A Data-Driven Approach to Recommending Privacy Preference for IoT systems

A Dissertation Proposal
by

Yangyang He

Aug 2018

Submitted to the graduate faculty of the
School of Computing
In Partial Fulfillment of the Requirements
for the Dissertation Proposal
and subsequent Ph.D. in Computer Science

Approved By:

Dr. Bart P. Knijnenburg
Advisor/Committee Chair

Dr. Larry F. Hodges
Committee Member

Dr. Alexander Herzog
Committee Member

Author's Publications

The work in this document is partially based on the following publications.

1. He, Y., Bahirat, P., Knijnenburg, B.P. (2018): A Data Driven approach to Designing for Privacy in Household IoT. Submitted to ACM Transactions on Interactive Intelligent Systems (TiiS).

2. Bahirat, P., He, Y., Knijnenburg, B.P. (2018): Exploring Defaults and Framing effects on Privacy Decision Making in Smarthomes. To appear on Interactive Workshop on the Human aspect of Smarthome Security and Privacy, SOUPS 2018, Baltimore, U.S.A.

3. Bahirat, P., He, Y., Menon, A., Knijnenburg, B.P. (2018): A Data-Driven Approach to Developing IoT Privacy-Setting Interfaces. IUI2018, Tokyo, Japan.

4. Liu, J., Shen, H., Yu, L., Narman, H.S., Zhai, J., Hallstrom, J.O., He, Y. (2018): Characterizing Data Deliverability of Greedy Routing in Wireless Sensor Networks. IEEE Transactions on Mobile Computing (TMC) 17, 543-559.

5. Ge, R., Feng, X., He, Y., Zou, P. (2017): The Case for Cross-Component Power Coordination on Power Bounded Systems. ICPP2016, Philadelphia, PA, USA

6. Zhai, J., He, Y., Hallstrom, J.O. (2015): A Software Approach to Protecting Embedded System Memory from Single Event Upsets. EWSN2015, Porto, Portugal.

7. He, Y., Du, Y., Hughes, S., Zhai, J., Hallstrom, J.O., Sridhar, N. (2015): DESAL$^{\beta}$: A Framework For Implementing Self-stabilizing Embedded Network Applications. International Internet of Things Summit, pp. 307-312. Springer, Cham, 2015.

8. Ruffing M., He Y., Kelly, M., Hallstrom, J.O., Olariu, S., Weigle, M.C. (2014): A Retasking Framework for Wireless Sensor Networks. Military Communications Conference (MILCOM), 2014 IEEE 1066-1071.

Outline

Abstract

Internet of Things (IoT) are more widely used recently, from general industrial equipment, to household electronics, to wearable devices. With IoT systems becoming more complex, users of IoT devices are paying more attention to their privacy, bringing new challenges to the privacy-setting interface designer. In this proposed dissertation, we focus on four of the most important challenges: (i). How to design privacy-setting interfaces for general IoT devices users? (ii) How to design privacy-setting interfaces for Household IoT devices users and how exactly does the ? (iii) How to design privacy-setting interfaces for Fitness tracker devices users? (iv). How satisfied are the user when they are using these privacy-setting interfaces? In this proposal, we focus on

Chapter 1

Introduction

Every passing day, our electronic device is getting smarter. It is no longer surprising that our refrigerator knows what food is stored inside it and notify us that we need to buy groceries when we start our car trying to go back home from work. Under the moniker of 'Internet of Things' (IoT), smart connected devices are revolutionizing our everyday life. These smart devices ranging from personal devices [2, ?] (e.g., fitness trackers, smart speakers, smart home appliances) to devices deployed in public areas and "smart cities" (e.g., smart billboards, RFID trackers, CCTV cameras) [3, ?, ?], are intended to collect information directly related to the users, such as fitness/healthy information, or the environment of users, such as users' home. A main feature of these smart devices, is that they are connected to a larger network of devices via local communication protocols and/or the Internet to create powerful new applications that supports our day-to-day activities.

IoT is not a new word to normal users nowadays. Samsung's smart-things, Phillips' Hue smart lighting, Google's Nest smart learning thermostat, and ADT smart home security, Smart watches and fitness trackers, such as the Apple, Android and Pebble watches, Fitbit, Garmin, Jawbone, and Misfit bands, are helping us record our steps, heartbeats, and calories burnt. IoT has already established a huge impact in our everyday lives. As forecast by Gartner [?], a total number of 21 billion IoT devices will be in use by 2020. This means that IoT devices are about to dethrone smartphones as the largest category of connected devices by then.

The rapid accelerating of the IoT brings a wealth of opportunity as well as risks. However, a lot of research has been focusing on the data and technology needs of the IoT – the sensors, data, and the storage, security, and analysis of the data. However, research to an important aspect of IoT adoption and usage–the humans interacting with those technologies, are lacking. The demand for reducing the complexity and the burden in controlling these devices is urgent. Hence, my dissertation proposal research focuses on simplifying the task of controlling IoT devices for users using a data-driven design. People is bad at making decisions. This is also true in IoT privacy-setting domain [**need reference**]. To solve this problem, I use statistical analysis and machine learning to analyze how IoT device users make decisions regarding the privacy settings of their devices. Based on the insights gained from this analysis, I design intelligent User Interfaces to reduce the complexity of the privacy-setting user interface.

Chapter 2

Motivation

Privacy issues are the underlying obstacles to the adoption of social and mobile technologies. Privacy concerns have been identified as an important barrier to the growth of Internet of Things.

When the users are considering adopting the new IoT devices, they want to take the benefit of using those smart connected electronic devices by sharing and disclosing their certain personal information to get more personalized experience. However, such dis-closured information could be accessed by other smart devices owned by themselves, other people, organizations, government, or some third-parties with good or bad purpose, which will result in unknown risks to the users. Users have to make choices on what information that they want to disclose.

Most Internet users take a pragmatic stance on information disclosure. They implicitly use a method called *privacy calculus* to process their information disclosure decisions. They compare the perceived risks and anticipated benefit, and make decisions based on this risk-benefit analysis.

However, as the increase of the diversity of IoT devices, it becomes more and more difficult to keep up with the many different ways in which data about ourselves is collected and disseminated. Although generally, users care about their privacy, few of them in practice find time to read the privacy policies or play around the privacy setting options that provided to them. There are several reasons leading to this problem: i) Users will think more of the benefit they will enjoy if they use the IoT devices or services than the potential risks if they disclose their information. ii) The privacy policies is too long, or the privacy setting of such devices are too complicated, making users irritated to finish reading/setting them. iii) As the rapid increment of numbers of IoT devices, the numbers and options of privacy setting for all the IoT devices are also increasing exponentially. This

Table 2.1: Participants Demographics

Age Range	21-35	
Gender	Male	8
	Female	2
Races	Chinese	2
	Indians	4
	Americans	3
	Latin American	1

privacy-setting choice overload makes it difficult for IoT users to correctly and precisely make their decision to express their true demands. Thus, the main research question I propose to answer in my dissertation proposal is thus:

How can we help users simplify the task of controlling privacy setting for IoT devices in a user-friendly manner, so that they can make good privacy decisions?

To answer this research question, we first conduct a preliminary user study based on interviews with potential users to understand the acceptability of IoT systems and devices. We interviewed 10 users with the demographics shown in Table 2.1. The interviews are approximately 30-50 minutes in length and covered a wide range of open questions related to IoT. These questions need participants to input their personal preferences about technology and self-perceived tech savviness. We first recorded the entire conversation with the participants on the understanding that their anonymity was kept. The entire recorded conversation was then transcribed manually. We also tried to take note of other interpersonal cues, e.g. body language, as well. Keywords, such as privacy and ease of use, have been focused on. During the analysis, we extracted the key statement from our interviews and used card sorting and affinity diagram techniques to group the specific statements.

Based on the results from our interviews, the factors that affect the acceptability of IoT devices can be summarized into following three aspects: Privacy, Usability, and Affordability. As shown in Figure 2.1, while making the decision of whether to adopt the IoT technology, the users usually consider the trade-off between privacy and usability as against affordability. If the user's find that they are going to get better usability and privacy at a price that they can afford, they are more likely to go ahead and choose an IoT system.

In a deeper level of usability, if the users find that the IoT systems will enhance their convenience, they will be more inclined to accept it. However, this is based on their perception of

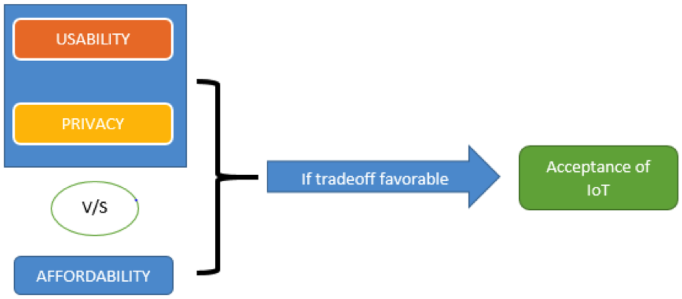

Figure 2.1: Process of accepting IOT as observed

the actual utility of the automation provided by IoT. For example, if someone stays near a grocery store, he/she would tend to believe that there is not enough purpose for an IoT system when it comes to automatic ordering of the same grocery list online.

The ability to control, which can also be seen as the capability to dominate over a technical entity and the extent to which this control can be exercised is one of the key aspects in determining the overall usability of the system. If the users think that they have a high level of control, they are likely to believe that the system has better usability.

In terms of privacy, the users primarily make judgements based on the trust they have on the brand/manufacturer and its public image. For example, one of our participants mentioned that he would trust apple when it comes to sharing of information, this participant had immense trust in Apple, based on some great reports recently published in newspapers. Hence, if they trust a brand with their data, they will have a better resolution of their privacy concerns, which would eventually lead to them accepting the technology. It is evident that the brand image will certainly play a key role in new users accepting the IoT technology.

2.1 IoT Privacy and Acceptability

In this section, we present the ralation between privacy concerns and the acceptability of IoT systems/devices. The most important thing central to any IoT systems/devices is that there exists a constant sharing of information during the usage of such systems/devices. For example, in an environment of Household IoT, a refrigerator can sense what are stored inside it and can notify users when they need to refill the groceries. The entire IoT systems are highly relying on such data collections and sharing in order to provide the best possible experience to the users. However, users may find some of these data collections to be intrusive in nature. The perceived risks from the data collection and sharing can be the main obstacle that users would adopt IoT systems/devices. As one of the participants mentioned that, “As long as the privacy issue can be managed and the companies can be responsible in keeping encrypted data so that it can’t be easily hacked and all that. As long as everybody is respecting that privacy. I love it.” Therefore, we consider privacy is one of the most important key factors which users would decide on, prior to accepting a new technology.

2.1.1 Type of Information: *What is collected/shared*

There are various types of information can be collected/shared in an IoT systems, such as location, photos, voice, and videos. From our interview, we observe that different types of information have different levels of importance to the user. For example, a user may perceive different privacy-related concerns when his/her photos or videos are shared. Below is an excerpt from an interview which highlights the importance of what information is collected/shared:

I: “So you are not ok with photo, video or voice?”

P: “Yes that’s s pretty good generalization. Any data that is visuals of me photographs, voice, video, I would probably not want to store it.”

I: “About voice?”

P: “I mean, I understand that it is being stored to improve your algorithms but what if that was to get leaked.”

typically, users are mostly uncomfortable with sharing their private data to other entities. “May be sharing birthday or address, sharing those kind of data I’m not comfortable with”. Another quote which proves the above point is ”Maybe you can just share your common information, such as heartbeat data, sleeping data. But more critical, privacy data I don’t want to share.” They have their reservations against their private data being shared as it might threaten their security. Privacy information like date of birth and address helps in identifying the person and can be used to hack or rob the person. Therefore, we can say that people are worried about sharing their private information.

However, some participants expressed that some of their private data can be shared unless it is sensitive. One participant mentioned, "At this point I am not much concerned about my location being shared. I mean if somebody wants to find me they can find me anyhow without my location being shared. I don't mind location, I don't like personal messages or personal pictures, personal communication being shared. That bothers me, example my email has some social security or something.".

Another participant also mentioned, *"Apart from photos, what other kind of information you like or don't like to be shared? Like saying something dirty to my girlfriend or something. That's okay like guy's being a guy. But if I am having really you know personal conversation about death of a loved one or something and we are trying to work out logistics or something. That's a problem for me. But for a regular conversation I am ok"*. So the voice, seen as private data by many users, can be recorded or shared for some users.

It is intriguing that users were well aware of what type of information is collected/shared. This suggests that the designer of future IoT privacy-setting interfaces should provide the user separated options of allowing or denying data collecting/sharing for various types of information.

2.1.2 Trust in IoT: *Who is collecting, storing, and sharing my data?*

Another aspect related to the IoT privacy we observed in our interviews is the **Trust**, the object of which is to whom users' informations are shared with. The object of trust from users can be varied in different contexts of IoT environments. For example, in general IoT environment, the objects can be an individual (e.g. your colleagues), an organization (e.g. your employer), the government and so on. While the user is in a Household IoT environment, his/her information may be first shared within all the connected IoT devices deployed in his/her home for various functionalities. Moreover, those smart IoT devices may further transfer users' information to their manufactures to store on a remote server (cloud) or even share them with the third-party for other purpose, such as advertisements and better recommendations.

From our interview, we observed that the trust to the second-party or even the third-party also varies from user to user. One of the participants pointed out that, *P: "For example, Apple in the news recently for refuting the FBI. FBI wanted in, Apple said we can't access these phone that actually turned me on to apple I previously used android. And the fact that they say they made*

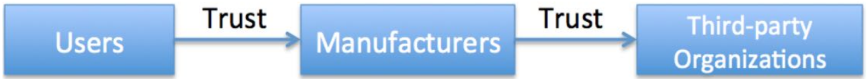

Figure 2.2: Trust Chain

their devices so secured that they can't even access them that really interests me. So yeah I am very concerned about it but I think now that I evolved into the Apple eco-system. I pretty much give apple everything because I trust them."

Another example is:

I: "Would you be alright if the manufacturer of those products collect your data and share with other organizations and provide more specific recommendation to you? Will you be OK with that?"

P: "I think I can be OK with that. Because the data this company collected are most time just shared or transfered to other companies who can analyze these data and get some information from these data."

I: "Any company or any organization?"

P: "I think most are the manufacturers that I trust."

I: "So you are OK with them to share your data?"

P: "Yes, I trust them."

It is evident from the conversation above that once established, trust can propagate from the second-party to the third-party via a "trust chain". As shown in Figure 2.2, a "trust chain" is established when the organization we trust, deals with a third party organization which we are not aware about in the first place but still choose to trust. This kind of trust can be established only when there is a clear sight at the benefits that the user might get out of such a connection.

Based on the interview results, users are well aware of who is collecting, storing, and sharing their data. They have a demand of controlling these data flows proceeded by different second-parties or third-parties. The designer of future IoT privacy-setting interfaces should solve the challenges of differing various second-parties and third-parties, and providing access control options available to users of different IoT contexts.

2.2 IoT Usability and Acceptability

We now present the effect that usability of the IoT devices has on the acceptability to IoT systems. We first describe the "convenience" and then move forward to discuss "control".

2.2.1 Convenience and Usability

The first most important aspect of usability is convenience. Convenience in case of IoT can be treated as the ease with which the IoT system offers funcitonality. Convenience can simply be a feedback which is provided by the temperature sensors in an household IoT system or the various recommendations provided by a recommender system in a way that it eases the shopping experience on e-commerce websites, such as *Amazon.com*. One of the users was asked about how they would feel being in an IoT environment replied by saying, "Excited actually! When you describe that I don't know if that's sharing your same excitement but.. umm it actually is exciting to me because its so wonderfully convenient, so beautifully convenient." The same participant further went on saying "I love it. I mean it would be awesome to look at my phone right now and say 'oh! My door's unlocked'. Actually my brother has that, actually he can check his phone can look if the door locks. And it's really cool! You don't have to worry when you go out on a trip. Or you can control the A/C if you forgot. It's really cool." It is clear from this statement that convenience of use of IoT systems is directly associated with the acceptability. Almost all of our participants pointed out the same thing in a similar way. The convenience offered through IoT systems by enabling the users with a common platform from where they can easily connect with their devices goes a long way in improving the overall usability of the systems and thereby impacts the acceptability of IoT in its totality. Usability for a few users also encompasses the aesthetics of any system which is evident from the statements made by participants.

2.2.2 Being in Control and Usability

Apart from convenience, the feeling of being in control of the system is also of equal importance. Another interesting aspect of control is that it is highly dependent on the information about the state of the system. Any individual will try to control something only when they are aware that it needs to be controlled or that it can be controlled. Therefore, being notified is primarily important before being able to control any aspect of the system. One of the participants when questioned about their opinion of overall usability of any device, mentioned enthusiastically that "I am excited by the idea that me being able to control what they want to do. I am less excited by the idea that them doing autonomously control what they want because some company told them to do it. Luckily the technology is so dumb right now. It's so linear, that it's not good at anticipating the things. But when it gets smarter, as long as it knew that I was an individual who would care, I think the same technology would allow you to totally automate your life but it would allow me to pick and choose which parts to automate". Even though users like a scenario of having everything automated, they still want to believe that they are in a position to control and are always aware of everything that the system is handling. It is evident from the comments that users want to keep absolute automation as a feature, but would probably completely rely on it when they have absolute confidence over its capability to handle things autonomously. A similar example in this regard would be the case of a pilot operating a commercial aircraft who would be prefer it more if the airplane were on autopilot while cruising. Although, he would also like to have the system informing him about the vital stats of the airplane while it's on autopilot. He would rather rely on his/her skills during landing and take-off of the aircraft. Lack of confidence in automated systems during decisive moments is a common trait found in human beings which in this case is clearly exhibited by the pilot.

2.2.3 Being Notified and Being in Control

"Control" can be the complete manual control of the system or it can be a situation where the user is notified regarding something which can be changed or altered subject to manual intervention. This is basically the system saying that it has an affordance which the user can utilize to better suit his/her convenience. In such a situation, the notification system (perhaps an application for IoT installed on the user's tablet) forms an interface between the machine and the user which serves as

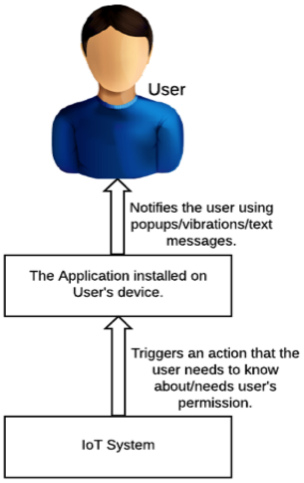
User
Notifies the user using popups/vibrations/text messages.
The Application installed on User's device.
Triggers an action that the user needs to know about/needs user's permission.
IoT System

Figure 2.3: An interface for providing the user with "control"

a medium to control the degree of automation. The entire idea behind having such an interface is to provide the user with control without compromising convenience. This phenomenon is depicted in the figure 2.3.

The assumption here is that the user is being notified about the several important aspects of the system. Being notified even after allowing something to take place is a requirement prevalent among many participants. One of the participants explicitly mentioned he would like periodic reminders about what is being recorded. This leads us to another interesting aspect of such a scenario which is the 'trust'. We assume that the user trusts the feedback from the system. The notification is perceived by the user as a kind of feedback and this leads to an impression of control in the user's mind where he/she is the master and the system is the apprentice. We think this situation is paramount in establishing trust and all participants desired it.

Chapter 3

Related Work

In this chapter, we discuss existing research on privacy-setting interfaces and on privacy prediction.

3.0.1 Personalization in Iot Systems

One of the key features of IoT environments is that they have a high potential for providing personalized services to their users [?, ?, ?]. For example, Russell et al. [?] use unobtrusive sensors and micro-controller to realize a human detection for further providing personalization in a scenario of a family making use of the IoT in their daily living. Henka et al. [?] propose an approach to personalize services in (household) IoT using the Global Public Inclusive Infrastructure's [?] preference set to describe an individual's needs and preferences, and then adapting a smart environment accordingly.

3.0.2 Privacy in Personalized systems

Researchers have shown that privacy can play a limiting role in users' adoption of personalized services [?]. For example, Awad and Krishnan [?] show that privacy concerns inhibit users' use of personalized services, and Sutanto et al. [?] demonstrated that privacy concerns can prevent people from using a potentially beneficial personalized application. Kobsa et al. [?] demonstrate that the personalization provider is an important determinant of users' privacy concerns.

Moreover, research has shown users' willingness to provide personal information to personalized services depends on both the risks and benefits of disclosure [?, ?, ?], and researchers therefore claim that both the benefits and the risks meet a certain threshold [?], or that they should be in balance [?].

3.0.3 Privacy in IoT

The argument that using user-generated data for personalization can result in privacy concerns has also been made in IoT environments [?]. One of the first examples in this regard was the work by, Sheng et al. [?], who showed that users of "u-commerce" services (IoT-driven mobile shopping) felt less inclined to use personalized (rather than non-personalized) u-commerce services, unless the benefits were overwhelming (i.e., providing help in an emergency).

In response, researchers have proposed frameworks with guidelines for evaluating the security and privacy of consumer IoT applications, devices, and platforms [?, ?]. Most of these guidelines are focused on minimizing data acquisition, storage, and collection sources. Along these guidelines, several researchers have proposed architectures that restrict unwanted access to users' data by IoT devices. For example, Davies et al. propose "privacy mediators" to the data distribution pipeline that would be responsible for data redaction and enforcement of privacy policies even before the data is released from the user's direct control [?]. Likewise, Jayraman et al.'s privacy preserving architecture aggregates requested data to preserve user privacy [?].

Other research has considered IoT privacy from the end-user perspective [?], both when it comes to research (e.g., Ur et al. investigated how privacy perceptions differ among teens and their parents in smart security systems installed in homes [?]) and design (e.g., Williams et al. highlight the importance of designing interfaces to manage privacy such that they are usable to the end users of IoT devices [21], and Feth et al. investigated the creation of understandable and usable controls [?]). The current paper follows this approach, by outlining a novel methodology for the development of usable and efficient privacy-setting interfaces and applying it to household IoT privacy management.

3.0.4 Existing privacy control schemes

Smartphones give users control over their privacy settings in the form of prompts that ask whether the user allows or denies a certain app access to a certain type of information. Such prompts are problematic for IoT, because IoT devices are supposed to operate in the background. Moreover, as the penetration of IoT devices in our homes continues to increase, prompts would become a constant noise which users will soon start to ignore, like software EULAs [8] or privacy policies [9].

Pejovic and Musolesi [**?**] presented the design and implementation of an efficient online learner that can serve as a basis for recognizing opportune moments for interruption. The design of the library is based on an in-depth study of human interruptibility. Comparatively, our work tries to find the most suitable privacy-setting profile for each user based on their privacy preference on different household IoT scenarios.

3.0.5 Privacy-Setting Interfaces

Beyond prompts, one can regulate privacy with global settings. The most basic privacy-setting interface is the traditional "access control matrix", which allows users to indicate which entity gets to access what type of information [18]. This approach can be further simplified by grouping recipients into relevant semantic categories, such as Google+'s *circles* [20]. Taking a step further, Raber et al. [15] proposed *Privacy Wedges* to manipulate privacy settings. Privacy Wedges allow users to make privacy decisions using a combination of semantic categorization (the various wedges) and inter-personal distance (the position of a person on the wedge). Users can decide who gets to see various posts or personal information by "coloring" parts of each wedge.

Privacy wedges have been tested on limited numbers of friends, and in the case of household IoT they are likely to be insufficient, due to the complexity of the decision space. To wit, IoT privacy decisions involve a large selection of devices, each with various sensors that collect data for a range of different purposes. This makes it complicated to design an interface that covers every possible setting [21]. A wedge-based interface will arguably not be able to succinctly represent such complexity, and therefore either be impossible, or still lead to a significant amount of information and choice overload.

We propose a data-driven approach to solve this problem: statistical analysis informs the construction of a layered settings interface, while machine learning-based privacy prediction helps us find smart privacy profiles.

3.0.6 Privacy Prediction

Several researchers have proposed privacy prediction as a solution to the privacy settings complexity problem—an approach known as "user-tailored privacy" (UTP) [?]. Systems that implement UTP first predict users' privacy preferences and behaviors based on their known characteristics. They then use these predictions to provide automatic default settings or suggestions in line with users' disclosure profiles, to educate users' about privacy features they are unaware of, to tailor the privacy-setting user interfaces to make it easier for users to engage with their preferred privacy management tools, or to selectively restrict the types of personalization a system is allowed engage in.

Most existing work in line with this approach has focused on providing automatic default settings. For example, Sadeh et al. [17] used a k-nearest neighbor algorithm and a random forest algorithm to predict users' privacy preferences in a location-sharing system, based on the type of recipient and the time and location of the request. They demonstrated that users had difficulties setting their privacy preferences, and that the applied machine learning techniques can help users to choose more accurate disclosure preferences. Similarly, Pallapa et al. [14] present a system which can determine the required privacy level in new situations based on the history of interaction between users. Their system can efficiently deal with the rise of privacy concerns and help users in a pervasive system full of dynamic interactions.

Dong et al. [6] use a binary classification algorithms to give users personalized advice regarding their privacy decision-making practices on online social networks. They found that J48 decision trees provided the best results. Li and et al. [12] similarly use J48 to demonstrate that taking the user's cultural background into account when making privacy predictions improves the prediction accuracy. Our data stems from a culturally homogeneous population (U.S. Mechanical Turk workers), so cultural variables are outside the scope of our study. We do however follow these previous works in using J48 decision trees in our prediction approach.

We further extend this approach using *clustering* to find several smart default policies ("profiles"). This is in line with Fang et al. [7], who present an active learning algorithm that comes up with privacy profiles for users in real time. Since our approach is based on an existing dataset, our algorithm does not classify users in real time, but instead creates a static set of profiles 'offline', from which users can subsequently choose. This avoids cold start problems, and does not rely on the availability of continuous real-time behaviors. This is beneficial for household IoT privacy settings, because users often specify their settings in these systems in a "single shot", leaving the settings interface alone afterwards.

Ravichandran et al. [16] employ an approach similar to ours, using k-means clustering on users' contextualized location sharing decisions to come up with several default policies. They showed that a small number of policies could accurately reflect a large part of the location sharing preferences. We extend their approach to find the best profiles based on various novel clustering approaches, and take the additional step of designing user interfaces that incorporate the best solutions.

3.0.7 Data-driven design

In our previous work [**?**], we leveraged data collected by Lee and Kobsa [11], which asked 200 participants about their intention to allow or reject the IoT features presented in 14 randomized scenarios. They varied the scenarios in a mixed fractional factorial design along the following dimensions: 'Who', 'What', 'Where', 'Reason', 'Persistence'.

We conducted a statistical analysis on this dataset to determine the relative influence of these parameters on users' privacy-related decisions. The outcome informed the design of a 'layered interface', which presents privacy settings with the most prominent influence first, relegating less prominent aspects to subsequently lower layers. Users can use this interface for making manual privacy settings.

We also conducted a machine learning analysis to predict participants' reactions to the scenarios. We used the outcomes of this analysis to develop a "smart" default setting, which preempts the need for many users to manually change their settings [19]. However, since people differ extensively in their privacy preferences [13], it is not possible to achieve an optimal default that is the same for everyone. Instead, different people may require vastly different settings [10, 13, 22]. By partitioning the participants in a number of clusters, we were able to construct a number of 'privacy profiles', which represented a selection of default settings for the user to choose from. These profiles automate (part of) the privacy-setting task.

As noted in the introduction, our current paper builds upon this existing work by applying it to a newly collected dataset focused on household IoT privacy decisions, and by refining both the statistical and machine learning procedures underlying this approach. The resulting procedure can be considered a blueprint for researchers interested in applying data-driven design to their (privacy-)settings interfaces.

Chapter 4

Recommending Privacy Preference for General IoT

In this chapter, we present the work completed to date in the areas of recommending privacy preference for general IoT, including the data-driven design, the dataset that we use, the inspection of users' behaviors using statistical analyses, prediction of users' behaviors using machine learning techniques, and the privacy-setting prototypes that we create based on both statistical and machine learning results.

4.1 Data-driven design

What design process allows us to develop a usable privacy-setting interface for IoT? The development of usable privacy interfaces commonly relies on user studies with existing systems. However, this method is not possible in our IoT control scenario, because the Intel control framework has yet to be implemented [5]. We therefore develop and employ a *data-driven design* methodology, leveraging an existing dataset collected by Lee and Kobsa [11], who asked users whether they would allow or deny IoT devices in their environment to collect information about them. We use this dataset in two phases.

In our first phase, we develop a "layered" settings interface, where users make a decision on a less granular level (e.g., whether a certain recipient is allowed to collect their personal information or not), and only move to a more granular decision (e.g., what types of information this recipient is allowed to collect) when they desire more detailed control. This reduces the complexity of the decisions users have to make, without reducing the amount of control available to them. We use statistical analysis of the Lee and Kobsa dataset to decide which aspect should be presented at the highest layer of our IoT privacy-setting interface, and which aspects are relegated to subsequently lower layers.

In our second phase, we develop a "smart" default setting, which preempts the need for many users to manually change their settings [19]. However, since people differ extensively in their privacy preferences [13], it is not possible to achieve an optimal default that is the same for everyone. Instead, different people may require different settings. Outside the field of IoT, researchers have been able to establish distinct clusters or "profiles" based on user behavioral data [10, 13, 22]. We perform machine learning analysis on the Lee and Kobsa dataset to create a similar set of "smart profiles" for our IoT privacy-setting interface.

The remainder of this paper is structured as follows: We first summarize previous work on privacy in IoT scenarios, and describe the structure of the Lee and Kobsa [11] dataset. We then *inspect* users' behaviors using statistical analysis. Next, we *predict* users' behaviors using machine learning methods. We subsequently present a set of prototypes for an IoT privacy-setting interface. Finally, we conclude with a summary of our proposed procedure and the results of our analysis.

4.1.1 Dataset

This study is based on a dataset collected by Lee and Kobsa [11]. A total of 2800 scenarios were presented to 200 participants (100 male, 99 female, 1 undisclosed) through Amazon Mechanical Turk. Four participants were aged between 18 and 20, 75 aged 20–30, 68 aged 30–40, 31 aged 40–50, 20 aged 50–60, and 2 aged > 60.

Each participant was presented with 14 scenarios describing a situation where an IoT device would collect information about the participant. Each scenario was a combination of five contextual parameters (Table 4.1), manipulated at several levels using a mixed fractional factorial design that allowed us to test main effects and two-way interactions between all parameters.

For every scenario, participants were asked a total of 9 questions. Our study focuses on the **allow/reject** question: "If you had a choice to allow/reject this, what would you choose?", with options "I would allow it" and "I would reject it". We also used participants' answers to three attitudinal questions regarding the scenario:

- **Risk:** How risky or safe is this situation? (7pt scale from “very risky” to “very safe”)
- **Comfort:** How comfortable or uncomfortable do you feel about this situation? (7pt scale)
- **Appropriateness:** How appropriate do you consider this situation? (7pt scale)

In this section we analyze how users’ behavioral intentions to allow or reject the information collection described in the scenario are influenced by the scenario parameters. In line with classic attitude-behavior models [1], we also investigate whether users’ attitudes regarding the scenario—their judgment of risk, comfort, and appropriateness—mediate these effects. This mediation analysis [4] involves the following test:

- **Test 1:** The effect of the scenario parameters (who, what, where, reason, persistence) on participants’ attitudes (risk, comfort, appropriateness).
- **Test 2:** The effect of participants’ attitudes on their behavioral intentions (the allow/reject decision).
- **Test 3:** The effect of the parameters on behavioral intentions, controlling for attitudes.

If tests 1 and 2 are significant, and test 3 reveals a substantial reduction in conditional direct effect (compared to the marginal effect), then we can say that the effects of the scenario parameters on participants’ behavioral intention are mediated by their attitudes. Moreover, if the conditional direct effect is (close to) zero, then the effects are fully (rather than partially) mediated.

4.1.2 Scenario Parameters and Attitude

4.1.2.1 ANOVA Test of Main Effects

To understand the effect of the scenario parameters on participants’ attitudes, we created a separate *linear mixed effects regression* (*lmer*) model with a random intercept (to account for repeated measures on the same participant) for each dependent variable (risk, comfort, appropriateness), using the scenario parameters as independent variables. We employed a forward stepwise procedure, adding the strongest remaining parameter into the model at each step and comparing it against the previous model. Table 4.2 shows that all parameters except **where** have a significant effect on each of the attitudes.

Table 4.1: Parameters used in the experiment. Example scenarios:
"A device of a friend records your video to detect your presence. This happens continuously, while you are at someone else's place, for your safety."
"A government device reads your phone ID to detect your identity. This happens once, while you are in a public place (e.g. on the street), for health-related purposes."

Parameter	**Levels**
Who *The entity collecting the data*	1. Unknown 2. Colleague 3. Friend 4. Own device 5. Business 6. Employer 7. Government
What *The type of data collected and (optionally) the knowledge extracted from this data*	1. PhoneID 2. PhoneID>identity 3. Location 4. Location>presence 5. Voice 6. Voice>gender 7. Voice> age 8. Voice>identity 9. Voice>presence 10. Voice>mood 11. Photo 12. Photo>gender 13. Photo>age 14. Photo>identity 15. Photo>presence 16. Photo>mood 17. Video 18. Video>gender 19. Video>age 20. Video>presence 21. Video>mood 22. Video>looking at 23. Gaze 24. Gaze>looking at
Where *The location of the data collection*	1. Your place 2. Someone else's place 3. Semi-public place (e.g. restaurant) 4. Public space (e.g. street)
Reason *The reason for collecting this data*	1. Safety 2. Commercial 3. Social-related 4. Convenience 5. Health-related 6. None
Persistence *Whether data is collected once or continuously*	1. Once 2. Continuously

Table 4.2: Effect of scenario on attitudes. Each model builds upon and is tested against the previous.

Model	χ^2	*df*	*p*-value
$risk \sim (1\|sid)$			
+who	315.37	6	$< .0001$
+what	67.74	23	$< .0001$
+reason	15.65	5	.0079
+persistence	9.95	1	.0016
+where	7.47	3	.0586
+who:what	166.47	138	.0050
Model	χ^2	*df*	*p*-value
$comfort \sim (1\|sid)$			
+who	334.06	6	$< .0001$
+what	83.24	23	$< .0001$
+reason	18.68	5	.0022
+persistence	14.73	1	.0001
+where	3.25	3	.3544
+who:what	195.07	138	.0001
Model	χ^2	*df*	*p*-value
$appropriateness \sim (1\|sid)$			
+who	315.77	6	$< .0001$
+what	72.87	23	$< .0001$
+reason	23.27	5	.0003
+persistence	8.97	1	.0027
+where	5.46	3	.1411
+who:what	214.61	138	$< .0001$

4.1.2.2 Post-hoc Comparisons

We also conducted Tukey post hoc analyses to better understand how the various values of each parameter influenced the attitudes. **Where** was excluded from these analyses, as it did not have an overall significant effect. Some key findings of these post hoc analyses are:

Who: Participants perceive more *risk* when the recipient of the information is ‘unknown’ than for any other recipient (d range = [0.640, 1.450] and all ps $< .001$, except for ‘government’: $d = 0.286$, $p < .05$). ‘Government’ is the next most risky recipient (d range = [0.440, 1.190], all ps $< .001$). Participants consider their ‘own device’ the least risky (d range = [0.510, 1.450], all ps $< .001$). Similar patterns were found for *comfort* and *appropriateness*.

Reason: Participants were more *comfortable* disclosing information for the purpose of ‘safety’ than for any other reason except ‘health’ (d range = [0.230, 0.355], all ps $< .05$). They also believe that disclosing information for the purpose of ‘health’ or ‘safety’ is more *appropriate* than for ‘social’ or ‘commercial’ purposes (d range = [0.270, 0.310], all ps $< .05$).

Persistence: Participants were more *comfortable*, found it more *appropriate*, and less *risky* to disclose their information 'once' rather than 'continuously' ($d = 0.146$, $p < .01$).

What: This parameter has a large number of values, so we decided to selectively test planned contrasts instead of post-hoc tests. We first compared different mediums (voice, photo, video) regardless of what is being inferred:

- Participants were significantly more *comfortable* with 'voice' than 'video' ($d = 0.260$, $p = .005$), and found 'voice' less *risky* ($d = -0.239$, $p = .005$) and more *appropriate* ($d = 0.217$, $p = .015$) than 'video'.
- Participants were significantly more *comfortable* with 'voice' than 'photo' ($d = 0.201$, $p = .007$) and found 'voice' more *appropriate* than 'photo' ($d = 0.157$, $p = .028$). There was no significant difference in terms of *risk* ($p = .118$).
- No differences were found between 'photo' and 'video' in terms of *risk* ($p = .24$), *comfort* ($p = .35$) and *appropriateness* ($p = .26$).

We also compared different inferences (e.g. age, gender, mood, identity) across mediums. The following planned contrasts were significant (all others were not):

- Participants were significantly more *comfortable* ($d = 0.363$, $p = .028$) and found it more *appropriate* ($d = 0.371$, $p = .018$) to reveal their 'age' rather than their 'identity'.
- Participants were significantly more *comfortable* ($d = 0.363$, $p = .008$) and found it more *appropriate* ($d = 0.308$, $p = .024$) to reveal their 'presence' rather than their 'identity'.

4.1.2.3 Interaction effects

We also checked for two-way interactions between the scenario parameters. The only significant interaction effect observed was between **who** and **what**. The last line of each section in Table 4.2 shows the results of adding this interaction to the model. Due to space concerns, we choose not to address the post-hoc analysis of the $7 * 24 = 168$ specific combinations of who and what.

4.1.3 Attitude and Behavioral intention

To test the effects of participants' attitudes on their allow/reject decision, we ran a *generalized linear mixed effects regression* (*glmer*) with a random intercept and a logit link function to

Table 4.3: Effect of attitudes and scenario on allow/reject.

Model	OR	χ^2	*df*	*p*-value
$allow \sim (1\|sid)$				
+risk	0.25	1005.24	1	$< .0001$
+comfort	5.04	723.27	1	$< .0001$
+appropriateness	3.47	128.17	1	$< .0001$
+who		8.80	6	.1851
+what		26.07	23	.2976
+reason		19.33	5	.0017
+persistence		12.69	1	.0004

Table 4.4: Effect of scenario on allow/reject, *not* controlling for attitudes.

Model	χ^2	*df*	*p*-value
$allow \sim (1\|sid)$			
+who	221.36	6	$< .0001$
+what	78.55	23	$< .0001$
+reason	21.95	5	.0005
+persistence	20.64	1	$< .0001$

account for the binary dependent variable. We found significant effects of all the three attitudes on participants' allow/reject decision (see Table 4.3). Each 1-point increase in **risk** results in a 4.04-fold decrease in the odds that the scenario will be allowed ($p < .0001$). Each 1-point increase in **comfort** results in a 5.04-fold increase ($p < .0001$), and each 1-point increase in **appropriateness** results in a 3.47-fold increase ($p < .0001$).

4.1.4 Mediation Analysis

The bottom half of Table 4.3 shows the *conditional* effects of the significant parameters (who, what, reason, persistance) on participants' allow/reject decision, controlling for attitude. **Who** and **what** are no longer significant; these effects are thus fully mediated by attitude. The effects of **reason** and **persistance** are still significant, but smaller than the marginal effects (i.e., without controlling for attitude, see Table 4.4)—their χ^2s are reduced by 12% and 39%, respectively. This means that the mediation effect was substantial in all cases. The final mediation model is displayed in Figure 4.1.

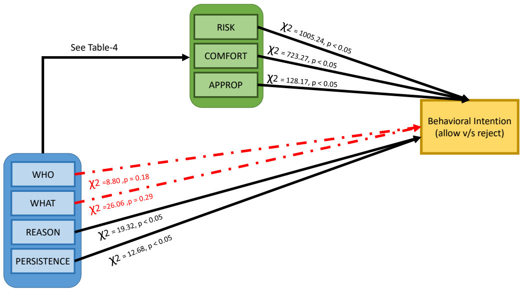

Figure 4.1: Mediation model of the effect of scenario parameters on participants' intention to allow/reject the scenario, mediated by attitudinal factors

4.1.5 Discussion of Statistical Results

Our statistical results show several patterns that can inform the development of an IoT privacy-setting interface. We find that **who** is the most important scenario parameter, and should thus end up at the top layer of our interface. People are generally concerned about IoT scenarios involving unknown and government devices, but less concerned about about data collected by their own devices. Mistrust of government data collection is in line with Li et al.'s finding regarding US audiences [12].

What is the next most important scenario parameter, and its significant interaction with **who** suggests that some users may want to allow/reject the collection of different types of data by different types of recipients. Privacy concerns are higher for photo and video than for voice, arguably because photos and videos are more likely to reveal the identity of a person. Moreover, people are less concerned with revealing their age and presence, and most concerned with revealing their identity.

The **reason** for the data collection may be used as the next layer in the interface. Health and safety are generally seen as acceptable reasons. **Persistence** is less important, although one-time collection is more acceptable than continuous collection. **Where** the data is being collected does not influence intention at all. This could be an artifact of the dataset: location is arguably less prominent when reading a scenario than it is in real life.

Finally, participants' attitudes significantly (and in some cases fully) mediated the effect of scenario parameters on behavioral intentions. This means that these attitudes may be used as a valuable source for classifying people into distinct groups. Such attitudinal clustering could capture a significant amount of the variation in participants in terms of their preferred privacy settings, espcially with respect to the **who** and **what** dimensions.

Chapter 5

Recommending Privacy Perference for Household IoT

In this chapter, we present the work completed to date in the areas of designing for privacy for Household IoT. We extend and improve upon the previously-developed data-driven approach to design privacy-setting interfaces for users of household IoT devices.

Chapter 6

Recommending Privacy Perference for Fitness IoT

In this chapter, we present the work completed to date in the areas of designing for privacy for Fitness IoT.

Chapter 7

Proposed Work

Chapter 8

Conclusion

Appendices

Bibliography

[1] Icek Ajzen and Martin Fishbein. Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological bulletin*, 84(5), 1977.

[2] Paritosh Bahirat, Yangyang He, and Bart P. Knijnenburg. Exploring Defaults and Framing effects on Privacy Decision Making in Smarthomes. In *USENIX symposium on Usable Privacy and Security*, Baltimore, MD, August 2018.

[3] Paritosh Bahirat, Yangyang He, Abhilash Menon, and Bart Knijnenburg. A data-driven approach to developing iot privacy-setting interfaces. In *23rd International Conference on Intelligent User Interfaces*, pages 165–176. ACM, 2018.

[4] Reuben M Baron and David A Kenny. The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of personality and social psychology*, 51(6):1173–1182, 1986.

[5] Richard Chow, Serge Egelman, Raghudeep Kannavara, Hosub Lee, Suyash Misra, and Edward Wang. HCI in Business: A Collaboration with Academia in IoT Privacy. In Fiona Fui-Hoon Nah and Chuan-Hoo Tan, editors, *HCI in Business*, number 9191 in Lecture Notes on Computer Science. Springer, 2015.

[6] Cailing Dong, Hongxia Jin, and Bart P Knijnenburg. Ppm: A privacy prediction model for online social networks. In *International Conference on Social Informatics*, pages 400–420, 2016.

[7] Lujun Fang and Kristen LeFevre. Privacy wizards for social networking sites. In *Proceedings of the 19th international conference on World wide web*, pages 351–360, 2010.

[8] Nathaniel Good, Rachna Dhamija, Jens Grossklags, David Thaw, Steven Aronowitz, Deirdre Mulligan, and Joseph Konstan. Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, pages 43–52, 2005.

[9] Carlos Jensen and Colin Potts. Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. In *2004 Conference on Human Factors in Computing Systems*, pages 471–478, 2004.

[10] Bart P Knijnenburg, Alfred Kobsa, and Hongxia Jin. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies*, 71(12):1144–1162, 2013.

[11] Hosub Lee and Alfred Kobsa. Understanding user privacy in internet of things environments. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 407–412, 2016.

[12] Yao Li, Alfred Kobsa, Bart P Knijnenburg, and MH Carolyn Nguyen. Cross-cultural privacy prediction. *Proceedings on Privacy Enhancing Technologies*, 2:93–112, 2017.

[13] Judith S Olson, Jonathan Grudin, and Eric Horvitz. A study of preferences for sharing and privacy. In *CHI'05 extended abstracts on Human factors in computing systems*, pages 1985–1988, 2005.

[14] Gautham Pallapa, Sajal K Das, Mario Di Francesco, and Tuomas Aura. Adaptive and context-aware privacy preservation exploiting user interactions in smart environments. *Pervasive and Mobile Computing*, 12:232–243, 2014.

[15] Frederic Raber, Alexander De Luca, and Moritz Graus. Privacy wedges: Area-based audience selection for social network posts. In *Proceedings of the 2016 Symposium on Usable Privacy and Security*, 2016.

[16] Ramprasad Ravichandran, Michael Benisch, Patrick Gage Kelley, and Norman M Sadeh. Capturing social networking privacy preferences. In *Proceedings of the 2009 Symposium on Usable Privacy and Security*, pages 1–18, 2009.

[17] Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, and Jinghai Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*, 13(6):401–412, 2009.

[18] R. S. Sandhu and P. Samarati. Access control: principle and practice. *IEEE Communications Magazine*, 32(9):40–48, 1994.

[19] N. Craig Smith, Daniel G. Goldstein, and Eric J. Johnson. Choice Without Awareness: Ethical and Policy Implications of Defaults. *Journal of Public Policy & Marketing*, 32(2):159–172, 2013.

[20] Jason Watson, Andrew Besmer, and Heather Richter Lipford. +Your circles: sharing behavior on Google+. In *Proceedings of the 8th Symposium on Usable Privacy and Security*, pages 12:1–12:10, 2012.

[21] Meredydd Williams, Jason RC Nurse, and Sadie Creese. The perfect storm: The privacy paradox and the internet-of-things. In *11th International Conference on Availability, Reliability and Security*, pages 644–652, 2016.

[22] Pamela J Wisniewski, Bart P Knijnenburg, and Heather Richter Lipford. Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies*, 98:95–108, 2017.