8-12-2021

# A Look into User's Privacy Perceptions and Data Practices of IoT Devices

Mahdi Nasrullah Al-Ameen
*Utah State University*, mahdi.al-ameen@usu.edu

Apoorva Chauhan
*University of Waterloo*, apoorva.chauhan@uwaterloo.ca

M.A. Manazir Ahsan
*Utah State University*, manazir.ahsan@aggiemail.usu.edu

Huzeyfe Kocabas
*Utah State University*, huzeyfe.kocabas@aggiemail.usu.edu



## Recommended Citation

Al-Ameen, M.N., Chauhan, A., Ahsan, M.A.M. and Kocabas, H. (2021), "A look into user's privacy perceptions and data practices of IoT devices", Information and Computer Security. https://doi.org/10.1108/ICS-08-2020-0134

# A Look into User's Privacy Perceptions and Data Practices of IoT Devices

Mahdi Nasrullah Al-Ameen*, Apoorva Chauhan†, M A Manazir Ahsan*, Huzeyfe Kocabas*
*Utah State University, Logan, UT, USA
†University of Waterloo, Waterloo, Ontario, Canada
mahdi.al-ameen@usu.edu, apoorva.chauhan@uwaterloo.ca,
manazir.ahsan@aggiemail.usu.edu, huzeyfe.kocabasn@aggiemail.usu.edu

***Abstract*—Purpose: 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. The prior research focused on identifying people's privacy preferences in different contexts of IoT usage, and their mental models of security threats. 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. We aim to identify these mismatched privacy perceptions in our work.**

**Methodology: We conducted a lab study with 42 participants, where we compared participants' perceptions with the data practices stated in the privacy policy of 28 IoT devices from different categories, including health & exercise, entertainment, smart homes, toys & games, and pets.**

**Findings: We identified the mismatched privacy perceptions of users in terms of data collection, sharing, protection, and storage period. Our findings revealed the mismatches between user's perceptions and the data practices of IoT devices for various types of information, including personal, contact, financial, heath, location, media, connected device, online social media, and IoT device usage.**

**Value: The findings from this study lead to our recommendations on designing simplified privacy notice by highlighting the unexpected data practices, which in turn, would contribute to the secure and privacy-preserving use of IoT devices.**

***Index Terms*—IoT; User Study; Mismatched Privacy Perceptions**

## I. Introduction

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 (Patel, Patel et al., 2016). 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 (Kaplan, 2016). Despite the increasing popularity and immense potential of IoT devices, security and privacy issues remain as major concerns (Emami-Naeini, Dixon, Agarwal and Cranor, 2019; Zeng, Mare and Roesner, 2017; Ziegeldorf, Morchon and Wehrle, 2014).

The prior study (Naeini, Bhagavatula, Habib, Degeling, Bauer, Cranor and Sadeh, 2017) 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 privacy and security threats in an IoT environment (Zeng et al., 2017; Malkin, Deatrick, Tong, Wijesekera, Egelman and Wagner, 2019), where users are found to trade their privacy for conveniences (Lau, Zimmerman and Schaub, 2018). In the landscape of privacy decision-making, people reported their interest to be notified about the data practices of IoT device (Naeini et al., 2017), 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 (Emami-Naeini et al., 2019).

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[1], 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 storage / retention period? How do their perceptions vary from the actual data practices of IoT devices?
- 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, storage period, and protection by IoT devices. Our analysis identifies the gaps between participants'

The article is published in Information & Computer Security. This is the author's copy of the accepted version. The final authenticated version is available online at https://doi.org/10.1108/ICS-08-2020-0134

[1]This article is an extension of our paper (Al-Ameen, Chauhan, Ahsan and Kocabas, 2020a), appeared in HAISA'20

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.

## II. Related Work

To protect user's digital privacy and security, the prior studies focused on studying the strategies of managing authentication secrets (Stobert and Biddle, 2018; Mayer and Volkamer, 2018; Kothari, Koppel, Blythe and Smith, 2017), investigating user's privacy needs and designing privacy-preserving technologies (Liu, Andersen, Schaub, Almuhimedi, Zhang, Sadeh, Agarwal and Acquisti, 2016; Al-Ameen, Tamanna, Nandy, Ahsan, Chandra and Ahmed, 2020b; Haque, Haque, Nandy, Chandra, Al-Ameen, Guha and Ahmed, 2020) improving the usability of security schemes (Al-Ameen and Wright, 2017; Biddle, Chiasson and Van Oorschot, 2012; Al-Ameen, Fatema, Wright and Scielzo, 2015), developing automated techniques to detect unauthorized access to user's accounts (King, Alhadidi and Cook, 2018), and building educational tools and warning systems (Alsharnouby, Alaca and Chiasson, 2015; Lastdrager, Gallardo, Hartel and Junger, 2017; Seng, Al-Ameen and Wright, 2018). With the increasing use of IoT devices, the research communities have started to focus on identifying the security and privacy vulnerabilities of users in an IoT environment, and developing usable technologies to address these issues. In this section, we briefly discuss the findings from recent studies on user's privacy and security in the landscape of Internet of Things (IoT).

The study of Naeini et al. (2017) investigated the privacy preferences of users in different scenarios of IoT usage. This vignette-based study (Naeini et al., 2017) reveals diverse privacy preferences of users, which are related to the contexts of using an IoT device. For instances, participants reported to be less comfortable with data collection in private places as compared to public settings, where they tend to allow data collection based on their perceived benefits (Naeini et al., 2017). The authors (Naeini et al., 2017) also found varying preferences of users in terms of the type of data collected by an IoT device, where participants reported less comfort with the collection of biometrics information as compared to the environmental data, e.g., room temperature.

The study of Zeng et al. (2017) examined the mental models, security and privacy concerns, and mitigation strategies of users who live in a smart home equipped with IoT devices. The findings from this study (Zeng et al., 2017) reveal the incomplete threat models and ad hoc mitigation strategies of users, influenced by their security practices for older technologies. The authors (Zeng et al., 2017) argue that the limited technical understanding of people often contributes to their incorrect mental model of security threats in an IoT environment. In a separate study, Geeng and Roesner (2019) examined the interaction of people in a multi-user smart home, where they found two categories of users for shared devices: smart home driver and passive user. Here, a smart home driver takes initiative to learn about and use smart devices, where a passive user adapts to device usage and rely on the smart home driver to control functionality and fix technical issues of the shared devices in a household (Geeng and Roesner, 2019).

The study of Page et al. (2018) unpacked the relation between people's perceptions and adoption of IoT technology. The authors (Page et al., 2018) divided the IoT users into two categories: "user-centric", who think that the IoT devices are to be controlled by users; and "agentic", who perceive that the control of IoT devices are to be negotiated between the machine and human. The study (Page et al., 2018) highlighted privacy concerns for the people coming from a user-centric perspective given that consumer-oriented IoT is currently moving towards the agentic view.

The prior studies (Malkin et al., 2019; Lau et al., 2018) examined people's privacy perceptions, concerns, and privacy-preserving behaviors around smart speakers, where Malkin et al. (2019) particularly focused on understanding user's beliefs and attitudes about the recordings that are made and shared by smart speakers. The authors (Malkin et al., 2019) 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 (Malkin et al., 2019). In a separate study, Lau et al. (2018) found that the privacy concerns of smart speaker users are impacted by different factors, including their incomplete mental models of privacy vulnerabilities and reliance on the socio-technical context in which a smart speaker resides. The authors (Lau et al., 2018) identified that users trade privacy for convenience with different levels of deliberation and privacy resignation, where the privacy control features of the smart speakers are rarely used because of their incompatibility with people's needs.

Users reported their interest to be notified about the data practices of IoT device (Naeini et al., 2017). 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 (Emami-Naeini et al., 2019). As reported in the study of Emami-Naeini et al. (2019), most of the participants did not consider the privacy and security issues prior to purchasing an IoT device. However, observing unexpected device behavior, and the knowledge gathered from media reports and social discussion later made them concerned about the security and privacy issues in an IoT environment (Emami-Naeini et al., 2019).

The overall findings from these studies indicate that there is a dearth in existing literature to understand the differences between people's perceptions and the actual data practices of IoT devices. We addressed this gap in our work through investigating users' perceptions and comparing that with the privacy policy of IoT devices from different categories.

## III. Methodology

We conduced individual study session with each participant in a lab setting. We recruited participants by sharing our study

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

TABLE I
LIST OF IOT DEVICES SELECTED FOR THE STUDY

information through email and online social media. Our study was approved by the Institutional Review Board (IRB) at Utah State University.

### A. Selection of IoT Devices

We selected 28 devices for our study (see Table I) 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.

### B. Types of Information

In light of prior work (Rao, Schaub, Sadeh, Acquisti and Kang, 2016) 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).

### C. 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 how long an IoT device keeps user's information stored, and 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.

### D. Analysis

We went through the privacy policy of each IoT device, and compared that with participants' perceptions in terms of information collection, sharing, protection, and storage period. 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.

## IV. RESULTS

### A. Participants

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%),

[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)

| 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 II
MATCH/MISMATCH BETWEEN PARTICIPANTS' PERCEPTIONS AND PRIVACY POLICY: DATA COLLECTION BY IOT DEVICES [*NA: INFORMATION IS NOT AVAILABLE IN PRIVACY POLICY]

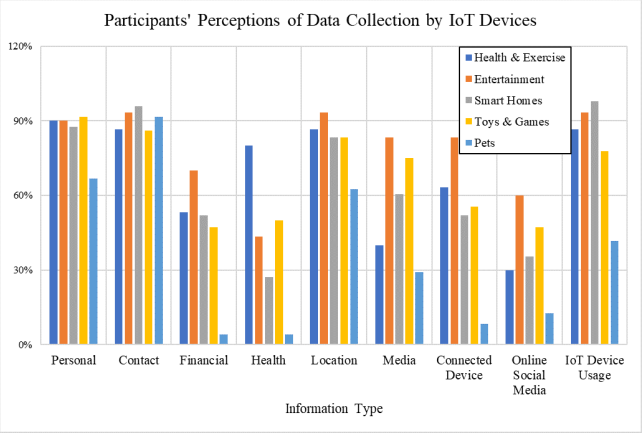


Fig. 1. Participants' Perceptions of Data Collection by IoT Devices

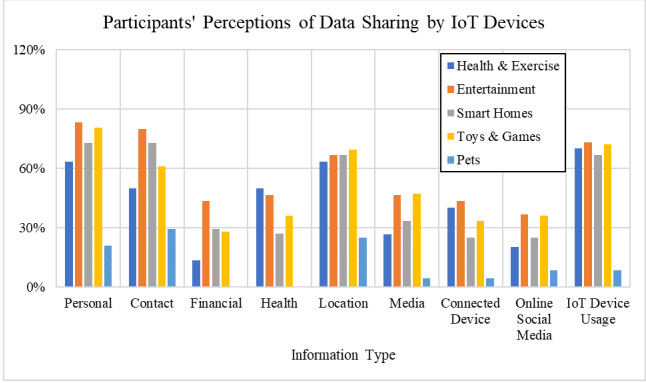


Fig. 2. Participants' Perceptions of Data Sharing by IoT Devices

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.

Below, we report the findings from this study.

| 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 | Yes-Yes | 0.00% | 7.14% | 0.00% | *NA | *NA |
| Device | 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 | Yes-Yes | 0.00% | 4.76% | 0.00% | 16.67% | 0.00% |
| Social Media | 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 | Yes-Yes | 0.00% | 42.86% | 31.91% | 17.86% | 10.00% |
| Usage | 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 III
MATCH/MISMATCH BETWEEN PARTICIPANTS' PERCEPTIONS AND PRIVACY POLICY: DATA SHARING BY IOT DEVICES [*NA: INFORMATION IS NOT AVAILABLE IN PRIVACY POLICY]

### *B. 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 II 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 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.

### C. 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 III 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 §IV-B 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 participants perceive that information sharing with third-party entities are required for improving the functionality of an IoT device.

### D. Data Storage by IoT Devices

Figure 3 illustrates participants' perceptions of how long an IoT device stores the information collected from a user, where 80% of participants perceive that "entertainment"-focused IoT devices store user's information *forever*. The IoT devices in "health & exercise" and "smart homes" category are perceived to store user's information *forever* by above 50% of participants. According to 30% of participants, "toys & games"-focused IoT devices retain user's information for *less than one year*, where above one-third of participants perceive that

[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 II and III)

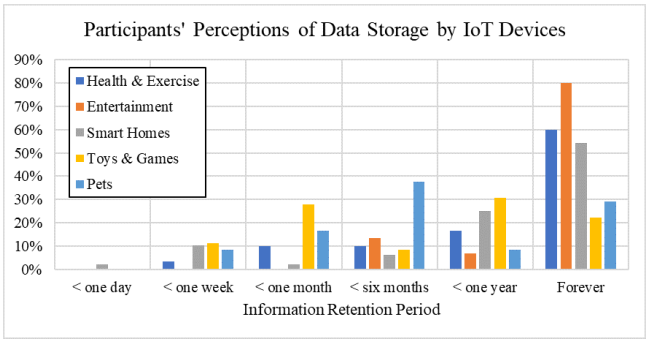


Fig. 3. Participants' Perceptions of Data Storage by IoT Devices

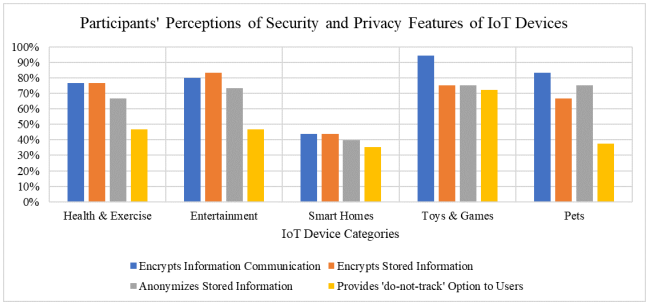


Fig. 4. Participants' Perceptions of Security and Privacy Features of IoT Devices

IoT devices in "pets" category keep user's information stored for *less than six months*. Almost no participants perceive that an IoT device stores user's information for *less than a day*.

As we compared participants' perceptions with the privacy policy of IoT devices (see Table V in Appendix), we found 83.3% 'No-Yes' mismatch for "toys & games"-focused IoT devices in terms of whether user's information is stored *forever*. That means, in 83.3% of cases, the IoT devices in "toys & games" category store user's information *forever* although our participants do not perceive so. We found most 'Yes-No' mismatch for the IoT devices in "smart homes" (58.33%) category, followed by the devices in "entertainment" (47.62%) and "pets" (33.33%) category in terms of whether user's information is stored *forever*.

### E. 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 4). 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 IV 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

| 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 IV
MATCH/MISMATCH BETWEEN PARTICIPANTS' PERCEPTIONS AND PRIVACY POLICY: SECURITY AND PRIVACY FEATURES OF IOT DEVICES [*NA: INFORMATION IS NOT AVAILABLE IN PRIVACY POLICY]

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 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 4), 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.

## V. DISCUSSION

In this section, we shed light on the implications of our findings, followed by a discussion on the the limitation of this study.

### A. Optimism Bias

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 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 (Davinson and Sillence, 2014), 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 (Davinson and Sillence, 2014; Naeini et al., 2017).

### B. Unexpected Data Practices

The privacy notice often fails to help users with making an informed privacy decision due to its excessive length, complicated language, or poor visualization (Mcdonald, Reeder, Kelley and Cranor, 2009; Gluck, Schaub, Friedman, Habib, Sadeh, Cranor and Agarwal, 2016; Cate, 2010). As recommended in prior studies (Schaub, Balebako, Durity and Cranor, 2015; Kelley, Cesca, Bresee and Cranor, 2010; Knijnenburg and Cherry, 2016), 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 unexpected data practices in a privacy notice to help them with protecting their privacy preferences. We also encourage 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.

### C. IoT Adoption

As shown in a recent study (Emami-Naeini et al., 2019), 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 II and III). 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 IV). 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, which in turn, would contribute towards the adoption of IoT devices by general users.

### *D. Limitations*

Our sample size is relatively small, where we focused only on a U.S. based population. We did not capture several variables that could impact user's privacy perceptions and awareness, e.g., their socio-economic status, where users with lower socio-economic status engage in fewer privacy and security behaviors (Redmiles, Kross and Mazurek, 2016). This means our results may not be generalizable to the entire population, and the variables that we did not study may moderate our findings.

Our study is based in urban areas. We note that users' privacy perceptions might be different in rural areas. Since users' security and privacy perceptions are positively influenced by their knowledge and technical efficacy (Ion, Reeder and Consolvo, 2015; Mazurek, Komanduri, Vidas, Bauer, Christin, Cranor, Kelley, Shay and Ur, 2013; Seng et al., 2018), and the literacy rate is generally higher in urban areas as compared to that in rural areas (of Statistics, 2008), we speculate that the privacy perceptions of users reported in this paper represent an upper bound. That means, the mismatches between users' privacy perceptions and the privacy policy of IoT devices might be higher for the less-educated population than the results reported in this paper.

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. We acknowledge that the different selection criteria might yield varying lists of IoT devices. In this paper, keeping consistent with the methodology suggested in prior work (Rao et al., 2016), we consider the privacy policy of a device to be representative of its data collection practices. Going further to identify the discrepancies between a device's privacy policy and its actual data collection practices is thus beyond the scope of this work. Future research to investigate such discrepancies would be valuable.

This study is conducted at a specific moment in time, and user's privacy perceptions and behaviors are ever evolving. So, the privacy perceptions reported in this paper will continue to shift over time. Despite this limitation, we believe that our findings are useful as a lens to investigate the changes in user's privacy perceptions of IoT devices in future studies.

## VI. Conclusion

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, protection, and storage period. In our future work, we would extend the findings from this study through the large-scale online survey, and leverage our results towards the design of simplified and usable privacy notice for IoT devices. We encourage Usable Security, Privacy, and HCI research communities to extend the findings of this work in the contexts of different domains and field sites, and use other methods as well, if required.

## References


Al-Ameen, M.N., Chauhan, A., Ahsan, M.A.M., Kocabas, H., 2020a. "most companies share whatever they can to make money!": Comparing user's perceptions with the data practices of iot devices, in: International Symposium on Human Aspects of Information Security and Assurance, Springer. pp. 329–340.

Al-Ameen, M.N., Fatema, K., Wright, M., Scielzo, S., 2015. The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords, in: Symposium On Usable Privacy and Security, pp. 185–196.

Al-Ameen, M.N., Tamanna, T., Nandy, S., Ahsan, M.M., Chandra, P., Ahmed, S.I., 2020b. We don't give a second thought before providing our information: Understanding users' perceptions of information collection by apps in urban bangladesh, in: Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies, pp. 32–43.

Al-Ameen, M.N., Wright, M., 2017. Exploring the potential of geopass: A geographic location-password scheme. Interacting with Computers 29, 605–627.

Alsharnouby, M., Alaca, F., Chiasson, S., 2015. Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies 82, 69–82.

Biddle, R., Chiasson, S., Van Oorschot, P.C., 2012. Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR) 44, 1–41.

Cate, F.H., 2010. The limits of notice and choice. IEEE Security & Privacy 8, 59–62.

Davinson, N., Sillence, E., 2014. 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, 154–168.

Emami-Naeini, P., Dixon, H., Agarwal, Y., Cranor, L.F., 2019. Exploring how privacy and security factor into iot device purchase behavior, in: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, ACM. p. 534.

Geeng, C., Roesner, F., 2019. Who's in control? interactions in multi-user smart homes, in: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery. p. 1–13.

Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L.F., Agarwal, Y., 2016. How short is too short? implications of length and framing on the effectiveness of privacy notices, in: Twelfth Symposium on Usable Privacy and Security, pp. 321–340.

Haque, S.T., Haque, M.R., Nandy, S., Chandra, P., Al-Ameen, M.N., Guha, S., Ahmed, S.I., 2020. Privacy vulnerabilities in public digital service centers in dhaka, bangladesh, in: Proceedings of the 2020 International Conference on Information and Communication Technologies and Development, pp. 1–12.

Ion, I., Reeder, R., Consolvo, S., 2015. "... no one can hack my mind": Comparing expert and non-expert security practices, in: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), pp. 327–346.

Kaplan, D., 2016. Majority of americans have an iot device - and they're open to advertising. URL: https://geomarketing.com/majority-of-americans-have-an-iot-device.

Kelley, P.G., Cesca, L., Bresee, J., Cranor, L.F., 2010. Standardizing privacy notices: an online study of the nutrition label approach, in: Proceedings of the SIGCHI Conference on Human factors in Computing Systems, ACM. pp. 1573–1582.

King, M., Alhadidi, D., Cook, P., 2018. Text-based detection of unauthorized users of social media accounts, in: Canadian Conference on Artificial Intelligence, Springer. pp. 292–297.

Knijnenburg, B., Cherry, D., 2016. Comics as a medium for privacy notices, in: Twelfth Symposium on Usable Privacy and Security.

Kothari, V., Koppel, R., Blythe, J., Smith, S., 2017. Password logbooks and what their amazon reviews reveal about their users' motivations, beliefs, and behaviors, in: European Workshop on Usable Security.

Lastdrager, E., Gallardo, I.C., Hartel, P., Junger, M., 2017. How effective is anti-phishing training for children?, in: Symposium on Usable Privacy and Security, pp. 229–239.

Lau, J., Zimmerman, B., Schaub, F., 2018. 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.

Liu, B., Andersen, M.S., Schaub, F., Almuhimedi, H., Zhang, S.A., Sadeh, N., Agarwal, Y., Acquisti, A., 2016. Follow my recommendations: A personalized privacy assistant for mobile app permissions, in: Twelfth Symposium on Usable Privacy and Security (SOUPS), pp. 27–41.

Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., Wagner, D., 2019. Privacy attitudes of smart speaker users. Proceedings on Privacy Enhancing Technologies 2019, 250–271.

Mayer, P., Volkamer, M., 2018. Addressing misconceptions about password security effectively, in: Workshop on Socio-Technical Aspects in Security and Trust, pp. 16–27.

Mazurek, M.L., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L.F., Kelley, P.G., Shay, R., Ur, B., 2013. Measuring password guessability for an entire university, in: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, ACM. pp. 173–186.

Mcdonald, A.M., Reeder, R.W., Kelley, P.G., Cranor, L.F., 2009. A comparative study of online privacy policies and formats, in: International Symposium on Privacy Enhancing Technologies, Springer. pp. 37–55.

Naeini, P.E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L.F., Sadeh, N., 2017. Privacy expectations and preferences in an iot world, in: Thirteenth Symposium on Usable Privacy and Security, pp. 399–412.

Page, X., Bahirat, P., Safi, M.I., Knijnenburg, B.P., Wisniewski, P., 2018. The internet of what? understanding differences in perceptions and adoption for the internet of things. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2.

Patel, K.K., Patel, S.M., et al., 2016. Internet of things-iot: definition, characteristics, architecture, enabling technologies, application & future challenges. International journal of engineering science and computing 6.

Rao, A., Schaub, F., Sadeh, N., Acquisti, A., Kang, R., 2016. Expecting the unexpected: Understanding mismatched privacy expectations online, in: Twelfth Symposium on Usable Privacy and Security, pp. 77–96.

Redmiles, E.M., Kross, S., Mazurek, M.L., 2016. How i learned to be secure: A census-representative survey of security advice sources and behavior, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM. pp. 666–677.

Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F., 2015. A design space for effective privacy notices, in: Eleventh Symposium On Usable Privacy and Security, pp. 1–17.

Seng, S., Al-Ameen, M.N., Wright, M., 2018. Understanding users' decision of clicking on posts in facebook with implications for phishing, in: Workshop on Technology and Consumer Protection (ConPro).

of Statistics, B.B., 2008. Literacy assessment survey 2008. http://www.un-bd.org/Docs/Publication/Bangladesh_Literacy_Assessment_Survey_2008.Pdf.

Stobert, E., Biddle, R., 2018. The password life cycle. ACM Transactions on Privacy and Security 21, 1–32.

Zeng, E., Mare, S., Roesner, F., 2017. End user security and privacy concerns with smart homes, in: Thirteenth Symposium on Usable Privacy and Security, pp. 65–80.

Ziegeldorf, J.H., Morchon, O.G., Wehrle, K., 2014. Privacy in the internet of things: threats and challenges. Security and Communication Networks 7, 2728–2742.

## APPENDIX

See next page.

| (Mis)Match | Health & Exercise | Entertainment | Smart Homes | Toys & Games | Pets |
|---|---|---|---|---|---|
| YES-YES | 60.00% | 9.52% | 0.00% | 16.67% | 0.00% |
| NO-NO | 0.00% | 38.10% | 41.67% | 0.00% | 66.67% |
| YES-NO | 0.00% | 47.62% | 58.33% | 0.00% | 33.33% |
| NO-YES | 40.00% | 4.76% | 0.00% | 83.33% | 0.00% |

TABLE V
MATCH/MISMATCH BETWEEN PARTICIPANTS' PERCEPTIONS AND PRIVACY POLICY OF IOT DEVICES: DATA STORAGE PERIOD - 'FOREVER'