Less than a year
   (c) 1 year
   (d) 2 years
   (e) 3 years
   (f) 4 years
   (g) 5 years
   (h) 6 years
   (i) 7 years
   (j) 8 years
   (k) 9 years
   (l) 10 years
   (m) More than 10 years
4. Are you a resident of Bloomington, Indiana?
   (a) Yes
   (b) No
5. Are you affiliated with Indiana University Bloomington?
   (a) Yes
   (b) No
6. [If YES to Q5] What is your affiliation with Indiana University Bloomington? (*Check all that apply.*)
   (a) Undergraduate Student
   (b) Graduate Student
   (c) Faculty
   (d) Staff
   (e) Retired
   (f) Something else. Please specify:

7. [If Q6 is answered as Faculty, Staff, Retired] What department or school are you affiliated with?
8. [If Q6 is answered as Undergraduate Student, Graduate Student] What is your major/field of study?
9. Which of the following Internet-connected device(s) do you own?
   (a) TV
   (b) Thermostat
   (c) Speaker (e.g., Amazon Echo, Google Home, etc.)
   (d) Refrigerator
   (e) Light bulb
   (f) Doorbell
   (g) Door lock
   (h) Burglar alarm
   (i) Toy
   (j) Small household appliance (e.g., Coffee maker, Toaster, Crock pot, etc.)
   (k) Garage door opener
   (l) Car
   (m) Other. Please specify:
10. How would you rate your familiarity with the following concepts or tools?

	I've never heard of this	I've heard of this but I don't know what it is	I know what this is but I don't know how it works	I know generally how this works	I know very well how this works
IP address	○	○	○	○	○
Cookie	○	○	○	○	○
Incognito mode/ private browsing	○	○	○	○	○
Encryption	○	○	○	○	○
Proxy server	○	○	○	○	○
Secure Sockets Layer (SSL)	○	○	○	○	○
Tor	○	○	○	○	○
Virtual Private Network (VPN)	○	○	○	○	○
Privacy settings	○	○	○	○	○

11. Please indicate whether you think each statement is true or false. Please select "I'm not sure" if you don't know the answer.

	True	**False**	**I'm not sure**
Incognito mode / private browsing mode in browsers prevents websites from collecting information about you.	○	○	○
Tor can be used to hide the source of a network request from the destination.	○	○	○
A VPN is the same as a proxy server.	○	○	○
IP addresses can always uniquely identify your computer.	○	○	○
HTTPS is standard HTTP with SSL to preserve the confidentiality of network traffic.	○	○	○
A request coming from a proxy server cannot be tracked to the original source.	○	○	○

12. How would you prefer to be interviewed? (*Check all that apply.*)
    (a) In-person
    (b) Telephone
    (c) Video Conference (e.g., Zoom)
13. If you qualify for the study, which email address should we use to contact you for scheduling a study session?

Semi-structured Interview Protocol

The interview should take around 45-60 minutes. I would like to ask you some questions about Internet-connected objects and devices you commonly use. It could be any object that connects to the Internet in some way. Some examples are security cameras, thermostats, TVs, etc. I would like to ask about your experiences of using such objects and devices and your thoughts on how they operate.

Before we start, do you have any questions?

1. Tell me a little bit about yourself.
2. Tell me your experience with technology.
3. Tell me some Internet-connected objects or devices you commonly use.

For participants who do not own a smart device, ask the following questions:

4. Have you ever considered getting one? Could you give me some examples?
5. [If No to Q4] What has prevented you from getting one?
6. [If Yes to Q4] Imagine that you have a (the item mentioned in Q4 or each of the following devices: Smart Speaker, Smart TV, Smart Weighing Scale, Smart Refrigerator, Smart Toy, Smart Thermostat, Anything else the participant thinks could be Internet-connected): How would you set it up?
7. How would you use it? What would be the process?
8. What data do you think it would use?
9. How do you think it would use this data?
10. What is your opinion about the data being collected and used?
11. What is the benefit or value you perceive in this data?
12. How do you perceive the sensitivity of the data?
13. How often do you think it would use this data?
14. How often do you think you would interact with it?
15. How or where do you think it would store this data?
    (a) What do you mean by cloud/local/etc.?
    (b) Who will provide the storage service?
    (c) Where is the storage located?
    (d) What kind of storage is it?
    (e) How will the storage protect your data from unauthorized access?
16. Who do you think owns this data?
    (a) How do you think they would access it?
    (b) Why do you think they own the data?
    (c) Why would they want to own the data?
    (d) What could they do with the data?
17. Who do you believe can see this data? How do you think they access it?
18. What benefit or value do you perceive other parties can get from this data (e.g., anyone else besides yourself, such as your friends, colleagues, other companies, device manufacturers, government, etc.)? Why?

19. Do you think you would be able to control or access this data? Why or why not?
    (a) What rights do you think you would have over the data?
    (b) What rights would you like to have over the data?
    (c) Why do you believe so?
    (d) Would you like to have control and access? If yes, how would you want to view/access/control the data? If no, why not?
20. What do you think the data collected by this device is worth? Why?
21. Who would pay for this data? (May need to inform the participant that different parties could have different valuations.)
22. How do you handle or manage the data collected about you by this device?
    (a) If the person does not manage or handle data: Why not?
    (b) If the person does manage or handle data: Why do you do it this way?
    (c) If the person wishes to manage or handle data but cannot do it or cannot do it well: What would make it easier or more convenient for you to manage the data?

For smart device owned by the participant, ask following questions:

23. When did you buy it?
24. Why did you buy it?
25. How did you set it up?
26. Could you please describe your experience? How do you use it? What is the process?
27. How do you think it operates?
28. What data do you think it uses?
29. Why do you think it uses this data?
30. How do you think this data is used?
31. What is your opinion about the data being collected and used?
32. What is the benefit or value you perceive in this data?
33. How do you perceive the sensitivity of the data?
34. How often do you think it uses this data?
35. How often do you interact with it?
36. How or where do you think it stores these data?
    (a) What do you mean by cloud/local/etc.?
    (b) Who do you think provides the storage service?
    (c) Where is the storage located?
    (d) What kind of storage is it?
    (e) How will the storage protect your data from unauthorized access?
37. Who do you think owns this data?
    (a) How do you think they access it?
    (b) Why do you think they own the data?
    (c) Why would they want to own the data?
    (d) What could they do with the data?
38. Who do you believe can see this data? How do you think they access it?

39. What benefit or value do you perceive other parties can get from this data (e.g., anyone else besides yourself, such as your friends, colleagues, other companies, device manufacturers, government, etc.)? Why?
40. Do you think you can control or access this data? Why or why not?
    (a) What rights do you think you have over the data?
    (b) What rights would you like to have over the data?
    (c) Why do you believe so?
    (d) Would you like to have control and access? If yes, how would you want to view/access/control the data? If no, why not?
41. What do you think the data collected by this device is worth? Why?
42. Who would pay for this data? (May need to inform the participant that different parties could have different valuations.)
43. How do you handle or manage the data collected about you by this device?
    (a) If the person does not manage or handle: Why not?
    (b) If the person does manage or handle: Why do you do it this way?
    (c) If the person wishes to manage or handle but cannot do it or cannot do it well: What would make it easier or more convenient for you to manage the data?

Give participants handouts and ask the following questions:

44. Here is a sheet of paper that has various common objects that are augmented with smart Internet-connected capabilities. Could you please write down your ranking of these devices in terms of the benefit or value you expect from them? Please rank in order starting from the most beneficial and ending with the least beneficial.

Device	**Rank**
Smart Speaker (e.g., Echo, Alexa, Google Home)	
Smart TV	
Smart thermostat	
Smart doorbell	
Smart toy	
Smart refrigerator	
Internet connected home security camera	
Smart light bulb	
Smart household appliance(e.g., Coffee maker, Toaster, Crock pot, etc.)	
Smart car	

    (a) Could you elaborate why you ranked the devices the way you did?
    (b) Why do you think [device] is the most beneficial one?
    (c) Why do you think [device] is the least beneficial one?

45. Here is another sheet of paper that has the same common objects that are augmented with smart Internet-connected capabilities. This time could you please write down your ranking of these devices in terms of your opinion regarding the sensitivity of the data they collect and process? Please rank in order starting from the most sensitive and ending with the least sensitive.

Device	**Rank**
Smart Speaker (e.g., Echo, Alexa, Google Home)	
Smart TV	
Smart thermostat	
Smart doorbell	
Smart toy	
Smart refrigerator	
Internet connected home security camera	
Smart light bulb	
Smart household appliance(e.g., Coffee maker, Toaster, Crock pot, etc.)	
Smart car	

(a) Could do you elaborate why you ranked the devices the way you did?
(b) Why do you think [device] is the most sensitive one?
(c) Why do you think [device] is the least sensitive one?

Wrap-up:

46. Is there anything you want to add?
47. Is there any other question I should have asked?