Life-Long Privacy in the IoT? Measuring Privacy Attitudes Throughout the Life-Cycle of IoT Devices

Alexandr Railean, Delphine Reinhardt

Life-long Privacy in the IoT? Measuring Privacy Attitudes Throughout the Life-cycle of IoT Devices

Alexandr Railean[1,2](✉) 0000-0002-7472-2108 and Delphine Reinhardt[2] 0000-0001-6802-2108

[1] Unabhängiges Landeszentrum für Datenschutz, Kiel, Germany
arailean@datenschutzzentrum.de
[2] University of Bonn and Fraunhofer FKIE Bonn, Germany
delphine.reinhardt@cs.uni-bonn.de

Abstract. The novelty of the Internet of Things (IoT) as a trend has not given society sufficient time to establish a clear view of what IoT is and how it operates. As such, people are likely to be unaware of the privacy implications, thus creating a gap between the belief of what a device does and its actual behaviour. The responses collected in our online survey indicate that participants tend to see IoT as computer-like devices, rather than appliances, though there are some important misconceptions about the way these devices function. We also find that privacy is a primary concern when it comes to IoT adoption. Nevertheless, participants have a propensity to keep using IoT devices even after they find out that the device abuses their trust. Finally, we provide recommendations to IoT vendors, to make their products more transparent in terms of privacy.

Keywords: Internet of Things, IoT, privacy, usability.

1 Introduction

The IoT is composed of *devices, sensors or actuators, that connect, communicate or transmit information with or between each other through the Internet* (adapted from [13]). It is rapidly growing, as the number of connected devices per person has increased from 1.84 to 3.3 between 2010 and 2016 [11, 26]. Many IoT devices, such as light bulbs, power switches, air quality monitors, or fitness trackers, are widely available. There is also strong support in the "do it yourself" community: there are 21,714 hits on Github.com, and 49,000 hits on Instructables.com when searching for the term "IoT". Moreover, some appliance manufacturers aim at increasing the share of their connected products. For instance, Samsung's CEO stated that all their products will be part of the IoT by 2020 [24]. Governments have also expressed interest in the IoT. For example, the Federal Trade Commission (FTC) issued a privacy and security guide

[6] for businesses involved in IoT development, while the European Commission is working on regulations that have provisions for IoT communications [23]. This indicates that IoT is on the path of becoming an indispensable part of our daily lives, based on the current attention of all involved parties, i.e., enterprises, governments, and end users.

However, such products may expose end users and product owners to privacy risks that can occur at the interplay of factors like resource-constrained hardware, poor usability, ubiquitous deployment or the availability of many pools of data. These factors can make the implementation of well-established privacy and security mechanisms difficult. Additionally, users may get little or no feedback about the data collected while interacting with an environment that lacks an interface (e.g. when sensors are seamlessly embedded into walls or furniture). A ubiquitous deployment means that insights about the users can be gathered in locations where they are not expecting data collection. Moreover, linking different data pools having information about the users can facilitate their identification, and hence lead to their deanonymization. For example, studies show that information about a person can be derived by correlating data from disparate sources, such as smartphone sensors [8, 16], social media [15] or online reviews [20]. At the same time, most people are not technically proficient [21], and even those who are often subvert their privacy [14]. This has been shown in the use of social media [5] or instant messengers [9].

This paper starts with a review of related work in Sec. 2. We then investigate whether the aforementioned patterns apply to IoT in Sec. 3, by means of an online questionnaire introduced in Sec. 4. The results, based on the answers of 110 participants, are shared in Sec. 5. The answers show that most participants are aware of privacy risks, though they are inclined to keep using a device that infringes on their privacy. Moreover, our results provide an understanding of the reasons behind the adoption of IoT devices by end users, and give a clearer picture of the attention our participants pay to privacy throughout the life-cycle of their IoT devices. We then test our hypotheses in Sec. 6. In Sec. 7 we discuss the results and limitations of our survey, as well as provide recommendations for IoT vendors. Sec. 8 concludes the paper and summarizes our findings. All the materials needed to replicate the survey are given in Appendix A.

2 Related Work

Naeini et al. explore people's preferences regarding IoT data collection and notifications of data collection in [19]. They found that the participants of their study were more open towards data collection in public settings, and less so when data collection occurs in a private environment, if it involves biometric data, or if the data will be stored for long periods of time. They also develop a model that can predict one's data-collection preferences based on three data-points. Other works examine IoT from a legal perspective, a definition of IoT privacy is given in [29], the paper identifies the possible privacy risks related to IoT. Peppet conducts another legal analysis in [22] and discusses how privacy is affected

by the difficulty of sensor data de-identification, thus questioning the distinction between personal data and other data. Another raised concern is that some IoT device vendors conflate the notion of "notice" with that of "consent", assuming that informing users about what a technology does is sufficient to indicate that use of technology implies consent (S_0, please note that the *statements* marked with S_n will be referred to in Sec. 7.2). The analysis also includes a comparison of the packages of several IoT devices with respect to privacy-related information, as well as their privacy policies. An extensive literature review and summary of IoT privacy issues is provided in [4, 7, 17]. Other works are focused on location privacy [10, 18], while [28] focuses on fitness trackers. Volkamer et al. discusses the importance of mental models formed by end-users and the role these models play in the trust and acceptance of new technologies in [27]. There are other papers that present IoT life-cycle models, however they take a data-centered approach, examining what happens to the personal data acquired and transmitted by IoT devices [18, 29]. Our work, on the other hand, takes a user-centered approach, focusing on the different stages of the relationship between users and their IoT devices.

3 Research Goals

To examine the participants' *privacy attitudes* and *user experience* in the context of IoT device ownership, we focus on the following *Research Questions* (RQ):

- RQ_1: What motivates potential users to acquire IoT devices?
- RQ_2: Would they continue using a device that infringes on their privacy?
- RQ_3: Are users aware of the extent to which IoT devices can interact with other equipment they own?

We then map the answers to the corresponding phases of the IoT device life-cycle (defined in Sec. 4), and look for user interface friction points that can potentially affect the privacy of end-users. This, in turn, enables us to suggest usability improvements and creates new research questions for the future.

The answers to the research questions help us test the following hypotheses (referred to as H), which are formulated on the basis of autoethnographic observations:

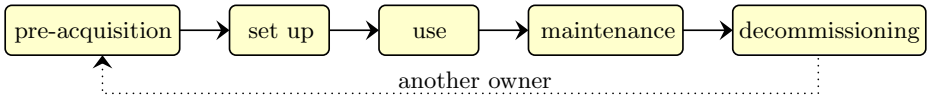
- H_1: When dealing with IoT devices, most users treat them as *appliances*, rather than *computers*.
- H_2: Users are inclined to keep IoT devices that infringe on their privacy, if those devices have a high *monetary value*.
- H_3: Users are inclined to keep IoT devices that infringe on their privacy, if those devices were *a gift from a close person*.

4 Methodology

To answer the questions and test the hypotheses, we designed an online questionnaire, which covers the phases of the IoT device life-cycle we consider to have an

impact on privacy: pre-acquisition, set-up, usage, maintenance, and decommissioning, as illustrated in Fig. 1. Note that we are not concerned with the factors that lead to decommissioning (e.g. resale, recycling, etc), we only focus on the privacy implications due to removal of IoT devices from service, regardless of the cause. In our questionnaire, we take a human-centered perspective and focus on what a person does with the device, rather than on what the device does with the data, in contrast to [18, 29]. We have especially phrased our questions in a way that should elicit what participants *think* about the device and what their *beliefs* about its behaviour are.

Fig. 1. IoT device lifecycle



4.1 Distribution and audience

We have invited our participants via word of mouth, mailing lists, social media, and survey sharing platforms. Because it appeals to a wide audience, we have particularly taken care that non-experts could understand the goal of our questionnaire. To this end, we have defined and detailed the terminology used and given concrete examples. The introduction also provided key details about how the collected data would be handled, i.e., full anonymity and no disclosure of individual answers.

In total, 193 participants have answered our online questionnaire. Among them, 110 participants have fully filled it out. We have therefore discarded the incomplete ones for computing the following results. The majority of our participants are male (57%), 5% preferred not to disclose their gender. The most represented age category is between 21 and 30 (52%), followed by 31 and 40 (28%), then by 41 and 50 (8%). 45% of the participants have a bachelor degree, 33% have a master degree, 8% have a secondary school level of education, 5% preferred not to disclose information about their education, while 3% have earned a doctorate degree. Geographically, most of our participants are from Eastern Europe (45%), followed by 31% from Western Europe and 14% from North America.

4.2 Self-selection bias

Since we have initiated the distribution of the survey, it is possible that the recruited participants fit a similar profile, thus biasing the sample. We have therefore asked the participants to indicate the different computer-related skills they have in question Q_{30} (see Appendix A). We then assign to each skill a

Table 1. Distribution of points for each considered computer-related skill (Q_{30})

Points	Skills	Points	Skills
2	play video games	5	type complex documents in word processors (e.g. macros, automatic indexes, dynamic fields)
2	view photos and watch videos	10	assemble computers or other electronics from components
2	browse the Internet and send emails	15	I know at least one programming language
2	use a word-processor to type documents		
5	set up email sorting filters		

number of points according to the distribution presented in Tab. 1. The total number of points obtained by a participant finally determines the category they belong to. We categorize participants with a total number of points below 8 as *novice*, between 8 and 20 as *medium*, and greater than 20 as *expert*. Our sample counts 55% rated as expert, 37% are medium and 7% are novice.

4.3 Priming concerns

To avoid priming participants into a privacy-oriented mindset, the topic of the survey has been announced as "IoT usability". There was no mention of the term "privacy" in the call for participation, e.g. *"You're invited to participate in an IoT usability survey"*. Additionally, privacy-themed questions and answer choices were uniformly distributed among other topics.

5 Results

Our results are based on the responses of 110 participants and are mapped to phases of our IoT lifecycle model. The first set of questions is aimed at all the participants, whether they own an IoT device or not. We have found that 41% of them do not own IoT devices, whereas the others own smart TVs (38%), smart watches (23%), fitness bracelets (18%), thermostats (12%) and voice assistants (12%) (multiple choices possible). 39% of the participants are planning to purchase new IoT devices in the next 6 months (74% of them already own an IoT device), 30% have no such plans (33% of them own an IoT device), while 27% are not sure about it (47% of them own an IoT device).

5.1 Pre-acquisition

We have then asked the participants to indicate, in a non-prioritized way, the "reasons to buy Internet-connected appliances" (Q_{21}). They have indicated 86 reasons in a free-text field, which we have clustered as follows: automation of routine tasks (38%), better remote control (31%), and new capabilities (31%). Being socially connected (16%) and health improvements (12%) were selected by fewer participants. On the other hand, the participants have given 109 reasons

Table 2. Desired IoT features (Q_{20})

Feature	%	Feature	%
ease of use	72	recommendations from friends and others	39
compatibility with my existing devices	66	stylish design	35
		availability of technical documentation	35
good brand reputation	48	certifications by authorities (e.g. TÜV, FCC)	20
low price	47		
clear privacy policy	46	other (please specify)	8

why they would not buy such appliances. The most represented concerns are privacy (34%), security (30%) and cost (12%). Some of the arguments supporting the latter concern being (a) interaction with IoT devices will consume their data plan and inflate the bill, (b) an insecure IoT device that can make purchases can be taken over, allowing hackers to order items for free, (c) the cost of IoT devices is usually greater, due to their novelty, not due to their actual benefits, and (d) these devices become obsolete very fast.

Tab. 2 shows what participants would be looking for, if they were purchasing an IoT device. The responses indicate that *convenience* plays a key role. 72% look for ease of use, while 66% seek compatibility with existing devices. We have also seen that privacy is not of particular importance, it ranked 46%, close to "good brand reputation" (48%) and "low price" (47%). Another important highlight is that certifications from organizations like Technischer Überwachungsverein (TÜV) or Federal Communications Commission (FCC) play little role in the choice of IoT devices. Such an attitude may be explained by a greater level of trust in product reviews published on the Internet, or by the fact that brand reputation is sufficient to decide which device to purchase.

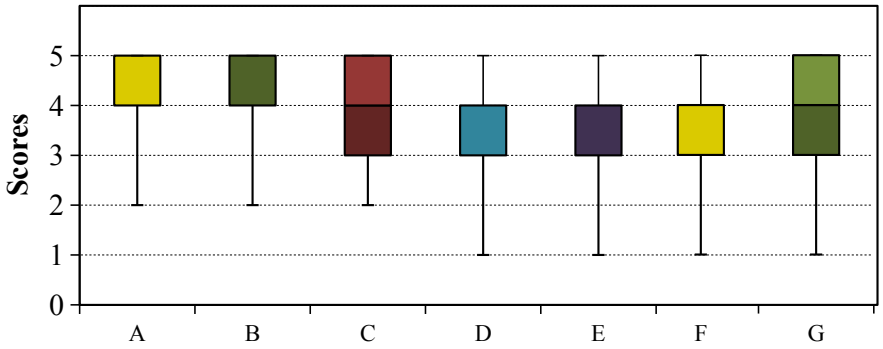
Other features mentioned in a free-text field by participants were (a) guaranteed updates period (2 mentions), (b) open hardware/software and firmware access (2 mentions), (c) good security record (3 mentions), (d) wide functionality and customizability (3 mentions). One participant specifically indicated that the privacy policy should be "SHORT and clear" (S_1).

To learn the reasons why our participants chose to acquire their IoT devices, we have asked them to "[...] indicate the benefits of connected devices that appeal to [them] personally" (Q_{23}). Although this question is similar to Q_{21}, it enables us to differentiate between benefits participants have heard of in principle, and benefits that they themselves are looking for. The results in Tab. 3 show that the responses are similar, the most common and least common reasons follow the same distribution, with a difference in health improvements. 12% chose it as a reason to buy IoT devices, 30% indicated that it is what appealed to them in particular. This observation leads us to the conclusion that in our sample, participants acquire IoT hardware for practical reasons, rather than because it is fashionable to do so.

Table 3. IoT benefits that appeal to you personally (Q_{23})

Option	%	Option	%
automation of routine tasks	59	health improvements	30
better remote control	55	being connected to friends or family in a new way	26
new capabilities	52	being connected to strangers or society in general	10
energy saving	49	I don't know	10
easier data management	34		

Fig. 2. Extrema and quartiles of the valid participants' answers to Q_6 based on the following criteria: plugging it in and connecting the cables (**A**, valid answers: 49), connecting it to [a] network or the Internet (**B**, 48), configuring the device settings (**C**, 50), accompanying documentation (**D**, 46), online materials (e.g. product site, support services) (**E**, 45), accompanying smartphone application (**F**, 43), resetting to default settings and wiping all data (**G**, 37). Invalid answers correspond to participants who skipped the questions or chose not to answer.

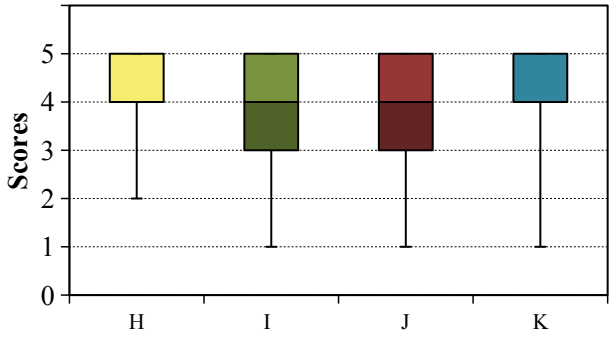


5.2 Set up

In this and subsequent sections, we provide the results related to questions that involved participants who own IoT devices. Note that these questions were not displayed to those who indicated that they do not own an IoT device. Therefore the percentages shown are relative to a total of 65 participants. In Q_6, we have asked participants "how satisfied [they] are with the process of using the device 'brand'?", the answers are expressed on a 5-point Likert scale, ranging from "very dissatisfied" (1) to "very satisfied" (5), based on several criteria in Fig. 2.

We have found that "satisfied" and "very satisfied" are the most common answers to all the questions, except when it comes to the level of satisfaction with the accompanying documentation, where 42% chose the "neutral" option. A possible explanation is that the manual was never consulted due to lack of need, preference, or lack of interest. Lack of need can be the result of a successful configuration based solely on the clarity of the interface, or the technical experience of the end user. It can also be explained by the fact that the majority of participants rated "online materials (e.g. site, support services)" as "satisfying",

Fig. 3. Extrema and quartiles of the valid participants' answers to Q_9 based on the following criteria: configuring the device is easy (**H**, valid answers: 55), configuring it via a smartphone app is easy (**I**, 54), configuring it via a web-interface is easy (**J**, 54), set it up without reading the manual (**K**, 53).



which could indicate that whatever questions they had were addressed online, as such materials are easier or faster to search.

We have further probed this matter by asking participants "when it comes to configuring [the IoT device], how much do [they] agree with the following statements" in Q_9, and find that 71% agreed and strongly agreed to being able to set up and configure their device without reading the manual (Fig. 3). This supports the assumption that *lack of need* is what leads to the documentation being neglected. Such a level of success can have an undesired effect: satisfied end-users can stop tinkering with the device as soon as they accomplish their primary goals, thus missing potentially critical security and privacy tips the documentation could offer. We conclude that important privacy-related controls should be incorporated into the initial setup procedure, to ensure that end-users make informed privacy-related decisions (S_2).

5.3 Usage

When asked about continued use of an IoT device that infringes on the owner's privacy (Q_{24}), two of the top three reasons are related to the monetary value of the product, "it was an expensive purchase" and "it is difficult to return it or get a refund" got a combined score of 53%. In contrast, options related to family values are the least convincing reasons to keep it (14%). Other mentioned reasons were: (a) if it provides a unique function, (b) if it is crucial for daily use, or (c) if the infringement is negligible. *Convenience* is a major factor and its importance is often expressed throughout the collected answers. We have found that *entertainment* scores as high as health-related benefits (20%). This attitude resonates with the "dancing pigs" adage in computer security: *"The user's going to pick dancing pigs over security every time"* [25]. While studies [2] concluded that a better user interface helps people make wiser security-related decisions, those findings are not necessarily applicable in our context. Our question asks

Table 4. Which of these resources you think are exposed to the IoT device? (Q_7)

Option	%
my smartphone	69
other computers on my home network	40
communications between other devices in my home and the Internet	31
purpose-specific data (e.g. temp., humidity)	25
other devices on my home network (e.g. printer)	24
communications between devices in my home	22
other computers on the Internet	15
I don't know	11

Table 5. Who can interact with the IoT device? (Q_8)

Option	%
me	84
others in my household (e.g. family)	65
the manufacturer	38
hackers	35
the government	13
my neighbors	4

about a participant's choice *in principle*, which implies that this is a conscious decision they would make, no matter what the interface looked like.

When it comes to discarding an IoT device that infringes on the owner's privacy (Q_{25}), the reasons chosen by participants were: "ethical and moral convictions" (46%), "it is easy to get a refund" (45%), "installing custom firmware voids the warranty" (38%), and "it is easy to re-sell" (32%). Among the reasons indicated in the free-text field, 2 participants mentioned that the decision depends on the magnitude of the infringement.

To get a better understanding of what IoT device owners think about the capabilities of their hardware, we have asked them to indicate "the resources [they] think are exposed to the IoT device" in Q_7. The distribution of the answers is shown in Tab. 4. In 69% of the responses, it is expected that an IoT device can interact with a smartphone, presumably because that is how it is configured and controlled. Other options have been chosen by fewer than 40% of the participants.

We have asked participants "who, in [their] opinion, can use, or otherwise interact with IoT [devices] installed in your home?" in Q_8. The responses show that 35% of participants consider that hackers are capable of doing so, while 13% think the government can do that as well. These numbers indicate that the efforts of IoT device vendors are insufficient to establish trust and convince the participants that their product is secure (S_3), as it has been argued in [27]. We have also found, by means of a Kruskal-Wallis test, that expert participants are more likely ($\chi^2 = 6.857$, $p = 0.032$)[3] to consider that the government can access their IoT hardware. Note that they do not hold the same opinion about hackers. This may be explained by an expert's confidence in their own ability to secure a system from typical attackers. On the other hand, their awareness of the fact that state-level actors have much more resources may justify the belief that governments could conduct successful attacks, if they choose so. We have finally asked our participants whether they have "examined the privacy policy" of their IoT device in Q_{12}, and find that 22% have done so. To understand whether IoT

[3] When $p \leq 0.5$, it indicates that the results are not likely to be caused by chance, and that another set of participants would provide similar answers.

Table 6. Who should be responsible for updating IoT devices? (Q_5)

Option	%
the manufacturer	60
me, as the device owner	44
the seller of the device	15
a government agency	1
I don't know	1

Table 7. Is your IoT device running fully up-to-date firmware/software? (Q_3)

Option	%
N/A, I do not own any IoT device	41
yes, it updates itself automatically	27
yes, I update it manually	11
I don't know	10
no, but newer firmware is available	5

device adoption is a conscious decision, rather than a forced one (i.e. the IoT-enabled device was purchased because there was no "dumb" analog), we have asked our participants if they "own any appliances, the IoT capabilities of which are not used" (Q_{17}). 22% of the participants who own IoT devices always use the IoT features, 5% turn them off explicitly, 5% are aware of the features but are ignoring them, while 2% use various external means to disable them. Among the recorded means, we have found stickers over cameras (two mentions), positioning the device with the camera pointing down (one mention) and using a network router to limit the traffic of particular devices (one mention).

5.4 Maintenance

To understand the participants' attitudes towards software updates, we have asked them "do [they] think IoT devices require software updates?" (Q_4). 92% consider that IoT devices require software updates, 5% do not know if that is the case, while 3% believe that updates are not necessary. In Tab. 6, we present the answers to the question "who should be responsible for updating the IoT device, in your opinion?" (Q_5). Although 60% of the participants consider that the manufacturer should be responsible for pushing updates to IoT devices (S_4), two participants indicated that they want to be the ones who decide whether an update is installed or not. This could be the result of prior experience with unwanted updates, that disabled useful features or added undesired ones (S_5). This could explain why some are aware of the availability of newer versions, but are not installing them (Tab. 7).

The results indicate that our participants see IoT devices as computer-like systems that require software updates, rather than "plug in and forget" devices. We emphasize that the most common expectation is for the updates to be rolled out by the manufacturer. This is an important point to be considered by IoT device designers, because if this expectation will not be met, it is possible that the devices will run outdated firmware, potentially exposing owners to security and privacy risks. The data also reveal a gap between those who expect updates to be automatically installed by the manufacturer (60%) and those who are aware that updates are automatic and are certain that their IoT device uses the latest version (27%). This difference could be explained in different ways, e.g. the IoT devices do not adequately reflect their update availability status (if at all) (S_6) or end users did not bother to check that. We measure that, using a 5-point

Likert scale, by asking participants "How well does the device [...] express what it is currently doing?", listing several use cases, of which one is "installing an update" (Q_{10}). We have found that participants consider this to be expressed clearly (20%) to very clearly (35%), while another 20% have not experienced this use case. Sec. 5.5 discuses other implications related to update policies.

5.5 Decommissioning

To determine whether participants have gone through this procedure and measure their level of satisfaction with it, we have asked them "how satisfied are you with the process of [...] resetting [...] to default settings and wiping all data?" (Q_6) and "how well does the device express [...] that it is currently resetting itself to default settings and wiping the data?" (Q_{10}). We have found that the many of our participants have not had the experience of wiping the data off their IoT device (31%) or have not had the chance to see how this process is reflected in the interface (45%). It should be noted that some of the participants could have chosen the "N/A" option because their IoT device does not provide such a feature or it is not relevant for its function, the survey does not distinguish between these possibilities. Since this use case has been less explored by end users, manufacturers have fewer opportunities to receive feedback about this procedure. Thus, any existing usability shortcomings can possibly remain in the product for a longer period of time. In contrast, use cases related to set up and usage are likely to attract far more attention. We conclude that IoT device manufacturers should not perceive the lack of customer complaints as an indicator of good usability of their product in the decommissioning phase. Instead, they ought to conduct tests targeting this particular scenario (S_7).

6 Testing the hypotheses

In what follows, we successively test the hypotheses defined in Sec. 3, based on the answers given by participants.

***H_1*: When dealing with IoT devices, most users treat them as *appliances*, rather than *computers*.** On one hand, the arguments detailed in Sec. 5.4 suggest that most of the participants consider IoT devices to be computers, rather than appliances, based on their awareness of the fact that such devices require regular updates and have to be secured. However, the analysis in Sec. 5.3 indicates that this awareness is limited. For example a smart TV that runs an operating system with network capabilities is exposed to all of the resources listed in Q_7, yet the participants' responses failed to reflect that. This could mean that some participants' level of confidence exceeds their actual understanding, which can lead to the false belief that the measures taken to protect their privacy are sufficient, when they are not. We cannot definitively support or refute H_1, because the premise appears to be wrong. It is possible that there exists another model in the spectrum between *computer* and *appliance*, which

describes more accurately how IoT devices are perceived. For example, participants may be used to smartphones and tablets, which require updates, but are nevertheless not treated as computers.

***H_2*: Users are inclined to keep IoT devices that infringe on their privacy, if those devices have a high *monetary value*.** The sampled population perceives privacy as a major concern in IoT adoption, but the concern can be overridden if the purchased IoT hardware was expensive, if it has an entertainment or utility value. In these circumstances, a substantial number of participants would continue using an IoT device, even if they are certain that it infringes on their privacy (Q_{24}, Q_{25}). This can be partially explained by *loss aversion*, thus what matters is whether the owner can get reimbursed easily, regardless of the cost of the IoT device. When a refund is not possible, or if it is a tedious process, an inexpensive device is more likely to be discarded than an expensive one. Thus H_2 is supported, although we have to emphasize that other factors are at play.

***H_3*: Users are inclined to keep IoT devices that infringe on their privacy, if those devices were *a gift from a close person*.** We have also found, by means of a Mann-Whitney U test, that females are more likely to keep using a rogue IoT device ($U = 1066$, $n = 42$, $p = 0.012$)[4] if it was a gift from a close person, thus H_3 is partially supported. It is possible that such attitudes are caused by emotional attachment to a person, however there may be other conditions too, e.g. the device has a likeable design, or it stores valuable content, like photographs. These additional factors were not checked by the questionnaire, so they should be investigated separately.

7 Discussion

The answers to Q_7, "Which of these resources you think are exposed to the IoT device?" discussed in Sec. 5.3 could be a reason of concern. For example, in the case of a smart TV, a typical feature is to stream videos from remote sources, which requires some form of communication over networks, such as the Internet. This, in turn, implies that the device has to have an implementation of a network stack and software that leverages it. However, only two participants (rated at a medium skill level) indicated that their smart TV can access both, computers on their home network as well as other computers on the Internet. The same reasoning applies to voice-activated assistants (e.g. "Amazon Echo"). Only one participant correctly identified that their "Echo" can interact with local and remote hosts, which means that some participants are unaware of the fact that this device can transmit information via the Internet. While it is possible that some IoT devices are deliberately constrained by their owners (e.g. using

[4] This indicates that the results are not likely to be caused by chance, and that if the same questions were given to other participants, the results would be similar.

firewalls), this should not be the case for assistants like "Echo", because they rely on an Internet connection for their basic features. Moreover, configuring Internet access is a required step in the setup phase, which the participants had to go through. This could be explained by the fact that they have an incomplete understanding of the capabilities of their device, or that someone else configured it for them (S_8). Product designers should consider this, because some of the user categories who could benefit from IoT, such as the elderly, may not be digitally literate, yet they must be aware of the implications of using the IoT device. Either the set-up procedure should be easy enough for anyone, or there should be a separate privacy summary that does not use technical or legal jargon and is easy to understand. We did not anticipate such results, therefore our survey was not crafted in a way that would enable us to determine whether this is a deliberate decision made by manufacturers, or an oversight, thus this matter has to be investigated separately.

Another important aspect is *obsolescence*, which we examine by analogy with smartphones. For example, the most common version of Android today has a market share of 31%, it was released two years ago [3]. The two latest versions, 8.0 and 7.1, have a combined market share of 3.3%. Thus, a substantial number of smartphones are running outdated software. This is one of the reasons why the American Civil Liberties Union (ACLU) filed an FTC complaint over Android security issues [1]. If the same pattern arises in IoT, end-users will be stuck with outdated devices which, at best, can only be secured by applying external technical means (e.g. firewalls) or custom firmware. Neither of these options is novice-friendly. A strategy consumers can adapt is to decommission the device before the support period ends. While this solves *their* problem, the obsolete device will become someone else's problem. This creates the premises for a "tragedy of the commons" [12], where the cost of security and privacy risks is distributed among all Internet users, instead of affecting IoT vendors or users specifically. Thus, the incentives to continue supporting and updating these devices is weak. This problem should be resolved in the future, otherwise it could hinder IoT adoption (S_9).

We have found some variation in attitudes, based on technical skills. Experts are more likely to indicate that they use a firewall, encrypted volumes and ad-blockers. They are also better-informed about IoT-related privacy and security news such as those about the Mirai botnet or the German steel factory incident. Note that we chose these topics because they were also covered by the international mainstream press, so non-experts could have heard about them. More surprisingly, the expert participants in our sample are also more likely to consider that manufacturers should be responsible for deploying IoT updates.

Note that our tests show that gender, age, and location do not have a significant impact on the participants' answers, unless otherwise stated.

7.1 Limitations

We encountered several limitations while running the survey. Firstly, people below the age of 18 were excluded, because of strict EU regulations concerning

data collection from minors. However, this population segment could represent a significant portion of IoT technology consumers, thus their opinions should be accounted for. Secondly, we reached out to a technologically proficient audience (only 7% fell into the "novice" category), which is not representative of society in general. The modest number of participants finally gave us some hints about questions worth pursuing, but a study of a larger scale is required to make definitive claims about privacy attitudes.

7.2 Recommendations for IoT vendors

Based on the different statements S_0 to S_9 we highlighted in the paper, we would like to make the following recommendations to IoT manufacturers, to improve their privacy practices:

- S_0 Do not conflate "notice" with "consent" (based on [22])
- S_1 Write concise privacy policies
- S_2 Make privacy-related settings a mandatory part of the set-up phase
- S_3 Find ways to address people's security and privacy concerns
- S_4 Provide an automatic update feature
- S_5 Make the list of version changes public
- S_6 Reflect the update availability status clearly
- S_7 Include decommissioning in usability tests
- S_8 Consider that someone other than the end-user can set up the IoT device
- S_9 Planned obsolescence should be more future-oriented

8 Conclusions

We have organized an online survey with 110 participants, to explore their privacy attitudes towards IoT devices. The results reveal a generally positive opinion about IoT, despite the awareness of existing privacy and security risks. The challenge is to address these issues before the end-users' skepticism creates a barrier in IoT adoption.

We have found a potential void in the user experience related to the decommissioning of such devices. Most participants have not gone through such a use case and there is a possibility that they will run into issues when they do so. Device manufacturers should consider this before releasing their products to the market. We have also found that the expected norm is that IoT devices are updated automatically and that it is the responsibility of the manufacturer to ensure the smoothness of the process. IoT device designers should implement such a capability in their product and provide clear information to end users when automatic updates are not available, and it is the user's responsibility to keep the device up to date.

Acknowledgments This research is funded by H2020 MSCA ITN Privacy&Us (project no 675730). We would like to thank the survey participants, Harald Zwingelberg and the anonymous peer reviewers for their helpful comments.

Appendix A Survey questions

The questions that featured in the survey are shown in Tab. 8. The list does not include the provided choices or other accompanying materials, they are available at `https://www.datenschutzzentrum.de/projekte/privacy-us/`. The site also provides the source code needed to replicate the survey and analyze the data.

Note that not all questions were shown to all participants (e.g. those who do not own IoT devices were not asked about their experience with such products). The label 'brand' was replaced with the IoT device name provided by participants in Q_2. The table also mentions the type of each question, FT: free-text, MS: questions that allowed *several* options to be selected at the same time, MC: questions for which participants had to choose *only one* option out of several, L: Likert scale questions.

Table 8: Survey questions

ID	Type	Question
Q_1	MS	Which of these IoT appliances do you own?
Q_2	FT	Focus on a specific device (note: here the participant is asked to name a specific device they own)
Q_3	MC	Is the selected device running fully up-to-date software/firmware?
Q_4	MC	Do you think IoT devices require software updates?
Q_5	MS	Who should be responsible for updating the device, in your opinion?
Q_6	L	How satisfied are you with the process of using the device 'brand'?
Q_7	MS	Which of these resources you think are exposed to the device 'brand'?
Q_8	MS	Who, in your opinion, can use, or otherwise interact with a 'brand' installed in your home?
Q_9	L	When it comes to configuring the device 'brand' how much do you agree with these statements?
Q_{10}	L	How well does the device 'brand' express what it is currently doing?
Q_{11}	L	How confident are you that the device 'brand' respects your privacy?
Q_{12}	MC	Have you examined the privacy policy of 'brand'?
Q_{13}	FT	What would make the device 'brand' more usable, in your opinion?
Q_{14}	FT	What are the most important things that you like in 'brand'?
Q_{15}	FT	What do you dislike the most about your experience with 'brand'?
Q_{16}	MC	Do you plan to buy any IoT devices in the next 6 months?
Q_{17}	MC	Do you own any appliances, the IoT capabilities of which are not used?
Q_{18}	FT	If you answered "yes" above, please list those appliances here. Optionally, indicate the feature.
Q_{19}	MC	Do you think it is possible that some of your devices or appliances are connected to the Internet without your knowledge?
Q_{20}	MS	Which qualities would you be looking for if you were buying an IoT device?
Q_{21}	FT	What are the reasons to buy Internet-connected appliances, in your opinion?

Q_{22}	FT	What are reasons NOT to buy such appliances, in your opinion?
Q_{23}	MS	Please indicate the benefits of connected devices that appeal to you personally.
Q_{24}	MS	You discover that an IoT device infringes on your privacy and you have no capability to change that. Which of these reasons will influence you to KEEP the device?
Q_{25}	MS	You discover that an IoT device infringes on your privacy and you have no capability to change that. Which of these reasons will influence you to DISCARD the device?
Q_{26}	MC	If you have a WiFi network at home, which of the options below best describes its security settings
Q_{27}	MS	Which of these security tools have you got on your computer?
Q_{28}	MC	What is your age?
Q_{29}	MC	What is your gender?
Q_{30}	MS	Please specify the computer-related skills you have.
Q_{31}	L	Have you heard anything about these in the news?
Q_{32}	MC	What is the highest level of education that you successfully completed?
Q_{33}	MC	Which of these best describes your location?
Q_{34}	FT	If you have any remarks that you would like to make, please use the form below.

References

[1] *ACLU Files FTC Complaint Over Android Smartphone Security*. URL: `https://aclu.org/blog/national-security/aclu-files-ftc-complaint-over-android-smartphone-security` (visited on 11/14/2017).

[2] D. Akhawe et al. "Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness." In: *Usenix Security*. 2013.

[3] *Android API Versions*. URL: `https://developer.android.com/about/dashboards/index.html` (visited on 11/14/2017).

[4] L. Atzori et al. "The Internet of Things: A Survey". In: *Computer Networks* (2010).

[5] S. B. Barnes. "A Privacy Paradox: Social Networking in the United States". In: *First Monday* (2006).

[6] *Careful Connections: Building Security in the Internet of Things*. 2015. URL: `https://ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf` (visited on 05/02/2017).

[7] X. Caron et al. "The Internet of Things (IoT) and its Impact on Individual Privacy: An Australian Perspective". In: *Computer Law & Security Review* (2016).

[8] D. Christin. "Privacy in Mobile Participatory Sensing: Current Trends and Future Challenges". In: *Journal of Systems and Software* (2016).

[9] A. De Luca et al. “Expert and Non-Expert Attitudes Towards (Secure) Instant Messaging”. In: *Proceedings of the 12th Symposium on Usable Privacy and Security (SOUPS)*. 2016.

[10] M. Elkhodr et al. “A Review of Mobile Location Privacy in the Internet of Things”. In: *Proceedings of the 10th International Conference on ICT and Knowledge Engineering*. 2012.

[11] D. Evans. *The Internet of Things - How the Next Evolution of the Internet Is Changing Everything*. Cisco, 2011. URL: `http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf` (visited on 04/25/2017).

[12] G. Hardin. “The Tragedy of the Commons”. In: *Journal of Natural Resources Policy Research* (2009).

[13] *Internet of things: Privacy & Security in a Connected World*. Staff report. FTC, 2015. URL: `https://ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf`.

[14] R. Kang et al. “”My Data Just Goes Everywhere” User Mental Models of the Internet and Implications for Privacy and Security”. In: *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS)*. 2015.

[15] M. Kosinski et al. “Private Traits and Attributes Are Predictable From Digital Records of Human Behavior”. In: *Proceedings of the National Academy of Sciences* (2013).

[16] N. D. Lane et al. “On the Feasibility of User De-anonymization From Shared Mobile Sensor Data”. In: *Proceedings of the 3rd International Workshop on Sensing Applications on Mobile Phones*. 2012.

[17] D. M. Mendez et al. “Internet of Things: Survey on Security and Privacy”. In: *arXiv:1707.01879 [cs]* (2017).

[18] R. P. Minch. “Location Privacy in the Era of the Internet of Things and Big Data Analytics”. In: *Proceedings of 48th Hawaii International Conference on System Sciences (HICSS)*. 2015.

[19] P. E. Naeini et al. “Privacy Expectations and Preferences in an IoT World”. In: *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS)*. 2017.

[20] A. Narayanan et al. “How to Break Anonymity of the Netflix Prize Dataset”. In: *arXiv preprint cs/0610105* (2006).

[21] OECD. *Skills Matter*. OECD Skills Studies. 2016. URL: `http://www.oecd-ilibrary.org/education/skills-matter_9789264258051-en` (visited on 11/15/2016).

[22] S. R. Peppet. “Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent”. In: *Tex. L. Rev.* (2014).

[23] *Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*. 2017.

[24] *Samsung: By 2020, All of Our Products Will Be Connected to the Web.* URL: http://mashable.com/2015/01/05/samsung-internet-of-things (visited on 11/14/2017).
[25] B. Schneier. *Secrets and Lies: Digital Security in a Networked World.* 2008.
[26] *Trends 17.* Globalwebindex, 2016. URL: http://insight.globalwebindex.net/hubfs/Reports/Trends-17.pdf (visited on 04/25/2017).
[27] M. Volkamer et al. "Mental Models - General Introduction and Review of Their Application to Human-Centred Security". In: *Lecture Notes in Computer Science.* 2013.
[28] W. Zhou et al. "Security/Privacy of Wearable Fitness Tracking IoT Devices". In: *Proceedings of the 9th Iberian Conference on Information Systems and Technologies (CISTI).* 2014.
[29] J. H. Ziegeldorf et al. "Privacy in the Internet of Things: Threats and Challenges". In: *Security and Communication Networks* (2014).