Understanding the Privacy Design Space for Personal Connected Objects

Alessandro Montanari
Computer Laboratory
University of Cambridge
William Gates Building, 15 JJ Thomson Ave
Cambridge, CB3 0FD (UK)
alessandro.montanari@cl.cam.ac.uk

Afra Mashhadi, Akhil Mathur
Bell Labs
Nokia
Clyde House
Dublin D15 Y6NT, Ireland
{*name.surname*}*@bell-labs.com*

Fahim Kawsar
Bell Labs
Nokia
Copernicuslaan 50
Antwerpen, Belgium
fahim.kawsar@bell-labs.com

Privacy is a major obstacle preventing the growth of the Internet of Things (IoT). As more connected objects become integrated in daily lives, ensuring that people feel comfortable with IoT's impact on their privacy becomes increasingly important. To date the understanding of users' perception regarding privacy risks in the connected object space is limited. In this paper we aim to shed lights on this issue through a qualitative study of in-depth interview with 16 people. Our results show that users are primarily concerned with the "Data Ownership" (i.e., who owns the data), when interacting with connected objects. Our findings suggest the need for an intuitive tool that can minimise the cognitive distance between users' mental model and the functionalities offered by connected objects. As a result we provide guidelines to design this kind of tool.

Privacy. Internet of Things. Semi-structured interview.

1. INTRODUCTION

With the advent of the Internet of Things (IoT) - more and more everyday objects are getting a digital makeover, and reshaping our experience with the physical world through new, useful, exciting, and sometimes entertaining smart services. It is debatable as to whether or not some of these technologies are currently sufficiently mature to fully deliver on the experiences that are advertised. Nonetheless, as the technology improves, and the overall perceived value of these items starts to outweigh their financial costs, there is little doubt that connected appliances will replace their non-connected counterparts in our homes. However, the financial price is perhaps not the only cost to be incurred by users of these appliances, as more connected services means more data being generated and exchanged.

Indeed, the common facet of all these connected objects is that they collect data that is produced *by* or *about* people to offer value added services. This increase in data volume and complexity raises the important issue of potential privacy and information exposure in this new hyperconnected world. Recent revelations, such as a connected TV silently capturing human conversations to facilitate a smart remote control service, make clear the privacy risks in the connected object space (Simon Sharwood 2015). Naturally, privacy protection and more importantly privacy awareness in the IoT space has become a fundamental challenge highlighted by both researchers (Mayer 2009; Ziegeldorf et al. 2014; Vermesan et al. 2011) and legislators (Federal Trade Commission 2015).

Unfortunately, to date our understanding of users' perception of possible information exposure and privacy risks in the connected object space is limited mostly to the attitudes of *web and mobile application users*. TRUSTe survey of web users has claimed that privacy concerns are major barriers to the growth of IoT, with 85% of U.S. Internet users having concerns regarding the data collection by the smart devices (TRUSTe 2014). As the predecessor of IoT, mobile computing and the Web 2.0 have also received substantial focus on understanding user's privacy perception. A vast body of literature has shown that as the usage of personal data drifts away from original intended purpose of the application, users' privacy concern raises with it accordingly (Consolvo et al. 2010; Egelman et al. 2011; Balebako et al. 2013; Lin et al. 2012).

However in the connected object space, this concern and awareness regarding the data collection and the purpose of the object may differ. This is because over one hundred years of usage of household appliances

has engrained certain familiarities and expectations regarding appliance's behaviour, whereas the new connected versions of these physical objects are now transforming their functional affordances without properly communicating the potential consequences to the end users. Furthermore, Nest and other successful examples of today's anticipatory connected objects have achieved their success by being silent observers of their owners' lifestyle without requiring any necessary input from them. This is in sharp contrast to online services where users' own actions (e.g., Google search, social network usage) had a more direct influence in their information exposure.

Therefore, the key question that we aim to explore is - does privacy awareness in the connected object space differ from general privacy awareness (e.g., in web and mobile space)? If so, which specific aspects of connected objects lead to these privacy concerns, and how can we take the first steps in providing useful privacy information to the future consumers?

In this paper, we explore the privacy space for personal connected objects through a qualitative study with 16 people. The study aimed at understanding their privacy perception and awareness of connected objects, through in-depth semi-structured interviews. In designing this study we adhere to the guidelines of notice and choice (Langheinrich 2001), allowing us to uncover what type of privacy information is considered important and useful to the participants (*Notice*), and for which type they request actions (*Choice*). Facilitating our interviews were two connected objects acting as icebreaker - a Philips Hue Connected Lamp, and a Withings Connected Body Scale. Our research questions are:

- What are the participants pre-existing levels of awareness regarding their information exposure? Does this awareness depend on the connected object type?
- What factors (e.g., awareness of collected data and how it is used, where the data is stored, who owns it, etc.) are more important to the users and can help increase their privacy awareness? What control mechanisms (i.e., how users prefer to manage their privacy) are desired?
- What design guidelines and implications can be drawn from this user study to help improve and address privacy concerns about connected objects at different stages?

While the general observations from our study confirm past work in the privacy literature, our findings provide deeper insights on what factors contribute to privacy concerns for connected objects. Specifically, our findings reveal that unlike the common belief that users are most (83%) concerned with data collection in the IoT space (TRUSTe 2014), our participants were less concerned with the data collection and more concerned with data ownership, that is how long the data is stored and who owns it. Our findings also suggest that despite their concerns, users are reluctant to spend too much time on their privacy management, and demand an intuitive and easy to use tool that shows what data the connected objects are collecting and using for offering value-added services. As a result of our study we provide a set of guidelines which could be used to increase privacy awareness and lower concerns, facilitating the diffusion of IoT devices.

2. RELATED WORK

Today, our understanding of users' privacy perception in the connected object space is limited to the attitudes of web and mobile application users because connected objects have not reached large market shares. TRUSTe have examined Internet users' concerns in the uptake of IoT and reported that the future consumers are concerned about the data that is collected and used by these objects. However, only a relatively low percentage (59%) of U.S. Internet users know that connected devices can collect personal information, and only 22% of U.S. Internet users believe that the benefits of connected objects outweighs their privacy concerns (TRUSTe 2014). In the ubiquitous computing literature there are many suggestions on how ubiquitous systems should be designed to address privacy concerns (Bellotti and Sellen 1993; Lederer et al. 2004; Hong et al. 2004; Hong and Landay 2004). However, the understanding of users' perception regarding possible information exposure and privacy risks is less studied, in particular when considering readily available personal connected objects. Nguyen et al. (2008) studied people's attitudes towards common and widespread recording technologies (e.g., credit cards, store loyalty cards, store video cameras and store RFID tags) and found that even if people show high concern regarding information privacy in general, they are significantly less concerned when using these everyday technologies. Similarly, in another study Nguyen et al. (2009) analysed people's reactions to being recorded by a wearable camera and found that people are more comfortable if they are informed about the data collection but would still accept the recording if it serves particular purposes (e.g. memory aid). Also Iachello et al. (2006) reported the need for informed consent when dealing with audio recording.

We next examine previous works in the Web 2.0 and mobile computing contexts as a source of inspiration to design our study. In the last fifteen years users' concerns about web privacy have increased

dramatically (Culnan and Milne 2001). The concerns arise by the fact that many web-services collect personal information about their users with different purposes (e.g. advertising and personalised content delivery). Privacy policies, due to their complexity, have been shown to be a poor way of providing information regarding the data collection (Jensen and Potts 2004; Privacy Leadership Initiative 2001). Several works have investigated the effect of better visualisation methods for privacy policies and have shown that the users make better decisions when they are aware of the information that is collected and its use (Kelley et al. 2009; Egelman et al. 2009).

Due to the proliferation of smartphones, with thousands of applications collecting users' private data, mobile computing has also experienced similar privacy challenges to the ones described for the web. This data collection could be argued to be even more sensitive due to the nature of smartphones (e.g. precise user's location through GPS, or activity through accelerometer) and has been shown to go unnoticed by the users (Balebako et al. 2013; Thurm and Kane 2010; Egele et al. 2011). Similarly, the permission pages (shown before the installation of an application) usually go unread and are often not understood by the users (Felt et al. 2012; Kelley et al. 2012; Egele et al. 2011). Several authors observed that mobile users would like to have more information about the applications' data practices and this could be beneficial to lower their privacy concerns (Balebako et al. 2013; Lin et al. 2012).

We aim, with this paper, to study the users' privacy perception and awareness when interacting with two real connected objects which could potentially see widespread adoption in the near future.

3. STUDY METHODOLOGY

The objective of this study is to offer an understanding of the privacy design space of connected objects. In doing so, we need to uncover users' perception of privacy and their concerns with information exposure in the connected object space. More specifically, through a qualitative lens we were interested to learn the pre-existing level of awareness that the participants hold regarding connected objects and derive to their core beliefs in order to understand what elements of connected objects lead to the privacy concerns or the lack of such awareness.

To cater for the exploratory and emergent nature of our study, we conducted semi-structured interviews following the laddering technique[1], a qualitative research method that seeks to understand the core values behind the user reactions to any questions. Our interviews had two main components. First, we took inspiration from the extensive privacy literature in the web space to structure our interview questions around the concepts of privacy *awareness*, *concern* and desired *action*. This enabled us to examine the similarity and differences in the privacy perceptions between the web and the connected object space. Second, during the study we introduced the participants to two commercially available connected objects. This served as an icebreaker for our subsequent discussions and also gave a tangible feel of the connected objects to the participants which helped them form their own opinions.

Finally, we also engaged in open-ended discussions with the participants to gain in-depth understanding of their privacy expectations with connected objects. In the next section, we first describe the two interview components in details, providing more information about participants and the study procedure.

3.1. Study Objects

Although there is a plethora of connected objects available commercially, we limited our study to two objects which are readily available in the market and that have been used in previous literature by Ur et al. (2013) to highlight privacy issues. In particular, we selected one object designed primarily for monitoring individual's health and one designed for aesthetic purposes (e.g. lifestyle):

Connected Body Scale. The first object used in the study was the Withings WS-30 Wireless Body Scale[2]. This scale provides connectivity through both Bluetooth 4.0 and WiFi 802.11. It offers a range of functionalities from simple measurement of the weight and BMI, to a more advanced weight tracking and goal setting. It allows the user to create a profile that includes her height and body shape. Furthermore, it enables the users to track and visualise their weight over time. Finally, it allows to share weight on social networks as well as on a leadership board. This connected object provides an excellent case study due to the nature of information that it collects as it may be highly privacy-sensitive to individuals, particularly given the longitudinal nature of its functionality (weight collection over time).

Connected Lights. As the second object for our study, we chose the Philips Hue LED lights[3]. These lights come in the form of ordinary bulbs, but are connected to the Internet through an Ethernet bridge attached to the home's WiFi router. They can be controlled through the website or smartphone applications, empowering the users to control lights both for practical (scheduling lights to turn on in

[1] http://www.uxmatters.com/mt/archives/2009/07/laddering-a-research-interview-technique-for-uncovering-core-values.php

[2] http://www.withings.com/us/ws-30.html

[3] http://www2.meethue.com/

the morning) and aesthetic purposes (e.g., changing lighting colour to reflect one's mood or movie/music). We selected Hue in our study as various privacy threats have been highlighted in the past (Ur et al. 2013). One of these is the ability to monitor lighting state which could allow an adversary to determine whether a space is currently occupied.

In our study, we first introduced the participants to these objects by providing them with the original packaging, and allowing them to perform the account set up and create their profile. Furthermore to ensure they are comfortable with the objects, we asked them to interact with the objects through a set of tasks. This included changing the light colour to reflect their mood and setting the desired brightness and exploring the functionalities of the Withings scale (visualisation of sample data, weigh themselves and check the result on the app). This phase lasted around 15-20 minutes per participant, however we let them use the connected objects and the mobile apps throughout the study if they wanted.

Although we limited our study to only two present objects in our open-ended discussions, we asked participants about their privacy perceptions for six additional categories of connected objects. These categories were: *cooking* (e.g., Connected Fridge, Cooking Pot), *safety* (e.g., Connected Lock, Security Camera), *health* (Connected toothbrush, Blood pressure monitoring), *entertainment* (e.g., Connected Tv, WiFi Speakers), *infrastructure* (e.g., Connected thermostat, Wifi power strip) and *others* (e.g., connected alarm clock, connected mirror). For each object, we gave them a concrete description of what it does, and then gathered their privacy views.

3.2. Privacy Concerns

In order to study participants' privacy perceptions regarding the two study objects, we designed a set of questions which aimed to uncover participants' privacy *awareness*, *concerns* and desired *action*. These questions corresponded to the possible privacy risks, information leaks and dynamic changes in the system. In designing these questions we followed the guidelines suggested by a recent research study (Pew Research Study 2014) allowing us to ground them on three different categories of:

Data Collection: to refer to the nature of the data captured by the connected object, be it participatory (e.g. height) or sensory (e.g. bulb colors). Here we focused on the raw data that these devices are able to collect because our goal was to firstly understand if participants were able to infer by themselves the devices capabilities and secondly to help us understand participants expectation versus those capabilities. We made clear to our participants that in this case we were interested in knowing their observations only regarding the actual data types recorded by the devices and not about the possibility of the data being shared or stored remotely, which are instead covered in the following categories.

Data Inference: regarding what the collected data is used for. These questions were designed to asses if participants were able to create a mental model of what the single data points, collected by the objects, could be used for and to study their reaction when we presented them with possible inferences that were not expected.

Data Ownership: to refer to the main entities that have lawful right to access and use the data. This category was intended to capture user's knowledge of to whom they are giving consent of their data when using a device. For example in the case of the connected lights, we formed the Data Ownership questions based on the Philips privacy policy which states:"Philips works with Google to be able to provide you the (Hue) Services [...] By using the Services, consent to the use by Google of your personal data needed for the service, and the applicability thereto of the Google Privacy Policy and of the European Privacy Directive".

As for the Data Ownership category, also for the other two we ensured that our questions are grounded on the real behaviour of these objects - for this, we read the privacy policies for the two objects and extracted the content of each question from these policies accordingly (Philips 2015; Withings 2015). In total, we designed 33 questions related to the two objects. Table 1 provides specific examples.

3.3. Study Procedure

Our interviews contained three phases. In the first phase, we asked each participants to complete a consent form and a demographic questionnaire. The participants were then given a short introduction and training for both connected objects, and had time to try them out for themselves. At the end of this stage we asked participants to rate through Likert scale their agreement with the following statement: "When I use the device I think about what information I am exposing to others."

In the second phase, we engaged the participants in the structured questions described earlier where we asked each participant a subset of the designed privacy questions (from Table 1) selected using systematic sampling technique and counter balanced using latin square. Each participant was posed 12 questions (6 for the connected body scale and 6 for the connected lights). After each question, we asked whether participants were aware of this information, whether this information caused a concern about privacy, and whether knowing this

Categories	Connected Body Scale	Connected Lights
Data Collection	Do you know that the scale collects your height?	Do you know that Hue collects your Bulb on-off status?
Data Inference	Do you know that the scale infers your obesity level?	Do you know that the Hue infers your lifestyle?
Data Ownership	Do you know that Withings owns your data?	Do you know that Google owns your data?

Table 1: *Examples of the privacy questions from four different categories.*

information would encourage them to take an action. This allowed us to extract descriptive qualitative inputs in regards with the awareness, concern level, and the need for action by the users.

In the third phase of the interview we asked the participants a series of open ended questions regarding their attitude and privacy perception of connected objects. Finally at the end of this phase we asked the participants to rate again their agreement with the awareness statement that was posited to them at the beginning of the study.

Each interview took one hour. The interview was recorded and later partially transcribed to complete the observer's notes. We used open coding (Corbin and Strauss 2014) to analyse the transcripts, extracting concepts and themes.

3.4. Participants

We recruited 16 people who were smartphone users for at least 5 years. Although it would have been ideal to do the study with existing owners of connected objects, however the reality is that the adoption of these devices is still quite low and it is difficult to find a sufficient number of people who own connected objects. Moreover, we argue that long-term smartphone users make a good target group for such studies for two reasons. Firstly, they are likely to be aware about the basic elements of data privacy, i.e. data collection (e.g., smartphone collects location data, personal information), and ownership (e.g. your personal data is accessed by Facebook or Google). Therefore, it is easy for them to relate to the basic data functionalities of a connected object. Secondly, many of these users are likely to be the target population to own connected objects in the future, when the technology becomes mature. As opposed to the early adopters who tend to be technology enthusiasts, these users would make a more informed decision to buy a connected object based on its value and privacy risks.

In total, nine males and seven females, aged 26-49 (μ = 32) with broad range of occupations (including students, marketing, human resources, administration, researchers and technical managers) were recruited through open email invitations and personal solicitation. All the interviews were conducted in English and all the participants were either native English speakers or proficient in English. The study was conducted in an EU member state and all the participants were given a £30 Amazon voucher.

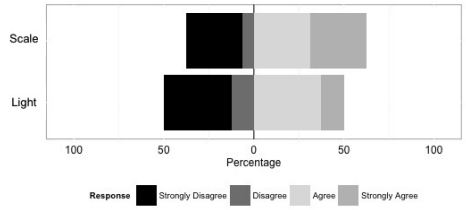


Figure 1: *Participants' level of concern about information exposure when using the objects before the study.*

4. STUDY RESULTS

Based on our open coding we extracted 7 concepts grouped into two core themes, described below.

4.1. Understanding users' mental model

In this section, we present our findings on the mental model and privacy expectations of the users with respect to connected objects. We first aim to understand whether users' perception of privacy is influenced by the type of the connected object. Do users trust a group of connected objects more than others, that may lead to unexpected privacy exposure? To this end, in our interviews we examined the degree of awareness of the participants regarding the two smart objects. We conducted a questionnaire at the beginning of the study, asking the participants to rank their agreement with a statement that captured attitudes toward information exposure on the connected body scale and the connected lights. In particular, the statement was: *"When I use the device I think about what information I am exposing to others"* and they were asked to rate it on a scale from 1 to 5, with 5 showing strong agreement to the statement. Figure 1 shows responses to this question for the connected lights and the connected body scale before the study. As we can observe the participants were more concerned that their interactions with the connected body scale (μ = 3.25, σ = 1.73) could lead to exposure of private information, as opposed to the connected lights (μ = 2.75, σ = 1.61).

Next, we gathered the participants' responses on privacy questions (examples in Table 1). After each response, we used the Laddering technique to understand the underlying reasons for it. An interesting pattern that emerged from our

discussions was that the participants' concern raised when they could not map the data collection to a functionality offered by the object. This finding was particularly strong in the case of the connected lights where participants reported a mismatch between what they expected the connected lights to use their data for and the actual functionalities offered by the object (e.g. inferring lifestyle, storing on-off status in cloud). This mismatch was reflected on the responses given by the participants. In fact, more responses raised privacy concerns for the connected lights (32.5%) than for the connected body scale (22.5% of the responses).

To understand this finding, we used the Laddering technique to probe the participants further. We learned that the source of the privacy concerns was closely linked to the mental model participants held regarding both the expectation and purpose of the object (Norman 1983a,b). More specifically, we uncovered a major *cognitive distance* between user's mental models and the objects' perceived affordances. People create mental models of the things with which they interact. In the case of domestic connected objects, this mental model has been formed over hundred years experience of using ordinary objects and appliances (e.g., light bulbs, tv) and helps the user to form an understanding of how they expect an object to behave. However, when the behaviour of the object does not fit the pre-existing mental model, it raises privacy concerns. Past research has shown that an incoherent or contradictory mental model can adversely affect user's interaction with everyday objects (Norman 2013) and raise privacy concerns in the web and mobile privacy space (Balebako et al. 2013; Lin et al. 2012). However, our study results highlight that this cognitive distance has a much more profound effect in the privacy perceptions of connected objects.

We found that cognitive distance impacts the privacy perception of users at two levels: first when inferring what data is collected by the object. This *mental inference* is greatly influenced by the object's ordinary counterpart and its *affordances*. For example, a scale (even an ordinary one) has a clear perceived *affordance*, that is, it affords measuring the user's weight when she stands on it. This clear affordance enables the user to make an easy inference regarding *when* the data is collected (that is upon standing on it) and *what* type of data is collected (i.e., weight). In our study, this correct mental model led to higher awareness and lack of concerns regarding the posited questions from Data Inference category. However, the same could not be said for the connected lights, as the affordance they provide is illumination (as their ordinary counterpart). But the data they collect deviates from what they afford, making it difficult for users to form a correct *mental model* about the object. In fact, 14 participants were concerned when the Data Inference questions were posed for the connected lights and only 3 of them were concerned for the connected body scale.

Secondly, we found that the cognitive distance impacts a user's understanding of what could be inferred from the collected data. For example, in the case of the scale this *mental translation* allows the user to infer that one's recorded weight could be used for inferring well-being and health status. Once the users have formed this *mental translation*, it may become easier to understand their exposure consequence. This exposure consequence could also be shaped and influenced by the society and the social stigma. For example, in our interviews all the participant were able to make some inference regarding how their health information could be (mis)used in profiling them (e.g., advertising diet products). However, almost all struggled to understand what could be inferred from connected lights's data. We speculate that the cognitive burden of making a mental inference and consecutively a mental translation for the connected lights prevented the users from creating a correct mental model, thus making them more prone to privacy risks. In our interviews one participant stated:

> P11: *"I was not aware of the amount of possible data collection that happens with the lights (i.e., Hue). Lights are just lights, they should not be so smart..."*

At the end of the study, i.e. after we discussed issues of data collection, inference, and ownership, we again asked the participants the same awareness question as we did pre-study. Figure 2 shows the change in awareness for connected lights and the connected body scale. The first point to highlight here is that by informing the users about how their data is collected, inferred and used we observed an increase in the privacy awareness for both the objects. However this is not a new finding: previous studies (Jensen and Potts 2004; Privacy Leadership Initiative 2001) have also shown that majority of users do not read privacy policies and have low awareness about the potential privacy risks. Indeed, our study also uncovered a similar behaviour (recall that all our interview questions were extracted from the actual privacy policies of the objects).

The second, and most important finding is that the increase in privacy awareness for connected lights (44.25% increase) was more than that of connected body scale (30.89% increase). A Wilcoxon signed-rank pairwise test also confirmed that the change is awareness for connected lights was higher ($W(16) = 0$, $Z = -3.07$, $r = 0.76$, $p < .005$) than for the connected body scale ($W(16) = 6$, $Z = -2.11$,

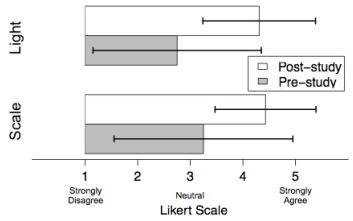
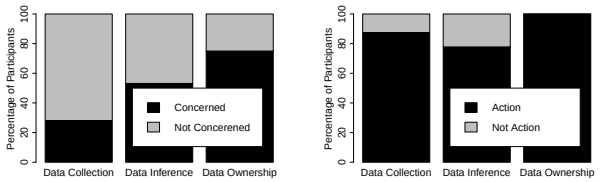


Figure 2: *Participants average Pre and Post study agreement rating concerning information exposure risks.*



(a) *Concern.* ***(b)*** *Action.*

Figure 3: *Users' concerns and preference for taking action to different questions types for both objects.*

$r = 0.52$, $p < .05$). Our qualitative interviews also confirmed this observation, where participants reported of their increase in knowledge and concern regarding the connected lights.

> P8: *"I don't mind people knowing what is my weight ... I found (after the study) the scale more friendly, for the bulb I am more worried about others having access to it and infer my mood..."*

This observation reaffirms that the users are more likely to be concerned about their privacy for those objects that they hold a preconception of the data that is collected and that they can perceive the associated exposure risks. For the connected lights, the initial privacy concern was lower as it was perceived as a ordinary household appliance like a regular light. However, due to the preconception of the risks associated with health-related objects, the initial concern with connected body scale was higher. The study, though, made the participants aware about the privacy aspects of both objects - and therefore, the post-study privacy concerns became very similar for both the objects.

Finally, to assess these findings for a broader range of objects, we asked participants about their privacy perceptions for six additional categories of connected objects (as we discussed earlier in the Methodology section). As expected majority of participants showed concern for the Health (62% of the participants), and safety (75% of the participants) category followed by all other four categories (Others, Cooking, Entertainment and Infrastructure) which were perceived as lesser concerning (less than 20%). While these expectations may work in single-purpose objects - the fact is that nowadays, IoT manufacturers are integrating arrays of various sensors in the connected objects so to compete in offering potential services. Therefore, it becomes even more important to educate the users to shape their mental model correctly and reduce their cognitive distance. This analysis calls for essential transparency and communication from the manufacturers of the connected objects to clearly explain the functionalities and corresponding data acquisition purpose and methods, enabling the users to shape a correct mental model and expectation of the object behaviour. In the next section we offer design guidelines and specific design choices that could reduce the cognitive distance.

4.2. The importance of control

During the second phase of our interview we extracted information regarding the participants' concern level for each category of data handling. We found that Data Ownership caused most of the users' concerns, followed by Data Inference (Figure 3a).

It was intriguing that participants showed less concerns with the actual Data Collection and Inference. Participants only felt concerned when they were presented with information highlighting potential users or owners of their data, as opposed to when they were told about data collection (e.g., Hue collecting on/off status) and data inference (e.g. obesity detection). This finding contrasts with the common belief that users are most concerned with data collection and data inference in the connected object space (TRUSTe 2014; Federal Trade Commission 2015). We also observed that, even when not concerned, the majority of the participants (n = 10) said that they would like to see more detailed information about the data practices. For instance, one participant mentioned:

> P13: *"I want to know the name of the site [that is receiving the data] and for what purpose they are using the data..."*

These findings clearly suggest the need for better communication between the connected objects' manufacturers and the end users to ensure that they completely comprehend the consequences of the wilful disclosure of their personal information.

Next, we seek to understand whether the participants wanted to take *action* when provided with specific privacy information. Figure 3b presents the percentage of participants who wanted to take an action on receiving privacy notices during various data handling stages. In general, the majority of participants (more than 75%) wanted to take action for all data categories. This percentage was particularly high for the Data Ownership category, which, as shown before, were the most privacy concerning.

Analysing the discussions we had with the participants a dominant pattern emerged regarding the

preference to keep the data local. Most participants (n = 10) did not necessarily want to stop the data collection or inference but rather prefer to keep the data local without sharing it with external entities. Typical comments were similar to the following two:

> P9: *"If I know that the data is not leaving the scale and I can delete it, everything is ok"*
>
> P7: *"I don't want to share data externally, if it remains inside my home is fine"*

This finding suggests the need for a control mechanism that provides to the users choices regarding *where* and for *how long* their data is stored. To this end, it is possible to envision a platform consisting of a *personal data storage* that resides at the user's premises and acts as a bridge between the connected objects and the Internet. Such platform can then be designed to incorporate a sandbox model as suggested by Vilk et al. (2014) to ensure the applications are monitored and given minimum required privileges. This is also in line with recent research which aims at putting the individuals at the centre of the management of their personal data by providing architectures to store their personal information allowing them to retain ownership of the data and selectively share it (Haddadi et al. 2015; Shakimov et al. 2011).

Broadly, our findings highlight that the user expectations regarding privacy in the connected object space are formed based on the prevailing privacy standards of the Web. For example, the European cookie law (Parliament 2002) requires websites to make users aware of how information about them is collected and used, and to give them a choice to allow it or not. Our participants expressed a similar desire for control with the connected objects.

However, we argue that bringing transparency and choice to the connected objects space is not as straightforward as the Web, especially because the IoT industry is moving towards Zero UI designs which potentially eliminate the display interfaces and rely more on other ways of interaction (e.g. gesture and audio). For a Web or standalone application, it is relatively easy to communicate its privacy policy to the users because manufacturers can always rely on the presence of a general purpose display. For connected objects instead, the trend is to create simple and intuitive interfaces which provide little possibilities to show long and complex privacy policies. Take Philips Hue lamps for example, in their privacy policy Philips (Philips 2015) states that by creating a Hue account, the user gives explicit consent to Philips to collect data regarding product usage and location (IP address). While this is just one example, the inherent nature of the connected appliances imposes the user consent to be often tied to the purchase of the appliance, or hidden as part of the registration process. This draws attention to the importance of informing the user about her potential privacy exposure during the set-up process when she is not yet familiar with the new object.

The privacy policies are also dynamic and often change as companies get involved in new partnerships. For example, Philips' partnership with Google (as indicated in their privacy policy) allows customer data to be shared with Google. This highlights the importance of a bi-directional communication with the user which provides just-in-time information about changes in policies and data usage, and through which the user can express her consent.

5. DESIGN SPACE

As the companies become the custodians of valuable customer data, the privacy concerns of average consumers must be addressed at all stages of the life cycle of these appliances. This begins with making users fully aware of the potential privacy exposure risks that connected objects bring to their lives. Unfortunately, this awareness does not come to people intuitively. Here we offer specific design guidelines that could increase this awareness.

5.1. Expect the Unexpected

We believe that the mismatch we identified between the expected system image that the user holds regarding the object and how the object actually behaves contributes to the wrong assessment of what data is collected and what inference could be made using the data. Although transparency is legislated by law which obliges companies to clearly state data protection methods in their privacy policies, it is known that very few people actually read and understand these policies (Kelley et al. 2012). Therefore, we believe the connected object space requires simple and transparent solutions to reduce this cognitive distance. We offer the following:

Scripting. One possible way to reduce the mental inference, is to directly communicate information regarding data practices at the set up stage through Scripting techniques. Scripting, which acts as implicit user manuals, could be conceptualised in terms of imperative messages, and could be embedded as peel off stickers on the object. For example, a Smart TV could have a label that reads "Be Careful! I have learned to listen." corresponding to the privacy policy clauses such as "Your appliance may capture voice commands so that we can provide you with Voice Recognition features". Providing this information at the out-of-box stage allows the user to create the correct mental model of the object early on.

Feed forward. Manufacturers and third party companies could also explicitly highlight the data collection in terms of signifiers available. For example accompanied smart phone apps could help

lower user's cognitive distance by visualising sample data, acquisition strategy, and sample analytics during on-boarding phase. This scheme will basically then act as a feed-forward, enabling users to form a correct expectation as to what type of data and with what granularity will be collected about them.

Persistent Notification. Finally, another key challenge when dealing with the data collection is not only with regards to what data is collected but *when* the data collection happens. An average user's understanding of privacy concerns on the Internet has primarily been shaped from the Web 2.0 and mobile apps usage, where often a direct action (e.g., uploading a picture) could trigger a potential privacy exposure. Unfortunately, in the connected object space there is often no link between a user interaction with an object and data collection. For example, Nest and other successful examples of today's connected home appliances achieved their success by being silent observants on their owner lifestyle and environment without requiring any input. Therefore it is important to make users understand that their privacy exposure is beyond the result of their interaction with the appliances. This could be achieved by employing techniques as persistent notices which often are used to illustrate when a data practice is active (e.g., GPS icon indicating the location being accessed in the smart phone)(Cranor et al. 2006; Schaub et al. 2015). For example, persistent icons, similar to what is illustrated by Egelman et al. (2015), could be embedded in the object to indicate what data is collected and when.

5.2. Need for a Perceptual Tool

Once the set-up is over and users begin cohabiting with the connected object, it becomes important to ensure that the users are aware of the privacy risks as privacy policies and services could change over time. Given the unsuitability of traditional privacy policies there is a need for new ways of integrating the *Notice and Choice* principle (Langheinrich (2001)) into the connected object space. In fact, the need for a simple mechanism that could help users in understanding the potential privacy exposure emerged from our interviews where, even if concerned, the majority of participants did not want to spend too much effort on privacy management, for example two participants stated:

> P9: *"Many times when I want to change something and is complicated I just give up."*

> P7: *"I think short information is already plenty for me, having to look somewhere else for it I would not bother..."*

To this end, we propose that an independent conceptual tool can be designed by third party companies to bring transparency and privacy dialogue to our homes. The conceptual tool would make users more aware about the data practices and would enable them to take action to control their privacy exposure. This tool can act as a notifier by bringing to attention the privacy notifications related to one or multiple objects at home. It could also act as an interface simplifying the mechanism that is needed for the users to act on their privacy settings by providing opt out and configuration choices through the tool itself. The two main results of our study, the cognitive distance between users' expectations and real objects' capabilities (Section 4.1), and the need for a mechanism that provides users with more control (Section 4.2), are the foundations for the following guidelines.

Provide Succinct Notification. The first important aim of this conceptual tool is to reduce the *cognitive distance* between user's mental models and the objects' perceived affordances. In fact, an important source of concerns we found during our interviews lies in the difficulty of relating the mental image of the object a person has with the augmented functionalities available on its connected counterpart. For this reason, the tool should present to the user short and simple notification messages about the changes in the objects that may affect her privacy as well as act as a reminder about the data that the connected devices collect and its intended purposes. The succinct notifications should create a basic level of awareness and reduce the cognitive distance between the user's mental model and the object's affordances. The user can then decide to take an action on the spot or trigger other modalities to learn more about the potential privacy exposure. The three categories we used to drive our interviews could be employed as a starting point to categorise the sources of information used for the notifications.

It is important to ensure the users can infer the notification information at a glance. Tam et al. (2010) examined different ways to present access-control information so that users who saw permission settings for only a few seconds could accurately answer questions about them. They found that icons were preferred and enabled users to quickly become aware of potential dangerous situations. Similarly, we believe icons could be incorporated into the tool as a mean to complement notifications and could be designed following similar guidelines as suggested by Raskin (2010) and Egelman et al. (2015).

Simple Control. As observed in our interviews, people's desire is not only to be aware of the possible privacy exposure, but it is also to own their data and be in control of the data practices adopted by the object (Section 4.2). The tool needs therefore to offer an intuitive interface to take decisions on the spot when notices appear. The envisioned

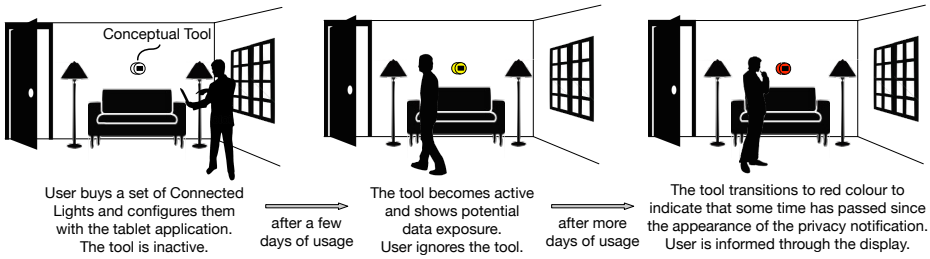


Figure 4: *Conceptual privacy management tool that shows privacy notification messages about collected data and changes that may affect users privacy and can help users to take informed actions to minimise risks associated with connected objects.*

control mechanism should be at a very high level to accommodate, as we found in our interviews, the needs of users who are not willing to spend a lot of effort on privacy management. A simple example of such control is the possibility to temporarily stop the functionality that caused the concern.

Tangible Form Factor. In essence, the conceptual tool could be realised as a soft display (e.g., a mobile application) or a tangible display, such as in a shape of a sticker, or a diagnostic meter which could be either directly attached to the appliance or spaces within the house. We argue that in the context of connected objects, the latter is an appropriate choice because it facilitates and promotes embodied interactions with the privacy tool. Embodied interaction has shown to reduce the fragmented attention of the user, especially in contrast to the application-centric solutions which are prone to attention fragmentation (Kawsar et al. 2010). Therefore, embodied interactions are highly desirable for a privacy tool as it ensures the user is more likely to focus on making decisions on the privacy notifications and less likely to be distracted by other surrounding information (e.g., other notifications and applications on the smartphone). By taking a tangible form, the tool could also follow the natural mapping design principles to ensure that its location also reflects on its control and effect on the connected appliance.

Detailed Information and Control. The tool described so far would already constitute a step forward in increasing users' awareness and lowering her cognitive distance. However, as highlighted by our participants, even if people are not concerned with the objects' data practices, they wish to receive more information to fully understand what the object is doing. Therefore, we foresee the possibility for the user to explicitly request more information about the notification shown. This will allow her to view more details on devices with enhanced input and output capabilities and have a full control over privacy settings. For example, a "tap" with an NFC-enabled smarthphone on the conceptual tool could expose more details on the user's phone. A possible implementation of this tool is represented by a situated micro display that could foster interactions as shown in Figure 4. Other than the display to show notifications and accept user input, the tool could also attract attention by changing its colour. When a privacy notification appears, the outer circle could illuminate in yellow - and as time elapses this light could transit to red. In this paper we do not dwell in describing the actual operation of the system as it is out of scope of this work.

6. CONCLUSIONS

We investigated users' perception and awareness in the connected object space through semi-structured interviews. We observed that users are more concerned with the Data Ownership (i.e. who owns the user's data) aspect rather than with the Data Collection (i.e. what data is collected). Additionally, we noticed that users have difficulties in creating a correct mental model about the connected object, leading to an higher level of concern. We showed the need for a tool to keep users aware of potential privacy threats and we provided possible design guidelines for this tool and future connected objects.

However, we note that to derive a complete set of design guidelines, the relation between the user and the proposed tool needs to be studied over time. Indeed, a longitudinal study could address questions such as whether the privacy notifications could lead to anxiety and thus a less usage of the connected objects over time; or whether the users would start to ignore the privacy notifications after an initial usage period. Additionally, in our guidelines we did not consider the potential gap between the tool designer's mental model and the objects affordances which requires further investigation.

The limited size of the study, prevented us to analyse the relationship between privacy perception and cultural traits. As highlighted by Kugler (2015), people perception of privacy issues vary greatly in different regions. Even if our participants were well mixed in terms of ethnicity, most of them had lived in a western European country for several years and none of them were American, therefore this difference could not be captured in our analysis. Our results may not be generalisable, however our in-depth qualitative study compensates for this and the guidelines we offer will be valuable in future works.

REFERENCES

Balebako, R., J. Jung, W. Lu, L. F. Cranor, and C. Nguyen (2013). Little brothers watching you: Raising awareness of data leaks on smartphones. In *Proceedings of the 9th Symposium on Usable Privacy and Security*. ACM.

Bellotti, V. and A. Sellen (1993). Design for privacy in ubiquitous computing environments. In *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW?93*, pp. 77–92. Springer.

Consolvo, S., J. Jung, B. Greenstein, P. Powledge, G. Maganis, and D. Avrahami (2010). The wi-fi privacy ticker: improving awareness & control of personal information exposure on wi-fi. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*. ACM.

Corbin, J. and A. Strauss (2014). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications.

Cranor, L. F., P. Guduru, and M. Arjula (2006). User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction (TOCHI) 13*(2), 135–178.

Culnan, M. J. and G. R. Milne (2001). The culnan-milne survey on consumers & online privacy notices: Summary of responses. *Washington DC: FTC*.

Egele, M., C. Kruegel, E. Kirda, and G. Vigna (2011). PiOS: Detecting Privacy Leaks in iOS Applications. In *Proceedings of 18th Annual Network and Distributed System Security Symposium*.

Egelman, S., R. Kannavara, and R. Chow (2015). Is this thing on?: Crowdsourcing privacy indicators for ubiquitous sensing platforms. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 1669–1678. ACM.

Egelman, S., A. Oates, and S. Krishnamurthi (2011). Oops, i did it again: Mitigating repeated access control errors on facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM.

Egelman, S., J. Tsai, L. F. Cranor, and A. Acquisti (2009). Timing is everything?: the effects of timing and placement of online privacy indicators. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM.

Federal Trade Commission (2015). Internet of Things: Privacy & security in a connected world. `https://www.ftc.gov/system/files/documents/reports/\federal-trade-commission-staff-\report-november-2013-workshop-\entitled-internet-things-privacy/150127iotrpt.pdf`. Last Accessed 25/05/2016.

Felt, A. P., E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner (2012). Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM.

Haddadi, H., H. Howard, A. Chaudhry, J. Crowcroft, A. Madhavapeddy, and R. Mortier (2015). Personal data: Thinking inside the box. *arXiv preprint arXiv:1501.04737*.

Hong, J. I. and J. A. Landay (2004). An architecture for privacy-sensitive ubiquitous computing. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services*. ACM.

Hong, J. I., J. D. Ng, S. Lederer, and J. A. Landay (2004). Privacy risk models for designing privacy-sensitive ubiquitous computing systems. In *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*, pp. 91–100. ACM.

Iachello, G., K. N. Truong, G. D. Abowd, G. R. Hayes, and M. Stevens (2006). Prototyping and sampling experience to evaluate ubiquitous computing privacy in the real world. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pp. 1009–1018. ACM.

Jensen, C. and C. Potts (2004). Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM.

Kawsar, F., E. Rukzio, and G. Kortuem (2010). An explorative comparison of magic lens and personal projection for interacting with smart objects. In *Proceedings of the 12th international conference on Human computer interaction with mobile devices and services*. ACM.

Kelley, P. G., J. Bresee, L. F. Cranor, and R. W. Reeder (2009). A nutrition label for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM.

Kelley, P. G., S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall (2012). A conundrum of permissions: installing applications on an android smartphone. In *Financial Cryptography and Data Security*. Springer.

Kugler, L. (2015, January). Online privacy: Regional differences. *Commun. ACM 58*(2), 18–20.

Langheinrich, M. (2001). Privacy by design-principles of privacy-aware ubiquitous systems. In *Proceedings of Ubicomp 2001: Ubiquitous Computing*. Springer.

Lederer, S., J. I. Hong, A. K. Dey, and J. A. Landay (2004). Personal privacy through understanding and action: five pitfalls for designers. *Personal and Ubiquitous Computing 8*(6), 440–454.

Lin, J., S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang (2012). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM International Conference on Pervasive and Ubiquitous Computing*, UbiComp '12. ACM.

Mayer, C. P. (2009). Security and privacy challenges in the internet of things. *Electronic Communications of the EASST 17*.

Nguyen, D. H., A. Kobsa, and G. R. Hayes (2008). An empirical investigation of concerns of everyday tracking and recording technologies. In *Proceedings of the 10th international conference on Ubiquitous computing*, pp. 182–191. ACM.

Nguyen, D. H., G. Marcu, G. R. Hayes, K. N. Truong, J. Scott, M. Langheinrich, and C. Roduner (2009). Encountering sensecam: personal recording technologies in everyday life. In *Proceedings of the 11th international conference on Ubiquitous computing*, pp. 165–174. ACM.

Norman, D. A. (1983a, apr). Design rules based on analyses of human error. *Communications of the ACM 26*(4).

Norman, D. A. (1983b). Some observations on mental models. *Mental models*.

Norman, D. A. (2013). *The Design of Everyday Things*. Perseus Books.

Parliament, E. (2002). Directive 2002/58/ec of the european parliament and of the council of 12 july 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, off. *JL 201, 31.7. 2002, at 37.(Directive on Privacy and Electronic Communications)*.

Pew Research Study (2014). Privacy In All Things Includes the Internet of Things. `http://www.abine.com/blog/2014/the-internet-of-things/`. Last Accessed 28/02/2015.

Philips (2015). Philips Hue Privacy Policy. `http://www2.meethue.com/en-us/privacy-and-cookies/`. Last Accessed 24/09/2015.

Privacy Leadership Initiative (2001). Privacy notices research final results. *Conducted by Harris Interactive*.

Raskin, A. (2010). Privacy Icons: Alpha Release. `http://www.azarask.in/blog/post/privacy-icons/`. Last Accessed 28/02/2015.

Schaub, F., R. Balebako, A. L. Durity, and L. F. Cranor (2015). A design space for effective privacy notices. *To appear in the*.

Shakimov, A., H. Lim, R. Ćaceres, L. P. Cox, K. Li, D. Liu, and A. Varshavsky (2011). Vis-a-vis: Privacy-preserving online social networking via virtual individual servers. In *Communication Systems and Networks (COMSNETS), 2011 Third International Conference on*, pp. 1–10. IEEE.

Simon Sharwood (The Register, 2015). WATCH IT: It's watching you as you WATCH IT (Your Samsung telly is). `http://www.theregister.co.uk/2015/02/09/samsung_listens_in_to_everything_you_say_to_your_smart_tellie/`. Last Accessed 28/02/2015.

Tam, J., R. W. Reeder, and S. Schechter (2010, May). I'm Allowing What? Disclosing the authority applications demand of users as a condition of installation. Technical Report MSR-TR-2010-54. Last Accessed 28/02/2015.

Thurm, S. and Y. I. Kane (The Wall Street Journal, 2010). Your Apps Are Watching You. `http://online.wsj.com/news/articles/SB10001424052748704694004576020083\703574602`. Last Accessed 28/02/2015.

TRUSTe (2014). Internet of Things Industry Brings Data Explosion but Growth Could be Impacted by Consumer Privacy Concerns. `http://www.truste.com/blog/2014/05/29/internet-of-things-industry-brings-\data-explosion-but-growth-could-be-\impacted-by-consumer-privacy-concerns`. Last Accessed 28/02/2015.

Ur, B., J. Jung, and S. Schechter (2013). The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security (HUPS)*.

Vermesan, O., P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, et al. (2011). Internet of things strategic research roadmap. *Internet of Things-Global Technological and Societal Trends*.

Vilk, J., D. Molnar, E. Ofek, C. Rossbach, B. Livshits, A. Moshchuk, H. J. Wang, and R. Gal (2014, February). Surroundweb: Least privilege for immersive "web rooms". Technical Report MSR-TR-2014-25. Last Accessed 28/02/2015.

Withings (2015). Withings Body Scale Privacy Policy. `http://www2.withings.com/uk/en/legal`. Last Accessed 24/09/2015.

Ziegeldorf, J. H., O. G. Morchon, and K. Wehrle (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*.