"Most Companies Share Whatever They Can to Make Money!": Comparing User's Perceptions with the Data Practices of IoT Devices

Mahdi Nasrullah Al-Ameen, Apoorva Chauhan, M. Ahsan, Huzeyfe Kocabas

"Most Companies Share Whatever They Can to Make Money!": Comparing User's Perceptions with the Data Practices of IoT Devices

Mahdi Nasrullah Al-Ameen[1], Apoorva Chauhan[2], M A Manazir Ahsan[1], and Huzeyfe Kocabas[1]

[1] Utah State University, USA
[2] University of Waterloo, Canada
mahdi.al-ameen@usu.edu, apoorva.chauhan@uwaterloo.ca, {manazir.ahsan, huzeyfe.kocabas}@aggiemail.usu.edu

Abstract. With the rapid deployment of Internet of Things (IoT) technologies, it has been essential to address the security and privacy issues through maintaining transparency in data practices, and designing new tools for data protection. To address these challenges, the prior research focused on identifying user's privacy preferences in different contexts of IoT usage, user's mental model of security threats, and their privacy practices for a specific type of IoT device (e.g., smart speaker). However, there is a dearth in existing literature to understand the mismatch between user's perceptions and the actual data practices of IoT devices. Such mismatches could lead users unknowingly sharing their private information, exposing themselves to unanticipated privacy risks. To address these issues, we conducted a lab study with 42 participants, where we compared the data practices stated in the privacy policy of 28 IoT devices with the participants' perceptions of data collection, sharing, and protection. Our findings provide insights into the mismatched privacy perceptions of users, which lead to our recommendations on designing simplified privacy notice by highlighting the unexpected data practices.

Keywords: IoT · User Study · Mismatched Privacy Perceptions

1 Introduction and Background

The Internet of Things (IoT) is a system of interrelated devices provided with unique identifiers and the ability to transfer data over a network without requiring human intervention [9]. The IoT devices are becoming increasingly popular in day-to-day lives, with nearly two-thirds of Americans owning at least one IoT connected device [3]. Despite the increasing popularity and immense potential of IoT devices, security and privacy issues remain as major concerns [2, 12].

The study of Naeini et al. [7] explored the privacy preferences of users in different contexts of IoT usage, where participants reported to be less comfortable with data collection in private places as compared to public settings. The limited technical understanding of people often contributes to their incorrect

mental model of security threats in an IoT environment [12]. A recent study by Malkin et al. [5] reported that almost half of their participants who were users of Amazon and Google smart speakers, did not know that their recordings were being permanently stored by the devices. Due to such unawareness, only a quarter of their participants reviewed their recorded interactions, where very few had ever deleted any recordings [5]. A separate study [4] on smart speakers identified that users trade privacy for convenience with different levels of deliberation and privacy resignation.

People reported their interest to be notified about the data practices of IoT device [7]. However, the privacy notice often fails to help users with making an informed decision to protect their privacy preferences while purchasing or using an IoT device [2]. The study of Page et al. [8] unpacked the relation between people's perceptions and adoption of IoT technology. The authors [8] divided the IoT users into two categories: "user-centric", who think that the IoT devices are to be controlled by users; and "agentic", who think that the control of IoT devices are to be negotiated between the machine and human. The study highlighted privacy concerns for the people coming from a user-centric perspective given that consumer-oriented IoT is currently moving towards the agentic view [8]. The findings from these studies call for an investigation to identify the gaps between people's perceptions and the actual data practices of IoT devices. We addressed this challenge in our work, which is guided by the following research enquiries:

- What are users' perceptions of information collection by IoT devices? How do their perceptions vary from the actual data practices?
- What are users' perceptions of information sharing (with third-party entities) by IoT devices? How do their perceptions vary from the actual data practices?
- What are users' perceptions of data protection strategies adopted by IoT devices? How do their perceptions vary from the actual data practices?

To address these research questions, we selected 28 IoT devices from different categories, including health & exercise, entertainment, smart homes, toys & games, and pets, and reviewed their privacy policies. We then conducted a lab study with 42 participants, where they reported their perceptions of data collection, sharing, and protection by IoT devices. Our analysis identifies the gaps between participants' perceptions and the actual data practices of IoT device. The findings from this study would contribute towards the design of simplified and usable privacy notice by highlighting the unexpected data practices of users.

2 Methodology

We conduced individual study session with each participant in a lab setting. We recruited participants by sharing our study information through email and online social media. A total of 42 participants (16 females, 25 males, and 1 other), who live in Logan, Utah, took part in this study. The age-range of our

participants varied between 18 and 64, where most (35, 83.3%) of them belonged to the age group 18-34. Among our participants, 26 (61.9%) identified as White, followed by Asian (16, 33.3%), Hispanic/Latino (1, 2.4%), and Other (1, 2.4%). A majority (26, 61.9%) of participants were students. None of our participants had any academic or professional background in cybersecurity. Our study was approved by the Institutional Review Board (IRB) at Utah State University.

Selection of IoT Devices. We selected 28 devices for our study (see Table 4 in Appendix) from the list of IoT devices compiled by Mozilla Foundation[1], where the devices are divided into different categories (e.g., health & exercise, entertainment, smart homes, toys & games, and pets) based on their core service and functionality. We conducted a series of focus-group discussion among researchers in this project and with our colleagues to finalize our device selection.

Types of Information. In light of prior work [10] and the privacy policy of selected devices, we identified nine categories of information that are generally collected by a device or service provider, where each type of information is divided into sub-categories. For example, name, gender, and date of birth of a user are collected as 'personal information'. The other types of information considered in our study include: *Contact* (email address, postal address, and phone number), *Financial* (bank account details, and credit or debit card number), *Health* (height, weight, and work out details), *Location* (current location: city level or more precise), and *Media* (audio, and video). We also considered the information about IoT device usage, and the information an IoT device may collect from a connected device (e.g., contact list from a smartphone) and from an online social media (e.g., friend list from Facebook).

Procedure. We conducted the study in a lab environment, where participants completed the survey hosted on Qualtrics[2] after they had read and agreed to informed consent document. Each participant was presented with four IoT devices, selected in a semi-random process from our list of 28 devices (each IoT device was presented to six participants). For each IoT device, the participant was presented with a visual description about its functionality. Participants could take as much time as they needed to familiarize themselves with the functionality of the device. Thereafter, they reported their perceptions of information collection and sharing by that device, where we presented them with each type of information (see the above paragraph for further details). Participants were also asked about their perceptions of the reasons behind information collection and sharing. Then, participants reported their perceptions of security and privacy strategies (e.g., encryption, anonymization) adopted by the device for data protection. For each participant, the above process was repeated for three other devices. At the end of study, participants answered a set of demographic questionnaire. On average, each session took around 45 minutes.

[1] List of IoT Devices, compiled by Mozilla Foundation: https://mzl.la/2zOK4II

[2] Qualtrics is an online survey platform used to create, distribute, collect, and analyze survey data (www.qualtrics.com)

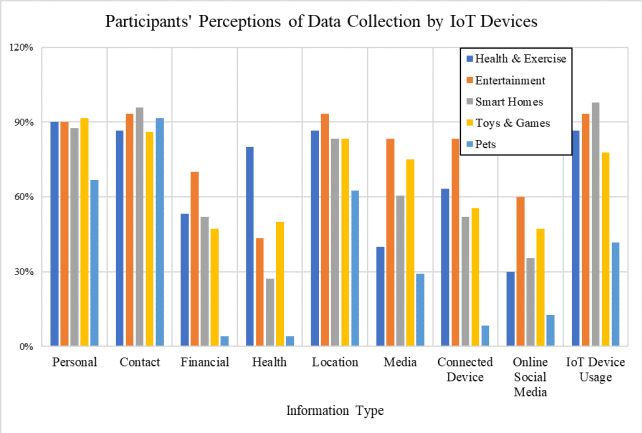

Fig. 1. Participants' Perceptions of Data Collection by IoT Devices

Analysis. We went through the privacy policy of each IoT device, and compared that with participants' perceptions in terms information collection, sharing, and protection. There are four cases resulting from our comparison: a 'Yes-Yes' match, a 'No-No' match, a 'Yes-No' mismatch, or a 'No-Yes' mismatch. Here, a 'Yes-Yes' match for information collection means, the user believes that the information is collected by a device and the privacy policy states that it is indeed collected, where a 'No-Yes' mismatch represents, the user thinks that the information is not collected by a device, but that information is collected according to the device's privacy policy.

3 Results

3.1 Data Collection by IoT Devices

Figure 1 presents participants' perceptions of data collection by the IoT devices, where most of the participants perceive that the IoT devices collect contact (91.07%), personal (86.31%), location (82.74%), and device usage information (82.74%). Participants' perceptions of data collection are related to the category of IoT devices. Considering all data types, IoT devices in "pets" category are perceived to collect least amount of information as compared to the devices in other categories, where the "entertainment"-focused devices are perceived to collect most amount of data from users. In some instances, participants' perceptions of collecting a specific type of information are related to the core service offered by the device, where IoT devices in "Health & exercise" category are perceived to collect more health information as compared to the devices in other categories (see Figure 1).

Table 1 presents the matches and mismatches between participants' perceptions and the privacy policy of IoT devices in terms information collection. From the perspective of user's privacy preservation, we consider a 'No-Yes' mismatch

Information Type	(Mis)Match	Health & Exercise	Entertainment	Smart Homes	Toys & Games	Pets
Personal	Yes-Yes	74.74%	56.30%	59.88%	77.78%	50.00%
	No-No	3.16%	0.00%	0.00%	0.00%	12.50%
	Yes-No	9.47%	0.00%	25.31%	0.00%	12.50%
	No-Yes	12.63%	43.70%	14.81%	22.22%	25.00%
Contact	Yes-Yes	79.76%	54.17%	64.20%	61.11%	91.67%
	No-No	0.00%	0.00%	0.00%	0.00%	0.00%
	Yes-No	0.00%	0.00%	17.28%	0.00%	0.00%
	No-Yes	20.24%	45.83%	18.52%	38.89%	8.33%
Financial	Yes-Yes	20.00%	27.16%	34.26%	35.19%	4.17%
	No-No	31.43%	35.80%	20.37%	0.00%	0.00%
	Yes-No	20.00%	16.05%	39.81%	0.00%	0.00%
	No-Yes	28.57%	20.99%	5.56%	64.81%	95.83%
Health	Yes-Yes	42.03%	0.00%	0.00%	*NA	*NA
	No-No	14.49%	80.00%	77.08%		
	Yes-No	28.99%	20.00%	8.33%		
	No-Yes	14.49%	0.00%	14.58%		
Location	Yes-Yes	96.43%	63.41%	52.63%	73.33%	58.33%
	No-No	0.00%	0.00%	14.04%	0.00%	0.00%
	Yes-No	0.00%	0.00%	17.54%	20.00%	0.00%
	No-Yes	3.57%	36.59%	15.79%	6.67%	41.67%
Media	Yes-Yes	14.29%	29.41%	37.50%	51.67%	20.83%
	No-No	51.79%	16.47%	33.33%	6.67%	66.67%
	Yes-No	12.50%	25.88%	15.63%	13.33%	8.33%
	No-Yes	21.43%	28.24%	13.54%	28.33%	4.17%
Connected Device	Yes-Yes	16.22%	35.71%	11.90%	*NA	*NA
	No-No	32.43%	16.67%	45.24%		
	Yes-No	32.43%	19.05%	26.19%		
	No-Yes	18.92%	28.57%	16.67%		
Online Social Media	Yes-Yes	15.79%	33.33%	11.90%	50.00%	0.00%
	No-No	26.32%	12.82%	59.52%	0.00%	60.00%
	Yes-No	5.26%	10.26%	19.05%	0.00%	0.00%
	No-Yes	52.63%	43.59%	9.52%	50.00%	40.00%
IoT Device Usage	Yes-Yes	92.59%	69.05%	48.33%	68.75%	45.83%
	No-No	0.00%	0.00%	11.67%	0.00%	0.00%
	Yes-No	0.00%	0.00%	10.00%	0.00%	0.00%
	No-Yes	7.41%	30.95%	30.00%	31.25%	54.17%

Table 1. Match/Mismatch between Participants' Perceptions and Privacy Policy: Data Collection by IoT Devices [*NA: Information is not available in privacy policy]

as the most critical one, where users believe that the IoT device does not collect an information, although it is actually collected by that device. For instance, we found a 'No-Yes' mismatch in 95.83% of cases for the devices in "pets' category in terms of collecting financial information. Considering all data types, we found most 'No-Yes' mismatch for the IoT devices in "entertainment" and "pets" category, followed by the devices in "toys & games", "health & exercise" and "smart homes".

As we asked participants about the reasons of information collection by an IoT device, in about half of the cases, they reported that information collection is required for the core functionality of a device. In around one-fourth of cases, participants perceive that information collection is needed for the organizations in IoT business to improve the functionality of their device and offer personalized service to the customers. Some participants believe that the business entities collect user information through their IoT devices for marketing, and advertising their other products to the customers.

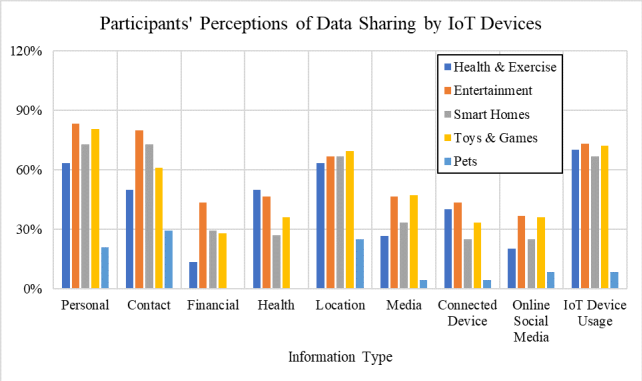

Fig. 2. Participants' Perceptions of Data Sharing by IoT Devices

3.2 Data Sharing by IoT Devices

Figure 2 illustrates participants' perceptions of data sharing by the IoT devices. A majority of participants perceive that the IoT devices share users' personal (67.26%), contact (61.31%), location (60.71%), and device usage (61.31%) information with third-party entities. Participants' perceptions of data sharing are related to the category of IoT devices. Considering all data types, IoT devices in "entertainment" category are perceived to share most amount of user data, where the participants perceive that the devices in "pets" category share least amount of user information with other entities. We also found that participants' perceptions of sharing a specific type of information varied across different categories of IoT devices. For instances, the "entertainment"-focused devices are perceived to share user's personal information in above 80% of cases, which is less than 30% for the devices in "pets" category.

Table 2 presents the matches and mismatches between participants' perceptions and the privacy policy of IoT devices in terms of information sharing, where a 'No-Yes' mismatch is considered to be the most critical one from the perspective of user's privacy preservation (see §3.1 for further details). Considering all data types[3], we found most 'No-Yes' mismatch for the IoT devices in "pets" category, followed by the devices in "toys & games", "entertainment", "smart homes", and "health & exercise". Such mismatches also vary across different categories of IoT devices with respect to information type. For example, we found a 54.84% 'No-Yes' mismatch for the devices in 'pets' category, which is 10% for "health & exercise"-focused devices.

As we asked participants about the reasons of information sharing (with third-party entities) by an IoT device, they mentioned about financial and business gain in about half of the cases. One of our participants said, "*I feel like most companies share whatever they can, so that they can make money.*" Some par-

[3] While considering all data types, the calculations of match and mismatch present a lower limit for the devices in "toys & games" and "pets" category, since some information are unavailable in their privacy policy (see 'NA' in Table 1 and 2).

Information Type	(Mis)Match	Health & Exercise	Entertainment	Smart Homes	Toys & Games	Pets
Personal	Yes-Yes	1.11%	26.98%	25.93%	56.48%	23.53%
	No-No	35.56%	30.16%	18.52%	3.70%	0.00%
	Yes-No	57.78%	22.22%	32.59%	12.96%	23.53%
	No-Yes	5.56%	20.63%	22.96%	26.85%	52.94%
Contact	Yes-Yes	3.33%	24.60%	24.62%	34.26%	22.58%
	No-No	48.89%	37.30%	26.15%	10.19%	0.00%
	Yes-No	37.78%	15.08%	20.00%	6.48%	22.58%
	No-Yes	10.00%	23.02%	29.23%	49.07%	54.84%
Financial	Yes-Yes	1.67%	8.33%	9.09%	7.14%	0.00%
	No-No	60.00%	63.10%	42.86%	47.62%	0.00%
	Yes-No	10.00%	15.48%	32.47%	9.52%	0.00%
	No-Yes	28.33%	13.10%	15.58%	35.71%	100.00%
Health	Yes-Yes	0.00%	0.00%	0.00%	*NA	*NA
	No-No	43.33%	80.95%	88.57%		
	Yes-No	56.67%	19.05%	11.43%		
	No-Yes	0.00%	0.00%	0.00%		
Location	Yes-Yes	0.00%	19.61%	18.60%	15.38%	12.00%
	No-No	33.33%	33.33%	32.56%	15.38%	16.00%
	Yes-No	66.67%	31.37%	32.56%	61.54%	20.00%
	No-Yes	0.00%	15.69%	16.28%	7.69%	52.00%
Media	Yes-Yes	0.00%	4.76%	10.94%	12.96%	0.00%
	No-No	81.67%	53.57%	53.13%	27.78%	0.00%
	Yes-No	18.33%	25.00%	6.25%	27.78%	0.00%
	No-Yes	0.00%	16.67%	29.69%	31.48%	0.00%
Connected Device	Yes-Yes	0.00%	7.14%	0.00%	*NA	*NA
	No-No	66.67%	54.76%	83.33%		
	Yes-No	33.33%	23.81%	11.11%		
	No-Yes	0.00%	14.29%	5.56%		
Online Social Media	Yes-Yes	0.00%	4.76%	0.00%	16.67%	0.00%
	No-No	70.00%	59.52%	80.56%	0.00%	0.00%
	Yes-No	30.00%	19.05%	11.11%	0.00%	0.00%
	No-Yes	0.00%	16.67%	8.33%	83.33%	100.00%
IoT Device Usage	Yes-Yes	0.00%	42.86%	31.91%	17.86%	10.00%
	No-No	23.33%	2.38%	29.79%	14.29%	0.00%
	Yes-No	76.67%	11.90%	10.64%	42.86%	10.00%
	No-Yes	0.00%	42.86%	27.66%	25.00%	80.00%

Table 2. Match/Mismatch between Participants' Perceptions and Privacy Policy: Data Sharing by IoT Devices [*NA: Information is not available in privacy policy]

ticipants perceive that information sharing with third-party entities are required for improving the functionality of an IoT device.

3.3 Security and Privacy Features of IoT Devices

A majority of participants perceive that the IoT devices in "toys & games", "pets", "entertainment", and "health & exercise" category encrypt user information in process of communication and storage (see Figure 3). Here, the devices in "toys & games" category are perceived by most of the participants encrypting their information as compared to the devices in other categories. As compared to other categories of IoT devices, the ones in "smart homes" category are perceived by the least number of participants offering security and privacy features.

Table 3 presents the matches and mismatches between participants' perceptions and the practices of IoT devices in protecting user information. Here, we consider a 'Yes-No' mismatch as the most critical one from the perspective of user's security and privacy preservation, where a user believes that an IoT device adopts a secure strategy (e.g., encryption) for information protection, although it does not adopt that strategy as noted in its privacy policy. For instance, we

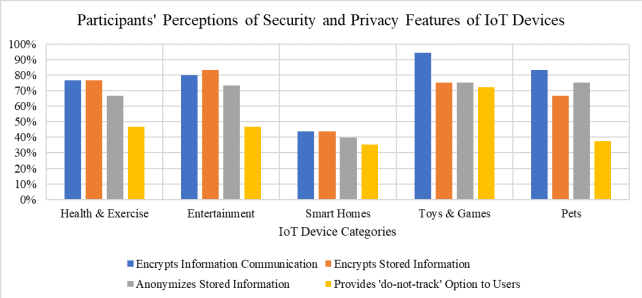

Fig. 3. Participants' Perceptions of Security and Privacy Features of IoT Devices

found a 'Yes-No' mismatch in 56.67% of cases for the devices in "health & exercise" category in terms of encrypting user data during storage. That means, in above half of the cases, participants had misconceptions about the secure storage of their information by the devices in "health & exercise" category. A majority of participants perceive that the devices in "pets" category encrypt their information during storage (see Figure 3), however, the privacy policy of these devices do not mention about their security-preserving steps during storage process. In these cases, we could not compare users' perceptions with the privacy policy of IoT devices.

4 Discussion

Our study reveals the mismatches between users' perceptions and the data practices stated in the privacy policy of IoT devices. We identified the misconceptions of participants that could potentially impact their privacy behavior. In many cases, participants believe that their information, including financial and health data are not collected by an IoT device, although those information are collected and shared (with third-party entities) by that device. Also, many participants

Security / Privacy Feature	(Mis)Match	Health & Exercise	Entertainment	Smart Homes	Toys & Games	Pets
Encrypts Information Communicated	Yes-Yes	53.33%	45.24%	35.71%	73.33%	77.78%
	No-No	16.67%	2.38%	10.71%	0.00%	0.00%
	Yes-No	23.33%	11.90%	3.57%	20.00%	0.00%
	No-Yes	6.67%	40.48%	50.00%	6.67%	22.22%
Encrypts Stored Information	Yes-Yes	20.00%	47.62%	33.93%	60.00%	*NA
	No-No	23.33%	2.38%	8.93%	3.33%	
	Yes-No	56.67%	11.90%	5.36%	16.67%	
	No-Yes	0.00%	38.10%	51.79%	20.00%	
Anonymizes Stored Information	Yes-Yes	0.00%	11.90%	13.11%	*NA	*NA
	No-No	33.33%	45.24%	39.34%		
	Yes-No	66.67%	40.48%	21.31%		
	No-Yes	0.00%	2.38%	26.23%		
Offers 'Do-not-Track' Option	Yes-Yes	3.33%	19.05%	33.33%	*NA	*NA
	No-No	36.67%	28.57%	16.67%		
	Yes-No	43.33%	14.29%	33.33%		
	No-Yes	16.67%	38.10%	16.67%		

Table 3. Match/Mismatch between Participants' Perceptions and Privacy Policy: Security and Privacy Features of IoT Devices [*NA: Information is not available in privacy policy]

believe that IoT devices protect their information through secure communication and storage, where we identified the mismatches between users' perceptions and actual practices. Such misconceptions could contribute to users' optimism bias [1], where they consider the risks of cyber attacks and information breach as 'distant harms'. As a result, they possess a false sense of security, lack interest and motivation to learn about secure behavior, and fail to take adequate steps to protect their information [1, 7].

The privacy notice often fails to help users with making an informed privacy decision due to its excessive length, complicated language, or poor visualization [6]. As recommended in prior studies [11, 6], a privacy notice should preserve the simplicity, brevity, and clarity in design for being understandable to general users. Our findings unpack the misconceptions of users about the data practices of IoT devices. The future research should build upon these results, and conduct further studies if needed, to design simplified privacy notice by highlighting the unexpected data practices, so that users could focus on the privacy aspects they are less informed about. We note that there is no 'one-size-fits-all' solution in this regard, as shown in our study that users' mismatched privacy perceptions vary across device category and information type. So, we recommend to consider each IoT device and information type individually, to identify users' privacy misconceptions and highlight that in a privacy notice to help them with protecting their privacy preferences.

As shown in a recent study [2], users' privacy perceptions of IoT technology could affect their adoption and purchase behavior, where their perceptions are rarely formed through the understanding of privacy policy. So, the design of a simplified and usable privacy notice is important not only for general users, but also for the organizations in IoT business; further emphasized by the findings from our study. We identified instances where participants perceive that a device collects and shares their information, although according to its privacy policy, the device does not collect that information (see 'Yes-No' mismatches in Table 1 and 2). We also found that some devices adopt data protection strategies, like encrypting user's information during communication and storage, while the participants do not perceive, those devices encrypt their information (see 'No-Yes' mismatches in Table 3). In this context, a usable and simplified privacy notice (see our recommendations in the above paragraph) would provide users with better understanding of the steps taken by organizations in IoT business to protect their customers' privacy interests.

We also recommend to extend our findings through further studies, in order to design usable and effective training materials (e.g., videos, comics, infographics) to raise the privacy awareness of people, where they should be informed about privacy misconceptions and unexpected data practices related to current technologies, including IoT.

5 Limitations and Conclusion

Our sample size is relatively small, where most of our participants were young and university-educated. Thus, our findings may not be generalizable to the en-

tire population. Our selection of IoT devices may not be not fully representative. As our analysis involves comparing user's perceptions with data practices stated in the privacy policy of IoT devices, the devices with better clarity in privacy policy were considered with higher priority in our selection. In this case, different selection criteria might yield varying lists of IoT devices. Despite these limitations, our study provides valuable insights into the mismatches between user's perceptions and the privacy policy of IoT devices in terms of data collection, sharing, and protection. In our future work, we would extend the findings from this study through a large-scale online survey, and leverage our results towards the design of simplified and usable privacy notice for IoT devices.

References

1. Davinson, N., Sillence, E.: Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions. International Journal of Human-Computer Studies **72**(2), 154–168 (2014)
2. 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. p. 534. ACM (2019)
3. Kaplan, D.: Majority of americans have an IoT device - and they're open to advertising (December 15, 2016), https://geomarketing.com/majority-of-americans-have-an-iot-device
4. Lau, J., Zimmerman, B., Schaub, F.: Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. In: Proceedings of the ACM on Human-Computer Interaction. pp. 1–31 (2018)
5. 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)
6. Mcdonald, A.M., Reeder, R.W., Kelley, P.G., Cranor, L.F.: A comparative study of online privacy policies and formats. In: International Symposium on Privacy Enhancing Technologies. pp. 37–55. Springer (2009)
7. Naeini, P.E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L.F., Sadeh, N.: Privacy expectations and preferences in an IoT world. In: Thirteenth Symposium on Usable Privacy and Security. pp. 399–412 (2017)
8. Page, X., Bahirat, P., Safi, M.I., Knijnenburg, B.P., Wisniewski, P.: The internet of what? understanding differences in perceptions and adoption for the internet of things. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. **2**(4) (2018)
9. Patel, K.K., Patel, S.M., et al.: Internet of things-IoT: definition, characteristics, architecture, enabling technologies, application & future challenges. International journal of engineering science and computing **6**(5) (2016)
10. Rao, A., Schaub, F., Sadeh, N., Acquisti, A., Kang, R.: Expecting the unexpected: Understanding mismatched privacy expectations online. In: Twelfth Symposium on Usable Privacy and Security. pp. 77–96 (2016)
11. Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F.: A design space for effective privacy notices. In: Eleventh Symposium On Usable Privacy and Security. pp. 1–17 (2015)
12. Zeng, E., Mare, S., Roesner, F.: End user security and privacy concerns with smart homes. In: Thirteenth Symposium on Usable Privacy and Security. pp. 65–80 (2017)

Appendix

Device Category	IoT Devices
Health & Exercise	Hidrate Spark 2.0 Water Bottle Peloton Bike Fitbit Charge 3 Fitness Tracker Athena Safety Wearable Samsung Gear Sport
Entertainment	Bose QuietComfort 35 II Google Pixel Buds PS4 Roku Streaming Players Apple TV
Smart Homes	Sonos One Mycroft Mark 1 Nest Learning Thermostat Amazon Echo Dot Amazon Cloud Cam Behmor Brewer Coffee Maker Philips Hue Smart Light Kit SmartThings Outlet
Toys and Games	EVO Robot Sphero Mini DJI Spark Selfie Drone CogniToys Dino Dot Creativity Kit Amazon Fire HD Kids Edition
Pets	Tractive 3GS Pet Tracker Tile Mate PetNet Smart Feeder Petzi Treat Cam

Table 4. List of IoT Devices Selected for the Study