Recommending Privacy Settings for Internet-of-Things

A Dissertation by
Yang He
Dec 2019

Submitted to the graduate faculty of the
School of Computing
In Partial Fulfillment of the Requirements
for the Dissertation
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

Dr. Ilaria Torre
Committee Member

Abstract

Privacy concerns have been identified as an important barrier to the growth of IoT. These concerns are exacerbated by the complexity of manually setting privacy preferences for numerous different IoT devices. Hence, there is a demand to solve the following, urgent research question: How can we help users simplify the task of managing privacy settings for IoT devices in a user-friendly manner so that they can make good privacy decisions?

To solve this problem in the IoT domain, a more fundamental understanding of the logic behind IoT users' privacy decisions in different IoT contexts is needed. We, therefore, conducted a series of studies to contextualize the IoT users' decision-making characteristics and designed a set of privacy-setting interfaces to help them manage their privacy settings in various IoT contexts based on the deeper understanding of users' privacy decision behaviors.

In this dissertation, we first present three studies on recommending privacy settings for different IoT environments, namely general/public IoT, household IoT, and fitness IoT, respectively. We developed and utilized a "data-driven" approach in these three studies—We first use statistical analysis and machine learning techniques on the collected user data to gain the underlying insights of IoT users' privacy decision behavior and then create a set of "smart" privacy defaults/profiles based on these insights. Finally, we design a set of interfaces to incorporate these privacy default/profiles. Users can apply these smart defaults/profiles by either a single click or by answering a few related questions. The biggest limitation of these three studies is that the proposed interfaces have not been tested, so we do not know what level of complexity (both in terms of the user interface and the in terms of the profiles) is most suitable. Thus, in the last study, we address this limitation by conducting a user study to evaluate the new interfaces of recommending privacy settings for household IoT users. The results show that our proposed user interfaces for setting household IoT privacy settings can improve users' satisfaction. Our research can benefit IoT users, manufacturers,

and researchers, privacy-setting interface designers and anyone who wants to adopt IoT devices by providing interfaces that put their most prominent concerns in the forefront and that make it easier to set settings that match their preferences.

Author's Publications on this topic

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

1. **He, Y.** (2019): Recommending Privacy Settings for IoT. In 24th International Conference on Intelligent User Interfaces (IUI '19 Companion), March 17–20, 2019, Marina del Ray, CA.

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

3. Sanchez, O., Torre, I., **He, Y.**, Knijnenburg, B.P. (2018) A Recommendation Approach for User Privacy Preferences in the Fitness Domain. User Modeling and User-Adapted Interaction (UMUAI).

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

5. Bahirat, P., **He, Y.**, Menon, A., Knijnenburg, B.P. (2018): A Data-Driven Approach to Developing IoT Privacy-Setting Interfaces. In 23th International Conference on Intelligent User Interfaces, 2018, Tokyo, Japan.

Outline

List of Tables

List of Figures

Chapter 1

Introduction

During the last two decades, computers have evolved into all kinds of small footprint internet-connected devices that are capable of: 1) tracking us as we move about the built environment such as public spaces, offices, schools, universities; 2) being embedded in household appliances such as smart phones, TVs, refrigerators, light fixtures and thermostats to create 'smart home' environments; 3) tracking our personal data daily as we wear them, such as smart watches, and fitness trackers. All these computers/devices have been integrated seamlessly into people's lives, which is defined as "Internet of Things". By using all kinds of wireless sensor technologies (e.g. RFID, cameras, microphones, GPS, and accelerometers) and artificial intelligence, these internet-connected devices are able to gain knowledge of their surrounding and their users, exchange data with each other, monitor and control remotely controlled devices, and further interact with third-parties to provide us better personalized services, recommendations, and advertisements. They have been widely used in many fields, such as tracking, transportation, household usage, healthcare and fitness [75, 107, 60, 58, 47].

A wide range of well-respected organizations has estimated that IoT will grow rapidly and bring huge social and economic potential. For example, Gartner [29] has predicted over 21 billion IoT devices will be in use by 2020; IoT product and service suppliers will generate incremental revenue exceeding $300 billion. IDC forecasts a global market for IoT will grow from $1.9 trillion in 2013 to $7.1 trillion in 2020 [96]. However, the rise of IoT also comes with a number of key security and privacy concerns. These include facilitation of the collection of large amounts of consumer data [128], processing and storing the data in ways unexpected by the consumer [81], and privacy

and security breaches [81, 139].

IoT devices are intended to collect information from the users to realize their functionalities. Technical solutions can be used to minimize the data collected for such functionality [67, 92, 122], but arguably, any useful functionality would necessitate at least some amount of personal data. Therefore, users will have to manage a trade-off between privacy and functionality: a solution that is fully privacy preserving will be limited in functionality, while a fully functional IoT solution would demand extensive data collection and sharing with others. Research has shown that user employ a method called *privacy calculus*—i.e. that they make disclosure decisions by trading off the anticipated benefits with the risks of disclosure [23, 70, 110]. However, as the diversity of IoT devices increases, it becomes increasingly 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 carefully read the privacy policies or the privacy-settings that are provided to them [28, 42]. For example, one found that 59% of users say they have read privacy notices, while 91% thought it important to post privacy notices [28]. In [115], Tuunainen et al. find that only 27% participants are aware that Facebook can share their information with people or organisations outside of Facebook for marketing purpose as their privacy policy.

There are several reasons for this problem: i) Users will pay more attention to the benefit than potential risks from using IoT devices or services [36]. ii) The privacy policies are too long, or the privacy setting of such devices are too complicated, making users irritated to finish reading/setting them [85]. iii) As the number IoT devices rapidly increases, the numbers and options of privacy setting for all the IoT devices will also increase exponentially. Moreover, each device will have its own fine-grained privacy settings (often hidden deep within an unassuming "other settings" category in the settings interface), and many inter-dependencies exist between devices — both in privacy and functionality. Therefore, there is a large chance that users would make inconsistent privacy decisions that either limit functionality of their IoT devices or that do not protect their privacy in the end. In addition, the current user interface for setting privacy preferences of present IoT devices is imperfect even for a smartphone, not to mention the complexity of manually setting privacy preferences for numerous different other IoT devices. Hence, there is an urgent demand to solve the following research question:

Can we simplify the task of managing privacy setting for users of different IoT contexts?

Prior research (chapter 2) has explored different approaches to this problem in other domains, including providing 1) transparency and control [30, 1, 61, 13, 17], and 2) privacy nudges [5, 79, 37, 79]. However, neither of them provides a satisfying solution in the IoT domain. Providing transparency and control does give users the freedom of managing their privacy in IoT according to their own privacy decisions, but privacy decision making is often not rational [61]. Thus, such extra transparency and control may increase the difficulty of setting appropriate privacy for users. Privacy nudges are usually implemented in the form of prompts, which will create constant noises given that the IoT systems usually work in the background. At the same time, they lack personalization to the inherent diversity of users' privacy preferences and the context-dependency of their decisions.

To solve these problems in the IoT domain, a more fundamental understanding of the logic behind IoT users' privacy decisions in different IoT contexts is needed. I therefore conducted a series of studies to contextualize the IoT users' decision making characteristics, and designed a set of privacy-setting interfaces to help them manage their privacy settings in various IoT contexts based on the deeper understanding of users' privacy decision behavior.

In this dissertaion, I first present the background and related work of this dissertation in Chapter 2 and 3. Then, I present three studies on recommending privacy settings for different IoT environments, namely general/public IoT in Chapter 4, household IoT in Chapter 5, and fitness IoT in Chapter 6, respectively. One should observe that the above three studies follow an decreasing order in terms of the IoT context scope. In the first study, I focused on the privacy decision regarding the entities collecting information from the users, while in the following two studies the context was moved to a more narrow environment (household IoT and fitness IoT), which shifts the focus to a more contextual evaluation of the content or nature of the information. This explains why in the first two studies, the dimensions used to analyze the context are the parameters of the corresponding IoT scenarios; and for the third study, the focus is on the fitness tracker permission questions. Note that the above three works all utilized a " data-driven design" — We first use statistical analysis (applicable to the first two works) and machine learning techniques on the collected user data to gain the underlying insights of IoT users' privacy decision behavior; and then a set of "smart" privacy defaults/profiles were created based on these insights. Finally, we design a set of interfaces to incorporate these privacy default/profiles. Users can apply these smart defaults/profiles by either a single click (applicable to the first two works) or by answering a few related questions (applicable to the third work). To test the presented interfaces and uncover what level of complexity (both

in terms of the user interface and the in terms of the profiles) is most suitable, I conducted a user study to evaluate the new interface of recommending privacy-settings for household IoT in Chapter 7. Finally, I conclude this dissertation with contributions and limitations in Chapter 8.

Chapter 2

IoT technology and IoT Acceptance

In this chapter, we first discuss how Internet-of-Things enter into people's daily lives, how people benefit from using IoT, what kinds of disadvantages IoT has brought, and the aspects that current IoT research has focused on. We then look at what factors are affecting potential IoT users when they are considering *adopting* this new technology.

When users are considering adopting new IoT devices, they want to take the benefits of using IoT devices by sharing and disclosing certain personal information to get a more personalized experience [41]. However, such disclosed information could be accessed by other smart devices owned by themselves, other people, organizations, the government, or some third-parties with good or bad purpose, which brings privacy risks to the users [83]. Thus, we attempt to obtain a clear understanding of the IoT acceptance model before our further research for the following reasons: 1) The factors that affect users' adopting phase may have a high chance to also have an effect on users' real using phase, which could help us understand how the IoT users make privacy decisions when they share their personal data in different IoT contexts; 2) These factors may further affect how we design the user interface for setting privacy preferences and recommend privacy-settings for different IoT contexts; 3) These factors can potentially help us develop the scales to evaluate the interfaces that we design, and build a theoretical model.

2.1 IoT Technology

The term "Internet of Things" (IoT) was first introduced by Kevin Ashton in the context of supply chain management in 1999 [7]. Atozri et al. define IoT as a pervasive presence around us of a variety of things or objects - such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through a unique addressing scheme, are able to interact with each other and cooperate with their neighbors to reach common goals [8]. As various wireless sensor technologies (e.g. RFID, embedded sensors, and actuator nodes) and artificial intelligence have advanced rapidly during the last two decades, the definition of IoT has evolved to more broadly covering a wide range of monitoring and control applications based on a network of sensing and actuating devices that are controlled remotely through the Internet in many fields, such as tracking, transportation, household usage, healthcare and fitness [75, 107, 60, 58, 47].

IoT can benefit both organizations and individual consumers in all above-mentioned domains by enhancing data collection, enabling real-time response, improving access and control of internet-connected devices, increasing efficiency, productivity, and satisfaction [128, 95]. With such huge social and economic potential, IoT is estimated to grow rapidly by a wide range of well-respected organizations. However, there exist several key security and privacy concerns associated with the rise of the IoT, including data processing and storage, privacy and security breaches[128, 81, 139].

Previous studies mostly focused on the technical issues of IoT technologies [33, 71, 104]. For example, Uckelmann et al. systematically explained the architecture of future IoT [116]. Chen et al. present a vision of IoT's applications in China [21]. Guinard et al. described the IoT's best practices based on the web technologies and proposed several prototypes using the web principles, which connect environmental sensor nodes, energy monitoring systems, and RFID-tagged objects to the web [45]. However, little attention has been devoted to, from the perspective of individual consumers, understanding how the user of IoT will trade off the above mentioned benefits and privacy concerns of IoT technology when they consider adopting it [4, 39, 86].

Furthermore, researchers identified security and privacy issues as the major challenges for consumer acceptance of the IoT technology's user-oriented IoT applications [83]. Arguably, if the users find that their privacy demands can not be satisfied when using IoT devices after adopting them, they would probably finally give up using these devices.

2.2 Model the Acceptance of IoT

In this section, we first discuss the original Technology Acceptance Model and the adapted Unified Theory of Acceptance and Use of Technology (UTAUT) model. Then we look at what are the factors that affect potential IoT users to adopt IoT systems.

2.2.1 Technology Acceptance Model

The Technology Acceptance Model (TAM) is arguably the most popular model that explains how users come to accept and use a technology [26]. TAM suggests that an individual's *Behavioral Intention* to Use an information technology is significantly dependent upon the individual's *Perceived Usefulness* and *Perceived Ease Of Use* of that information technology. Specifically, perceived usefulness is the extent to which an individual believes that using a particular information technology will have a positive impact on his/her performance. Perceived ease of use is the extent to which an individual perceives that using a particular information technology will be free of effort. TAM also proposes that perceived ease of use can explain the variance in perceived usefulness. TAM has been applied to a wide range of technology adoption contexts [134], such as the adoption of PC [120], smartphones [90], mobile marketing [12], Internet banking [94], facebook [74, 98], and online shopping [40].

2.2.2 UTAUT

The unified theory of acceptance and use of technology (UTAUT) is a technology acceptance model proposed by Venkatesh et al. [121]. Compared to TAM, UTAUT identifies four key factors: 1) performance expectancy, 2) effort expectancy, 3) social influence, and 4) facilitating conditions, related to predicting behavioral intention to use a technology and actual technology use primarily in organizational contexts. The first three factors are theorized and found to influence behavioral intention to use a technology, while behavioral intention and facilitating conditions determine technology use. UTAUT also identifies four moderators (i.e., age, gender, experience, and voluntariness).

UTAUT has been applied or extended in many contexts, such as electronic learning [125], e-government [127], and cloud computing [77]. UTAUT is developed upon previous models of technology adoption, and designed specifically to investigate users' acceptance of a new technology. Thus, it has explanatory power higher than previous models.

2.2.3 The Acceptance of IoT

Researchers have attempted to identify the factors that affect the acceptance of IoT by customers. Acquity Group [44] conducted a user study investigating the concerns of customers to adopt the IoT. Based on more than 2000 US-based customer survey, They find that awareness of the technology, usefulness, price (cost), security, privacy are the main concerns of the customers. In [39], Gao and Bai present a user study (N=368) to investigate the factors that affect the acceptance of IoT in China. They used the factors of TAM (i.e. perceived ease of use and perceived usefulness) along with other factors such as trust, social influence, perceived enjoyment, and perceived behavioral control. Their results show that perceived usefulness, perceived ease of use, social influence, perceived enjoyment, and perceived behavioral control have significant effect on users' behavioral intention to use the IoT. In [73], Lee and Shin develop and test factors determining user acceptance of IoT services by extending current UTAUT model to include an extra hindering condition to explain the dual attitudes of users such as technical anxiety.

2.2.4 A preliminary study (original work)

We also conducted a preliminary/pilot study on Clemson University campus (N=15) with the aim to investigate the various factors that affect the adoption of IoT by interviewing with potential IoT users. The interviews were approximately 30-50 minutes in length and covered a wide range of open questions related to IoT. These questions asked participants about their personal preferences regarding to the technology and self-perceived tech savviness. In this study, the conversations with our participants were recorded only after obtaining their consent. This study was approved by IRB. The entire recorded conversation was then transcribed manually. We then extracted keywords from participants' statements during the interview, such as "privacy" or "ease of use". These keywords were then grouped using card sorting and affinity diagram techniques. We then used a grounded approach to creating a theory, which is shown in Figure 2.1.

The results showed similar findings as aforementioned work [39, 4]. However, in our study, we noticed an interesting phenomenon that no literature has mentioned – once trust with the manufacturers is established, it can propagate from the manufacturers to a third-party, which users are not aware of or even know about in the first place. We define this phenomenon as **Trust Chain**. An example of Trust Chain from our interview is:

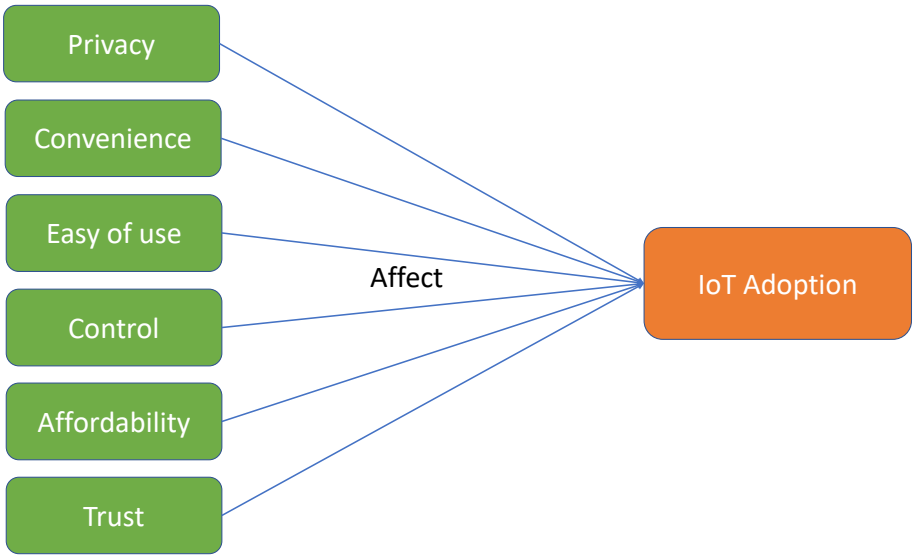


Figure 2.1: The factors that affecting users' adoptions of IoT found in our study

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 transferred 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."

As shown in Figure 2.2, Trust Chain is established mostly because of the trust from the users to the manufacturers (i.e. the brand of the devices), and can arguably be categorized as an emotional behavior because users would not have a clear sight at the benefits and risks when they choose to trust the third parties that manufacturers choose to shared their data with. Such benefits and risks have been defined as abstract benefits and risk. One of our current undergoing research has shown that, in IoT domain, users are more likely to perceive concrete benefits and abstract risks, resulting this emotional behavior phenomenon. Such behavior could bring harm to their privacy and security. To be more rational, we suggest users to investigate the third parties that will handle their

Figure 2.2: Trust Chain

personal data. Thus, we suggest the manufacturer/designers of the IoT privacy to provide users transparency and control on what third parties they will share users' data with to reduce the risks of insecure Trust Chain sharing behavior.

Knowing all these factors that affect users' decision on adopting IoT device will help us develop the scales for evaluating our designed privacy-setting interfaces in our proposed work (Chapter 7). Based on the insights gained from this study, we encourage the designers of IoT privacy-setting interfaces to face the difficult challenge of maximizing the usability and the privacy control of the user interface while minimizing the privacy threats to the users, making IoT more acceptable.

2.3 Summary

In this chapter, I have noted the following points: 1) IoT have grown in use rapidly with the advancing of RFID and other wireless sensor technologies. 2) IoT have brought convenience and enjoyment to our daily lives. 3) Privacy concern is an important factor that affects users' decisions when adopting IoT. 4) The acceptance of IoT is still not systematically examined.

In the next chapter, we discuss the reason that causes the privacy issues in IoT, how effective existing privacy control schemes are, and the work that aims to help users protect their privacy more effectively.

Chapter 3

Privacy setting technologies in IoT

In chapter 2, we discuss the development of IoT and its acceptance model. As IoT systems gain popularity and bring privacy issues at the same time, it is urgent to study the cause of these privacy issues. By doing this, we can improve our design of IoT applications to protect IoT users' privacy, and make IoT more acceptable.

3.1 Privacy Preference

Researchers have attempted to examine users' privacy preferences in different areas, such as Social Networks and mobile applications. Research has shown people differ extensively in their privacy settings [88], but can be clustered into groups [6, 65]. In [131, 62], Facebook users are found to belong to one of 6 types of privacy profiles which range from Privacy Maximizers to Minimalists. In the health/fitness domain, emerging sensors and mobile applications allow people to easily capture fine-grained personal data related to long term fitness goals. Brar and Kay discover that users' preferences change for every fitness/heath index. Weight was found to be the most sensitive index [16].

At the same time, users are found to have difficulties managing their privacy settings with current privacy-setting schemes. Liu et al. use an online survey (N=200) to investigate the difference between the desired privacy settings and the actual privacy settings of Facebook users. Their results show that 63% of the privacy settings for photo sharing did not match the users' desired settings. In [82], Madejski et al. conduct user studies to find the difference between Facebook users' sharing

intentions and their actual privacy settings. Their results show that there is at least one violation in the privacy settings for each of the 65 participants.

The reasons for the failure of existing privacy-setting schemes are diverse. One reason for this is that the increasing number of privacy rules make manual privacy configuration excessively challenging for normal users [38]. Knijnenburg et al. discover that people's information disclosure behaviors vary along multiple dimensions [65]. People can be classified along these dimensions into groups with different "disclosure styles". This result suggests that we could classify users into their respective privacy groups and adapt their privacy practices to the disclosure style of this group to satisfy different types of information and users. However, on the other hand, more privacy policies would lead to more decision-making and more burden for users. Note that in the IoT environment, the number for different IoT devices could be vast, which could potentially make choosing adequate privacy settings a very challenging task that is likely to result in information and choice overload [130]. Therefore, in this thesis, we will use a data-driven approach (machine learning techniques) to discover suitable smart privacy profiles, which are generated from the results of both statistical analysis and machine learning techniques, for users with different "disclosure styles".

3.2 Privacy in IoT

IoT systems are capable of providing a highly personalized services to their users [118, 31, 41]. Henka et al. [49] propose an approach to personalize services in household IoT using the Global Public Inclusive Infrastructure's [119] preference set to describe an individual's needs and preferences, and then adapting a smart environment accordingly. Russell et al. [100] use unobtrusive sensors and a micro-controller to realize human detection to provide personalization in a household IoT environment.

Researchers have shown that privacy plays a limiting role in users' adoption of personalized services [111]. For example, Awad and Krishnan [9] show that privacy concerns inhibit users' use of personalized services, and Sutanto et al. [108] demonstrated that privacy concerns can prevent people from using a potentially beneficial personalized application. Kobsa et al. [68] 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 [93, 50, 52], and researchers

therefore claim that both the benefits and the risks should meet a certain threshold [113], or that they should be in balance [20].

The argument that using user-generated data for personalization can result in privacy concerns has also been made in IoT environments [135, 39, 4]. One of the first examples in this regard was the work by Sheng et al. [105], 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 [91, 80]. 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 [24]. Likewise, Jayraman et al.'s privacy preserving architecture aggregates requested data to preserve user privacy [56].

Other research has considered IoT privacy from the end-user perspective [35], 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 [117]) 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 [130], and Feth et al. investigated the creation of understandable and usable controls [35]). We followed this approach and developed a novel data-driven approach to developing usable and efficient privacy-setting interfaces for several different IoT contexts.

3.3 Existing Privacy Setting Models

Previous studies in smartphone privacy have shown that the current smartphone privacy interfaces lack the potential to provide the necessary user privacy information or control for both Android and iOS systems [78]. Several solutions have been proposed to improve mobile privacy protection and offer users more privacy control [34, 14]. These lead into rapid improvement of privacy management of current mobile systems, providing more control on the user's privacy settings.

Android system mainly use Ask On Install (AOI) and Ask On First Use (AOFU) models for

privacy settings [114, 129]. In the AOI model, the smartphone permissions are asked in bulk before installing a new app. The user's option is only to allow or deny all, which clearly gives less privacy control. Also, only few users would read or pay attention to the privacy settings when installing the app, and even fewer users can understand their meaning [34, 59]. Several third-party apps have been developed to cope with this problem, such as Turtleguard [114] and Mockdroid [14]. In the AOFU model [114], permissions are only asked during the first use of an app or when some function of the app is demanding a specific permission of the smartphone. In this case, the user will trade off his privacy (data sharing) and the functionality of the app. Users can also revisit and review permissions in their phone privacy settings for each app. This model makes users more informed and gives them more control compared to AOI [37].

A few privacy management solutions were developed to simplify the task of controlling personal data for smartphone users. For instance, ipShield [18] is a context-aware privacy framework for mobile systems that provides users with great control of their data and inference risks. My Data Store [123] offers a set of tools to manage, control and exploit personal data by enhancing an individual's awareness of the value of their data. Similarly, Databox [19] enables individuals to coordinate the collection of their personal data, and make those data available for specific purposes. However, these data managers do not include user privacy profiling and recommendation in the complex IoT environment. Privacy can also be protected by providing different anonymity levels of data that are given to third parties. However, it might not be possible to implement the most effective privacy standards such as data obfuscation due to numerous trade-offs and restrictions, especially in the health care and fitness domain.

In the smartphone domain, active privacy nudging is an effective scheme to increase users' awareness [5]. Privacy nudging allows users to be informed about both their privacy settings and how third party applications access their data [79, 37]. In a study by Liu et al., 78.7% [79] of the nudges were adopted by smartphone users. However, such active nudges 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, nudging would become a constant noise which users would soon start to ignore, like software EULAs [43] or privacy policies [57]. In addition, privacy nudges lack the personalization and provide only a general recommendation.

3.4 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 [102]. This approach can be further simplified by grouping recipients into relevant semantic categories, such as Google+'s *circles* [126]. Taking a step further, Raber et al. [97] 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 [130]. 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 used 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.

3.5 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) [63]. 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. [101] 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. [89] 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. [27] 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. [76] 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. [32], 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. [99] 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.

In this dissertation, we extend this *clustering* 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 for different IoT contexts.

3.6 Summary

In this chapter, we have noted following points: 1) Existing research has shown that people are extensively different in their privacy settings, but can be grouped. 2) People are bad at managing privacy settings using currently privacy setting schemes. 3) Privacy prediction can be used by utilizing machine learning algorithms to help design a new privacy-setting interface to simplify the task of managing privacy setting for users. It is possible that we can leverage the user diversity and use the predictive approach to develop privacy-setting interfaces for the users. Thus, in the next chapter, we will present how we design for privacy in the general/public IoT context using a data-driven manner, the contributions and the limitations of our work.

Chapter 4

Recommending Privacy Settings for General/Public IoT

4.1 Introduction

In chapter 2 and 3, we have discussed the benefits and risks of IoT technology, and the key factors affecting users to adopt IoT systems/devices, the privacy risks caused by inappropriate privacy disclosure. We also discussed that people's information disclosure behaviors vary along multiple dimensions [65], which enables us to classify users into their respective privacy groups and adapt the privacy practices to their disclosure styles.

Current privacy control schemes make it difficult for IoT users to manually configure their privacy settings. In this chapter, we developed a data-driven approach to solve this problem: statistical analysis is used to inform the construction of a layered settings interface, while machine learning-based algorithms are used to predict people's privacy decisions and help us find most suitable smart privacy profiles. By using this data-driven approach, we developed a set of "smart defaults/profiles", which are able to help user configure their IoT privacy settings with a single click. Note that the novelty of our work is not about the statistical analysis and the machine learning techniques that we used; the real invention is that we are using these techniques (a data-driven approach) to have a direct influence on design of privacy interface settings. Arguably, there is no existing similar work in this area.

In this chapter, we intend to answer the following questions:

- Q1: Is our data-driven approach useful in the general/public IoT context?
- Q2: What results can be achieved by using our approach?

By general/public IoT, we are referring to those IoT devices deployed in public space, outside people' home, where people have little control over the data collection practices of the devices. These IoT devices can be operated by many entities (i.e. government, employers, friends, colleagues, etc) to collect data with or without people's awareness. Different types of data, such as photos, videos, or locations, can be collected to track people or provide convenience, health-related or social-related information/advice. Due to the high uncertainty and low Controllability, general/public IoT can cause various privacy risks and concerns. The demand to get notified about surrounding public IoT devices or to be able to control these devices is urgent. Researchers at Intel are working on a framework that allows people to be notified about surrounding IoT devices collecting personal information, and to control these collection practices [22], but no suitable interface has been developed for this system yet.

Developing a usable privacy-setting interface for IoT to simplify users' task of managing privacy settings seems promising. However, developing such an interface would commonly require user studies with existing systems. Since the Intel control framework [22] has not been implemented yet, this method is not possible. We therefore propose to develop user interface designs for managing the privacy settings of general/public IoT devices using a *data driven design* approach: rather than evaluating and incrementally improving an existing interface, we leveraged data collected by Lee and Kobsa [72], which gathered users' feedback on general/public IoT scenarios *before* developing the interface. This approach allows us to create a navigational structure that preemptively maximizes users' efficiency in expressing their privacy preferences. Moreover, it allows us to anticipate the most common privacy settings, and capture them into a series of 'privacy profiles' that allow users to express a complex set of privacy preferences with the single click of a button.

In this chapter, we first discuss the dataset that we use, then we present how we apply our data-driven approach in the general/public IoT context, including the inspection of users' behaviors using statistical analyses and prediction of users' behaviors using machine learning techniques. Finally, we present the privacy-setting prototypes that we create based on both statistical and machine learning results.

4.2 Dataset and design

In the data collected by Lee and Kobsa [72], 200 participants were asked about their intention to allow or reject the IoT features presented in 14 randomized scenarios. These scenarios are manipulated in a mixed fractional factorial design along the following dimensions: 'Who', 'What', 'Where', 'Reason', and 'Persistence' (See Table 4.1). 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.

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)

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 [106]. However, since people differ extensively in their privacy preferences [88], 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 [65, 88, 132]. We perform machine learning analysis on this dataset to create a similar set of "smart profiles" for our

Table 4.1: Parameters used in the experiment[1]

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

[1] 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."

general IoT privacy-setting interface.

4.3 Statistical Analysis

We conducted a statistical analysis on this dataset to determine the effect of each scenario parameter on users' decisions to allow the presented general IoT scenario and how this effect is mediated by the user's attitudes. [1]

Using this approach, we find that the 'Who' parameter has the strongest effect on users' decision to allow the scenario, followed by the 'What', the 'Reason', and the 'Persistence' parameter. The 'Where' parameter has no effect at all. 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 [76].

'What' is the second 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 is the third most important scenario parameter. 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, especially with respect to the 'who' and 'what' dimensions.

[1] The statistical analysis and the subsequent layered interface were developed by my co-author Paritosh Bahirat. These endeavors are presented in summarized form since they are not an official part of this dissertation. For more details, please refer to [11].

Moreover, we found no significant interaction effects of parameters on decision beyond the significant interaction between 'Who' and 'What' onto the attitudes. The outcome informed the design of a 'layered interface', which present privacy settings with the most prominent influence first, relegating less prominent aspects to subsequently lower layers (See Figure 4.1). Users can make a decision based on a single parameter only, and choose 'yes', 'no', or 'it depends' for each parameter value. If they choose 'it depends', they move to a next layer, where the decision for that parameter value is broken down by another parameter.

The manual interface is shown in Screens 2-4 of Figure 4.1. At the top layer of this interface should be the scenario parameter that is most influential in our dataset. Our statistical results inform us that this is the **who** parameter. Screen 2 shows how users can allow/reject data collection for each of the 7 types of recipients. Users can choose "more", which brings them to the second-most important scenario parameter, i.e. the **what** parameter. Screen 3 of Figure 4.1 shows the data type options for when the user clicks on "more" for "Friends' devices". We have conveniently grouped the options by collection medium. Users can turn the collection of various data types by their friends' devices on or off. If only some types of data are allowed, the toggle at the higher level gets a yellow color and turns to a middle option, indicating that it is not completely 'on' (see "Friends' devices" in Screen 2).

Screen 4 of Figure 4.1 shows how users can drill down even further to specify **reasons** for which collection is allowed, and the allowed **persistence** (we combined these two parameters in a single screen to reduce the "depth" of our interface). Since **reason** and **persistence** explain relatively little variance in behavioral intention, we expect that only a few users will go this deep into the interface for a small number of their settings. We leave out **where** altogether, because our statistical results deemed this parameter to be non-significant.

4.4 Predicting users' behaviors (original work)

To further simplify the task of manually setting privacy preferences, we used machine learning to predict users' decisions based on the scenario parameters. Our goal is to find suitable *default settings* for an IoT privacy-setting interface. Consequently, we do not attempt to find the most accurate solution; instead we make a conscious tradeoff between parsimony and prediction accuracy. Accuracy is important to ensure that users' privacy preferences are accurately captured and/or need

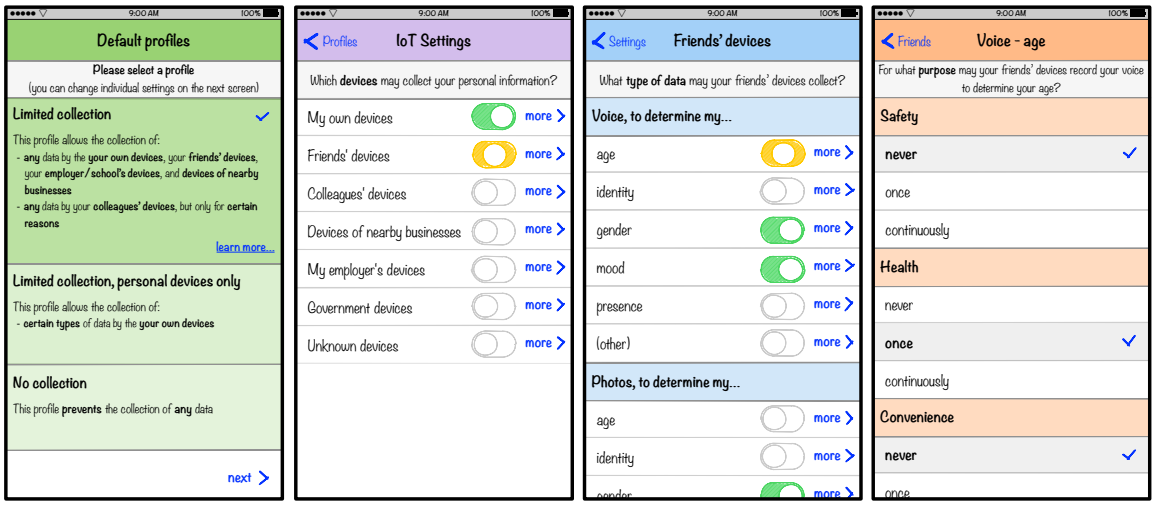


Figure 4.1: From Left, Screen 1 shows three default settings, Screen 2,3 and 4 shows layered interface

only few manual adjustments. Parsimony, on the other hand, prevents overfitting and promotes fairness: we noticed that more complex models tended to increase overall accuracy by predicting a few users' preferences more accurately, with no effect on other users. Parsimony also makes the associated default setting easier to understand for the user.

Our prediction target is the participants' decision to allow or reject the data collection described in each scenario, classifying a scenario as either 'yes' or 'no'. The scenario parameters serve as input attributes. These are nominal variables, making decision tree algorithms such as ID3 and J48 a suitable prediction approach. Unlike ID3, J48 uses gain ratio as the root node selection metric, which is not biased towards input attributes with many values. We therefore use J48 throughout our analysis.

We discuss progressively sophisticated methods for predicting participants' decisions. After discussing naive solutions, we first present a cross-validated tree learning solution that results in a single "smart default" setting that is the same for everyone. Subsequently, we discuss three different procedures that create a number of "smart profiles" by clustering the participants and creating a separate cross-validated tree for each cluster. For each procedure, we try various numbers of clusters. Accuracies of the resulting solutions are reported in Table 4.2.

Table 4.2: Comparison of clustering approaches

Approach	clusters	Accuracy	# of profiles
Naive	1	28.33%	1 (all 'yes')
classification	1	71.67%	1 (all 'no')
Overall	1	73.10%	1
Attitude-based clustering	2	75.28%	2
	3	75.17%	3
	4	75.60%	3
	5	75.25%	3
Fit-based	2	77.99%	2
clustering	3	81.54%	3
Agglomerative	200	78.13%	4
clustering	200	78.27%	5

Table 4.3: Confusion matrix for the overall prediction

Observed	Prediction		Total
	Yes	No	
Yes	124 (TP)	669 (FN)	793
No	84 (FP)	1923 (TN)	2007
Total	208	2592	2800

4.4.1 Naive Prediction Methods

We start with naive or "information-less" predictions. Our dataset contains 793 'yes'es and 2007 'no's. Therefore, predicting 'yes' for every scenario gives us a 28.33% prediction accuracy, while making a 'no' prediction gives us an accuracy of 71.67%. In other words, if we disallow all information collection by default, users will on average be happy with this default for 71.67% of the settings.

4.4.2 Overall Prediction

We next create a "smart default" by predicting the allow/reject decision with the scenario parameters using J48 with Weka's [46] default settings. The resulting tree is shown in Figure 4.2. The confusion matrix (Table 4.3) shows that this model results in overly conservative settings; only 208 'yes'es are predicted.

Figure 4.2 shows that this model predicts 'no' for every recipient ('who') except 'Own device'. For this value, the default setting depends on 'what' is being collected (see Table 4.4). For some levels of 'what', there is a further drill down based on 'where', 'persistence' and 'reason'.

We can use this tree to create a "smart default" setting; in that case, users would on average

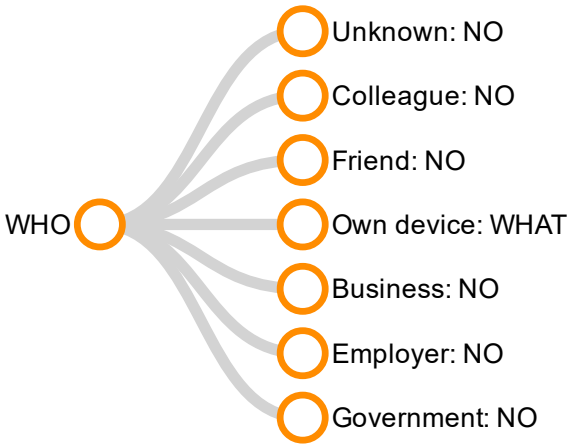


Figure 4.2: The Overall Prediction decision tree. Further drill down for 'who' = 'Own device' is provided in Table 4.4

be content with 73.10% of these settings—a 2% improvement over the naive "no to everything" default setting.

Given that people differ substantially in their privacy preferences, it is not unsurprising that this "one size fits all" default setting is not very accurate. A better solution would cluster participants by their privacy preferences, and then fit a separate tree for each cluster. These trees could then be used to create "smart profiles" that new users may choose from. Subsequent sections discuss several ways of creating such profiles.

4.4.3 Attitude-Based Clustering

Our first "smart profile" solution uses the attitudes (comfort, risk, appropriateness) participants expressed for each scenario on a 7-point scale. We averaged the values per attitude across each participant's 14 answers, and ran k-means clustering on that data with 2, 3, 4 and 5 clusters. We then added participants' cluster assignments to our original dataset, and ran the J48 decision tree learner on the dataset with the additional **cluster** attribute. Accuracies of the resulting solutions are reported in Table 4.2 under "attitude-based clustering".

All of the resulting trees had **cluster** as the root node. This indicates that this parameter is a very effective parameter for predicting users' decisions. This also allows us to split the trees at the root node, and create separate default settings for each cluster.

The 2-cluster solution (Figure 4.3) has a 75.28% accuracy — a 3.0% improvement over the

Table 4.4: Drill down of the Overall Prediction tree for 'who' = 'Own device'

What	**Decision**		
PhoneID	Yes		
PhoneID>identity	Yes		
Location	No		
Location>presence	Reason	Safety	Yes
		Commercial	Yes
		Social-related	No
		Convenience	No
		Health-related	Yes
		None	Yes
Voice	No		
Voice>gender	Where	Your place	No
		Someone else	No
		Semi-public	No
		Public	Yes
Voice> age	No		
Voice>identity	Yes		
Voice>presence	Yes		
Voice>mood	Yes		
Photo	No		
Photo>gender	No		
Photo>age	No		
Photo>identity	Yes		
Photo>presence	No		
Photo>mood	No		
Video	No		
Video>gender	No		
Video>age	No		
Video>presence	No		
Video>mood	Yes		
Video>looking at	Persistence	Once	Yes
		Continuous	No
Gaze	No		
Gaze>looking at	Reason	Safety	Yes
		Commercial	No
		Social-related	No
		Convenience	Yes
		Health-related	Yes
		None	Yes

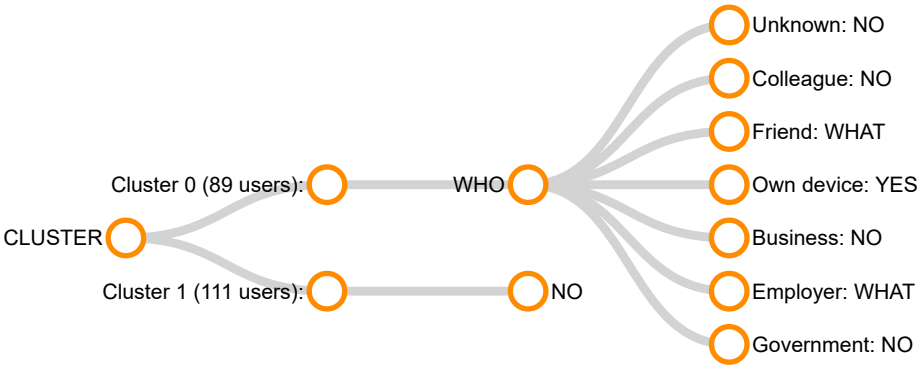


Figure 4.3: Attitude-based clustering: 2-cluster tree.

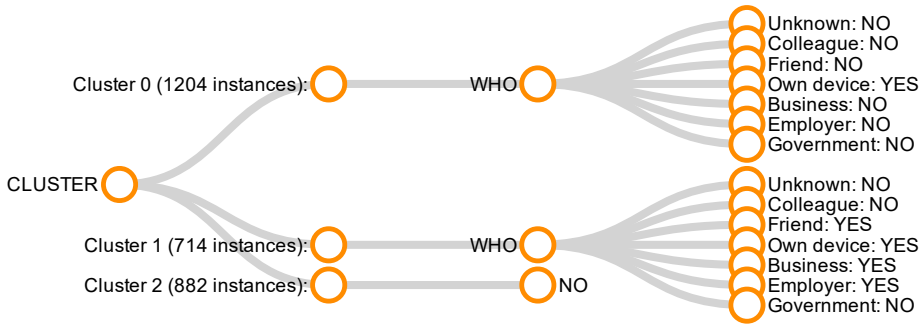


Figure 4.4: Attitude-based clustering: 3-cluster tree

"smart default". This solution results in one profile with 'no' for everything, while for the other profile the decision depends on the recipient (**who**). This profile allows any collection involving the user's 'Own device', and may allow collection by a 'Friend' or an 'Employer/School', depending on **what** is being collected.

The 3-cluster solution has a slightly lower accuracy of 75.17%, but is more parsimonious than the 2-cluster solution. There is one profile with 'no' for everything, one profile that allows collection by the user's 'Own device' only, and one profile that allows any collection except when the recipient is 'Unknown' or the 'Government'. The 4- and 5-cluster solutions have several clusters with the same sub-tree, and therefore reduce to a 3-cluster solution with 75.60% and 75.25% accuracy, respectively.

4.4.4 Fit-based clustering

Our fit-based clustering approach clusters participants without using any additional information. It instead uses the fit of the tree models to bootstrap the process of sorting participants into

clusters. Like many bootstrapping methods, ours uses *random starts* and *iterative improvements* to find the optimal solution. The process is depicted in Figure 4.5, and described in detail below. Accuracies of the resulting solutions are reported in Table 4.2 under "fit-based clustering".

Random starts: We randomly divide participants over N separate groups, and learn a tree for each group. This is repeated until a non-trivial starting solution (i.e., with distinctly different trees per cluster) is found.

Iterative improvements: Once each of the N groups has a unique decision tree, we evaluate for each participant which of the trees best represents their 14 decisions. If this is the tree of a different group, we switch the participant to this group. Once all participants are evaluated and put in the group of their best-fitting tree, the tree in each group is re-learned with the data of the new group members. This then prompts another round of evaluations, and this process continues until no further switches are performed.

Since this process is influenced by random chance, it is repeated in its entirety to find the optimal solution. Cross-validation is performed in the final step to prevent over-fitting. Accuracies of the 2- and 3-cluster solutions are reported in Table 4.2 under "fit-based clustering". We were not able to converge on a higher number of clusters.

The 2-cluster solution has a 77.99% accuracy—a 6.7% improvement over the "smart default". One profile has 'no' for everything, while the settings in the other profile depends on **who**: it allows any collection by the user's 'Own device', and may allow collection by a 'Friend's device' or an 'Employer', depending on **what** is collected.

The 3-cluster solution (Figure 4.6) has a 81.54% accuracy — an 11.5% improvement over the "smart default". We find one profile with 'no' for everything; one profile that may allow collection by the user's 'Own device', depending on **what** is being collected; and one profile that allows any collection except when the recipient (**who**) is 'Unknown', the 'Government', or a 'Colleague', with settings for the latter depending on the **reason**.

4.4.5 Agglomerative clustering

Our final method for finding "smart profiles" follows a hierarchical bottom-up (or agglomerative) approach. It first fits a separate tree for each participant, and then iteratively merges them based on similarity. 156 of the initial 200 trees predict "no for everything" and 34 of them predict "yes for everything"—these are merged first. For every possible pair of the remaining 10 trees, the

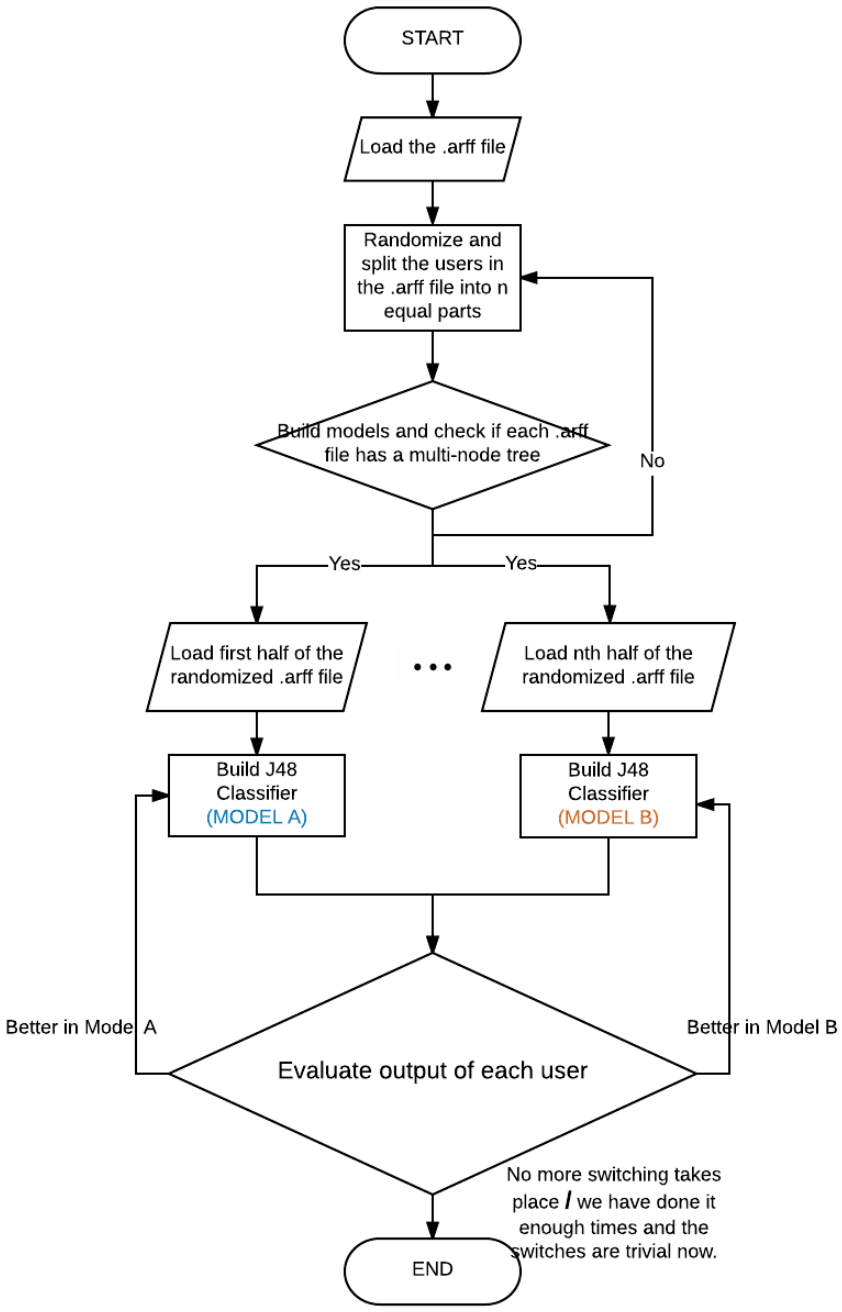


Figure 4.5: The Flow Chart for Fit-based Clustering

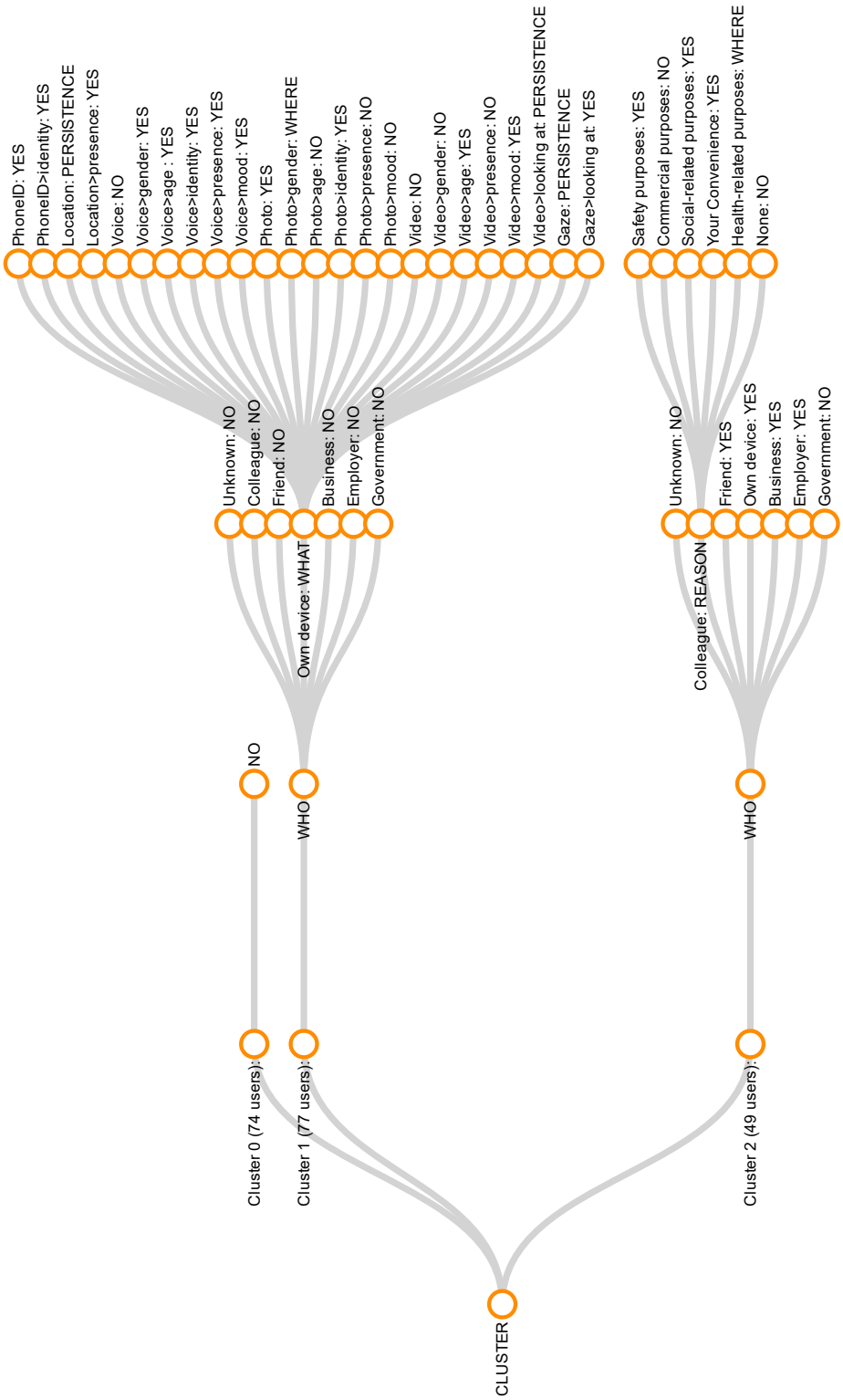


Figure 4.6: Fit-based clustering: 3-cluster tree. Further drill down is hidden for space reasons.

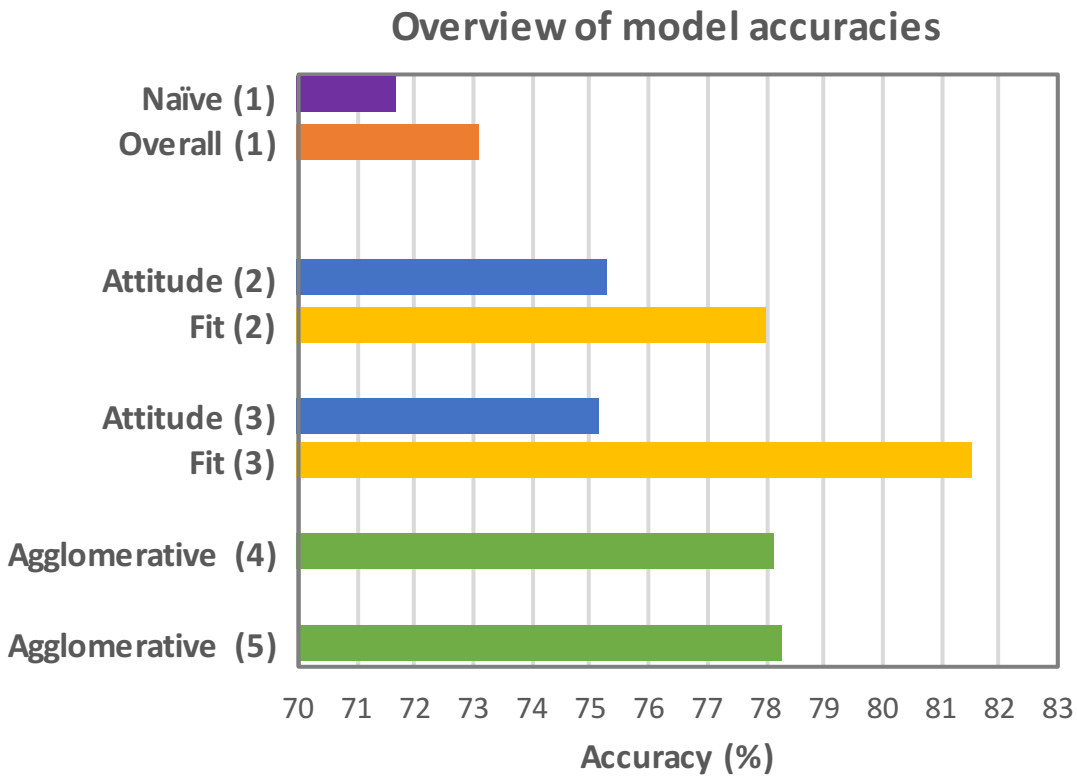


Figure 4.7: Accuracy of our clustering approaches

accuracy of the pair is compared with the mean accuracy the individual trees, and the pair with the smallest reduction in accuracy is merged. This process is repeated until we reach the predefined number of clusters.

We were able to reach a 5- and 4-cluster solution. The 3-cluster solution collapsed down into a 2-cluster solution with one profile of all 'yes'es and one profile of all 'no's (a somewhat trivial solution with a relatively bad fit). Accuracies of the 4- and 5-cluster (Table 4.2, "agglomerative clustering") are 78.13% and 78.27% respectively. For the 4-cluster solution, we find one profile with 'no' for everything, one profile with 'yes' for everything, one profile that depends on **who**, and another that depends on **what**. The latter two profiles drill down even further on specific values of **who** and **what**, respectively.

4.4.6 Discussion of Machine Learning Results

Figure 4.7 shows a comparison of the presented approaches. Compared to a naive default setting (all 'no'), a "smart default" makes a 2.0% improvement. The fit-based 2-cluster solution

results in two "smart profiles" that make another 6.7% improvement over the "smart default", while the three "smart profiles" of the fit-based 3-cluster solution make an 11.5% improvement. If we let users choose the best option among these three profiles, they will on average be content with 81.54% of the settings—a 13.8% improvement[2] over the naive "no to everything" default. This rivals the accuracy of some of the "active tracking" machine learning approaches [101].

In line with our statistical results, the factor **who** seems to be the most prominent parameter, followed by **what**. In some cases the settings are more complex, depending on a combination of **who** and **what**. This is in line with the interaction effect observed in our statistical results.

Even our most accurate solution is not without fault, and its accuracy depends most on the **who** parameter. Specifically, the solution is most accurate for the user's own device, the device of a friend, and when the recipient is unknown. It is however less accurate when the recipient is a colleague, a nearby business, an employer, or the government. In these scenarios, more misclassifications tend to happen, so it would be useful to 'guide' users to specifically have a look at these default settings, should they opt to make any manual overrides.

4.5 Privacy shortcuts (original work)

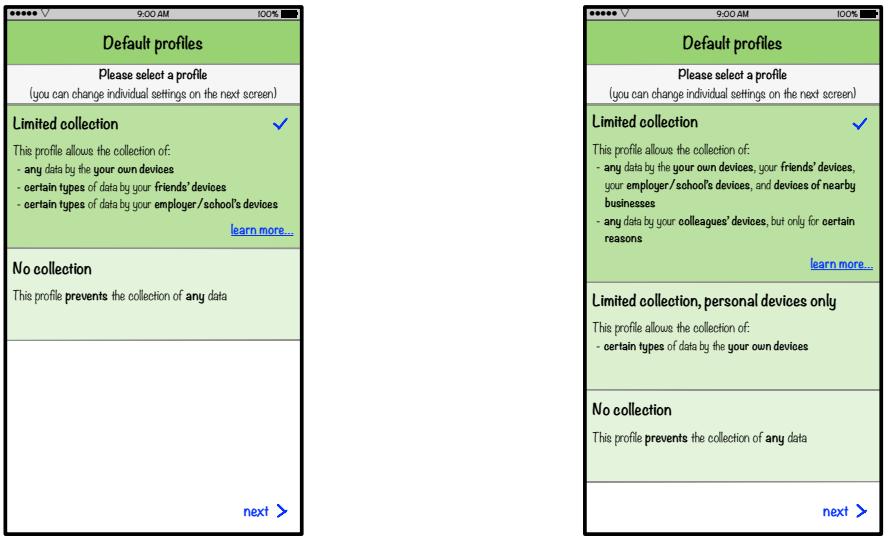
In Section 4.3, we developed a "layered" interface that general IoT users can use to manually set their privacy settings (see Figure 4.1). Our machine learning analysis (Section 4.4) resulted in a number of interesting solutions for "smart profiles" that would allow users of this interface to set their privacy settings with a single click (i.e., a choice of profile). In this section we therefore present how we integrate the "smart profiles" with our prototype.

4.5.1 Smart Default Setting

The design of "layered" interface is based on our statistical results that there exists no interaction effect between the parameters, our "smart default" settings can be easily integrated to this prototype. For the "yes to everything" or "no to everything" default, we can just simply set all the settings in the Screen 4 of Figure 4.1 to all 'on' or 'off'.

For the results from our Overall Prediction (see Figure 4.2), we can create a "smart default" setting that is 73.10% accurate on average. In this version, the IoT settings for all devices are set to

[2] 81.54.39 / 71.67 = 1.138



(a) 2-profile choice interface (b) 3-profile choice interface

Figure 4.8: Two types of profile choice interfaces

'off', except for 'My own device', which will be set to the middle option. Table 4.4 shows the default settings at deeper levels. As this default setting is on average only 73.10% accurate, we expect users to still change some of their settings. They can do this by navigating the manual settings interface.

4.5.2 Smart Profiles

To improve the accuracy of the default setting, we can instead build two "smart profiles", and allow the user to choose among them. Using the 3-cluster solution of the fit-based approach (see Figure 4.6), we can attain an accuracy of 81.54%. Screen 1 in Figure 4.1 shows a selection screen where the user can choose between these profiles. The "Limited collection" profile allows the collection of any information by the user's own devices, their friends' devices, their employer/school's devices, and devices of nearby businesses. Devices of colleagues are only allowed to collect information for certain reasons. The "Limited collection, personal devices only" profile only allows the collection of certain types of information by the user's own devices. The "No collection" profile does not allow any data collection to take place by default.

Once the user chooses a profile, they will move to the manual settings interface (Screens 2–4 of Figure 4.1), where they can further change some of their settings.

4.6 Discussion and Limitations

Our statistical and machine learning results both indicated that recipient of the information (**who**) is the most significant parameter in users' decision to allow or reject IoT-based information collection. This parameter therefore features at the forefront in our layered settings interface, and plays an important role in our smart profiles. The **what** parameter was the second-most important decision parameter, and interacted significantly with the **who** parameter. This parameter therefore features at the second level of our settings interface, and further qualifies some of the settings in our smart profiles.

Our layered interface allows a further drill-down to the **reason** and **persistence** parameters, but given the relatively lesser importance of these parameters, we expect few users to engage with the interface at this level. Moreover, the **where** parameter was not significant, so we left it out of the interface.

While a naive ('no' to all) default setting in our interface would have provided an accuracy of 71.67%, it would not have allowed users to reap the potential benefits associated with IoT data collection without changing the default setting. Our Overall Prediction procedure resulted in a smart default setting that was a bit more permissive, and increased the accuracy by 2%.

The fit-based clustering approach, which iteratively clusters users and fits an optimal tree in each cluster, provided the best solution. This resulted in an interface where users can choose from 3 profiles, which increases the accuracy by another 11.5%.

The scenario-based method presented in this paper is particularly suited for novel domains where few real interaction exist. We note, though, that this novelty may hamper our approach: users' decisions are inherently limited by the knowledge they have about IoT. Lee and Kobsa [72] made sure to educate users about the presented scenarios, hence their data is arguably better in this regard than data from "live" systems. However, as the adaptation of IoT becomes more widespread, the mindset and knowledge regarding such technologies—and thus their privacy preferences—might change. Our "smart profiles" may thus eventually have to be updated in future work, but for now, our current profiles can at least help users make make better privacy decisions in their initial stages of usage.

One limitation of our work is that we did not test our layered interface, so we do not know whether users are comfortable with the interface or whether they prefer a single "smart default"

setting or a choice among "smart profiles" (i.e. at what level of complexity in terms of profiles the user would prefer.). This is why I conduct a user study in Chapter 7 to investigate this problem. Another caveat of our work is that we did not manipulate the pruning parameter of our machine learning models in the privacy decision prediction. Note that, the decision tree shown in Figure 4.6 is rather complicated, leading to a complicated privacy profile implied by the decision tree. It will be difficult to explain a privacy profile in natural language to the users when the profile is getting too complicated. We note, though, that pruning the decision tree may reduce the accuracy of our models' results. I explore this interesting trade-off between the accuracy and parsimony (i.e. simpler profile) in Chapter 5 where I apply our data-driven approach in the Household IoT context.

4.7 Summary

In this chapter, we have presented the following:

- The definition of general/public IoT, and how we came up with the data-driven approach.
- The dataset we used and the process of the data-driven design.
- Using statistical analysis, uncovered the relative importance of the parameters that influence users' privacy decisions. Developed a "layered interface" in which these parameters are presented in decreasing order of importance.
- Using a tree-learning algorithm, created a decision tree that best predicts participants' choices based on the parameters. Used this tree to create a "smart default" setting.
- Using a combination of clustering and tree-learning algorithms, created a set of decision trees that best predict participants' choices. Used the trees to create "smart profiles".
- Developed a prototype for an IoT privacy-setting interface that integrates the layered interface with the smart default or the smart profiles.

In the next chapter, we discuss the challenges and solutions when we apply our approach in the household IoT context.

Chapter 5

Recommending Privacy Settings for Household IoT

5.1 Introduction

In Chapter 4, we have discussed how we apply the data-driven approach to the general/public IoT context and developed an IoT privacy-setting interface prototype that integrated a layered interface with smart defaults/profiles by predicting users' privacy decisions. In this chapter, we present the work we did in the area of designing for privacy for Household IoT. We expand and improve upon the previously-developed data-driven approach to design privacy-setting interfaces for users of household IoT devices. Moving the context to a more narrow environment shifts the focus of the privacy decision from the entity collecting information (which was the dominant parameter in our previous work) to a more contextual evaluation of the content or nature of the information [87]. In addition, as discussed in 4.6, an important limitation that we did not solve in our previous work is balancing the trade-off between parsimony and accuracy. Accuracy is important to ensure that users' privacy preferences are accurately captured and/or need only few manual adjustments. Parsimony, on the other hand, prevents overfitting and promotes fairness: we noticed that more complex models tended to increase overall accuracy by predicting a few users' preferences more accurately, with no effect on other users. Parsimony also makes the associated default setting easier to understand for the user. In this chapter, we try to address these concerns.

5.2 Experiment Setup

In Chapter 4, we leveraged data collected by Lee and Kobsa [72], 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'. These all are appropriate dimensions for general/public IoT context, however, a new user study is needed for collecting data in the domain of household IoT. Given that we are narrowing our focus of IoT context in the chapter from general/public IoT to household IoT, it is necessary to investigate whether these dimensions are still suitable for our next-step experiment. At the same time, some new parameters may need to be added into our consideration for better expressing the features of the new, narrowed IoT context.

In this section, we first discuss the changes in IoT context dimensions for our new user study. We then present the factorial procedure by which we developed 4608 highly specific IoT scenarios, as well as the questions we asked participants to evaluate these scenarios. Finally, we describe the participant selection and experimental procedures used to collect over 13500 responses from 1133 participants.

5.2.1 Dimension Design

We consider following dimension design changes in our user study:

- When applying our data-driven approach on Lee and Kobsa's dataset in previous chapter, we found the dimension "where" does not have a significant effect on uses' disclosure decisions. Considering that we are moving to household IoT context, the usage environments will always be in users' homes. Moreover, the structure of users' houses are different from case to case, it would be too complicated if we define "where" to a more finer-granulated level, such as bedroom, kitchen, etc. Hence there there is no need to retain the parameter "where".

- "Persistence" of tracking is more relevant in public IoT, while persistent tracking is less common in household IoT. Hence, we removed "Persistence" from our current experiment.

- From the qualitative feedback in our previous study, we have learned that the secondary use of information was a prominent concern among users. Hence, we split the original dimension "purpose" into two dimensions – "purpose" and "Action", where the latter one will be used

to indicate the secondary use of information.

- A new dimension "Storage" was added in addition to our existing dimensions because it is possible for household IoT systems to operate (and thus store data) locally, and because the sharing of data with third parties is not as common in household IoT as in public IoT.

By applying the above dimension changes, we aim to conduct a new user study focusing on household IoT in particular, and further refine our approach to allow us to create more carefully tailored user interfaces for the household IoT context. Next, we present the factorial procedure by which we developed highly specific household IoT scenarios.

5.2.2 Contextual Scenarios

The scenarios evaluated in our study are based on a full factorial combination of five different Parameters: Who, What, Purpose, Storage and Action. A total of $8(who) * 12(what) * 4(purpose) * 4(storage) * 3(action) = 4608$ scenarios were tested this way.

The scenarios asked participants to imagine that they were owners and active users of the presented IoT devices, trying to decide whether to turn on or off certain functionalities and/or data sharing practices. To avoid endowment effects, the scenarios themselves made no indication as to whether the functionality was currently turned on or off (such endowment effects were instead introduced by manipulating the framing of the Decision question; see section 5.2.3). An example scenario is: *"Your smart TV (Who) uses a camera (What) to give you timely alerts (Purpose). The data is stored locally (Storage) and used to optimize the service (Action)."* This scenario may for example represent a situation where the smarthome system has detected (via camera) a delivery of a package and then alerts the user (via the smart TV) about its arrival. In this particular scenario we note that the video data is stored locally to optimize service; this could mean that the smarthome system uses the video stream to (locally) train a package detection algorithm. Similarly, another example scenario is: *"Your Smart Assistant uses a microphone to detect your location in house. The data is stored on a remote server and shared with third parties to recommend you other services."* Similarly, this scenario could represent a situation where the smarthome has detected (via microphone) it's user's location in the house and this information is shared to the smart assistant. In the scenario, the data is stored on remote server and shared with third parties so that it can recommend additional services (like weather or local transportation) via third parties to the user.

The levels of all five parameters used in our experiment are shown in Table 5.1. The parameters were highlighted in the scenario for easy identification, and upon hovering the mouse cursor over them each parameter would show a succinct description of the parameter. Figure 5.1 shows a screenshot of a scenario as shown to participants in the study. A thirteenth scenario regarding the interrelated control of various IoT devices (e.g. *"You can use your smart TV to control your smart refrigerator"*) was also asked, but our current analysis focuses on the information-sharing scenarios only.

5.2.3 Scenario Evaluation Questions

The first question participants were asked about each scenario was whether they would enable or disable the particular feature mentioned in scenario (Decision). Subsequently, they were asked about their attitudes regarding the scenario in terms of their perceived Risk, Appropriateness, Comfort, Expectedness and Usefulness regarding the presented scenario (e.g., *"How appropriate do you think this scenario is?"*). These questions were answered on a 7-point scale (e.g., *"very inappropriate"* to *"very appropriate"*). In every 4th scenario, the Risk and Usefulness questions were followed by an open question asking the participants to describe the potential Risk and Usefulness of the scenario. We asked these question mainly to encourage participants to carefully evaluate the scenarios. Figure 5.1 shows the questions asked about each scenario.

The framing and default of the Decision question were manipulated between-subjects at three levels each: positive framing ("Would you enable this feature?", options: Yes/No), negative framing ("Would you disable this feature?", options: Yes/No) or neutral framing ("What would you do with this feature?", options: Enable/Disable); combined with a positive default (enabled by default), negative default (disabled by default), or no default (forced choice).

5.2.4 Participants and Procedures

To collect our dataset, 1133 adult U.S.-based participants (53.53% Female, 45.75% Male, 8 participants did not disclose) were recruited through Amazon Mechanical Turk. This significant increase in participants over the Lee and Kobsa [72] dataset is commensurate with our expectation of more complex privacy decision behaviors in household IoT compared to public IoT. Participation was restricted to Mechanical Turk workers with a high reputation (at least 50 completed tasks

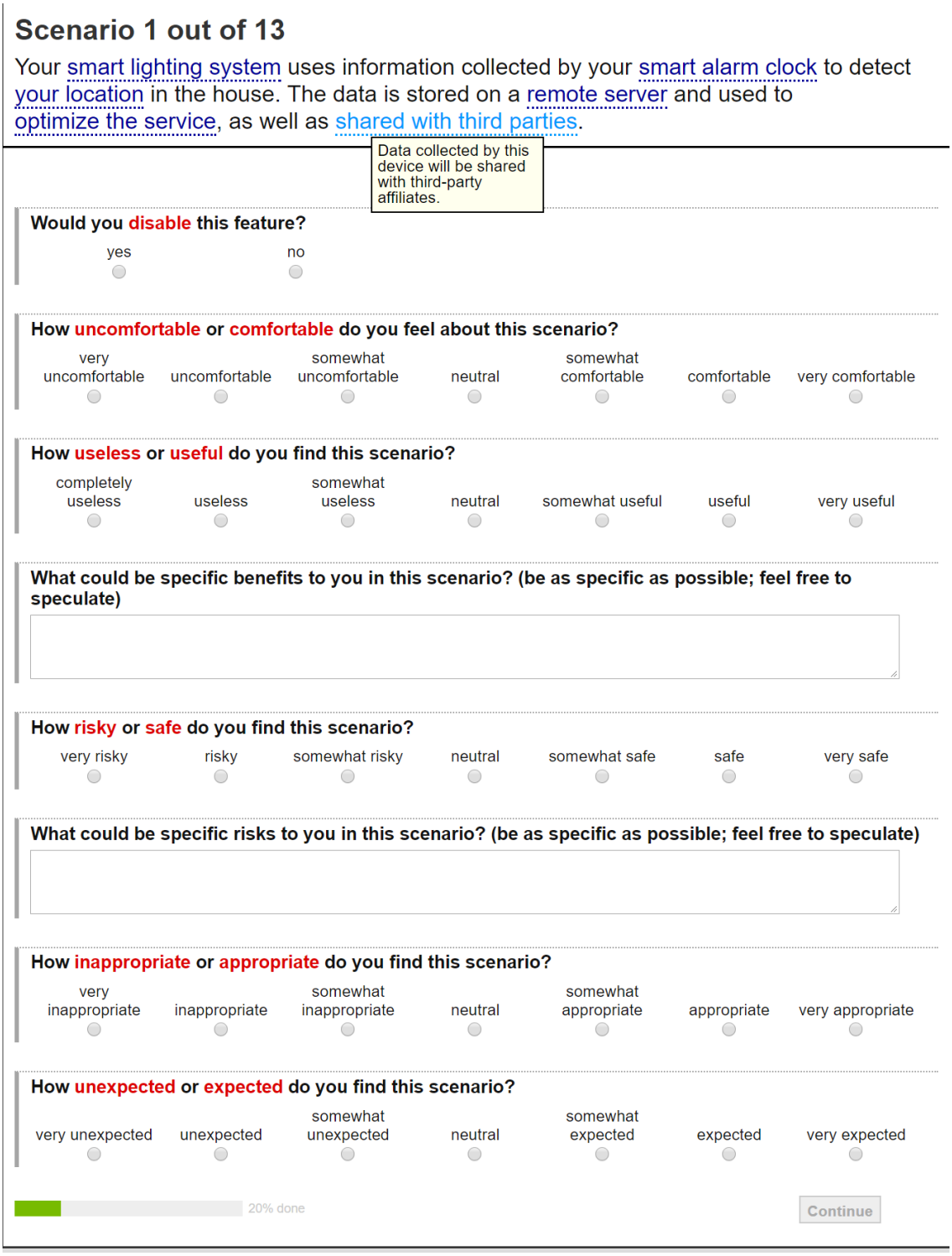


Figure 5.1: Example of one of the thirteen scenarios presented to the participants.

Table 5.1: Parameters used to construct the information-sharing scenarios.

Parameter	**Levels**	**Code**[1]
Who:	1. Home Security System	SS
Your Smart...	2. Refrigerator	RE
	3. HVAC System	HV
	4. Washing Machine	WM
	5. Lighting System	SL
	6. Assistant	SA
	7. TV	TV
	8. Alarm Clock	SC
What:	1. Home Security System	CSE
...uses information	2. Refrigerator	CRE
collected by your...	3. HVAC System	CHV
	4. Washing Machine	CWA
	5. Lighting System	CLI
	6. Assistant	CAS
	7. TV	CTV
	8. Alarm	CAL
	9. uses a location sensor	CLO
	10. uses a camera	CCA
	11. uses a microphone	CMP
	12. connects to your smart phone/watch	CSW
Purpose :	1. detect whether you are home	PH
...to...	2. detect your location in house	LH
	3. automate its operations	AO
	4. give you timely alerts	TA
Storage:	1. locally	L
The data is stored...	2. on remote server	R
	3. on a remote server and shared with third parties	T
Action:	1. optimize the service	O
...and used to...	2. give insight into your behavior	I
	3. recommend you other services	R
	4. [None]	N

[1] The "codes" are used as abbreviations in graphs and figures throughout this chapter.

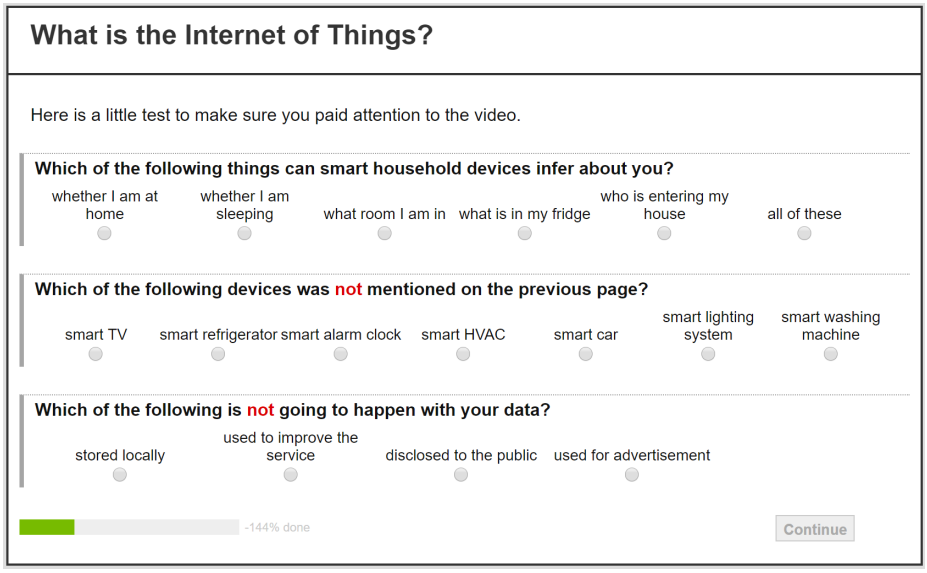


Figure 5.2: Attention check questions asked to participants

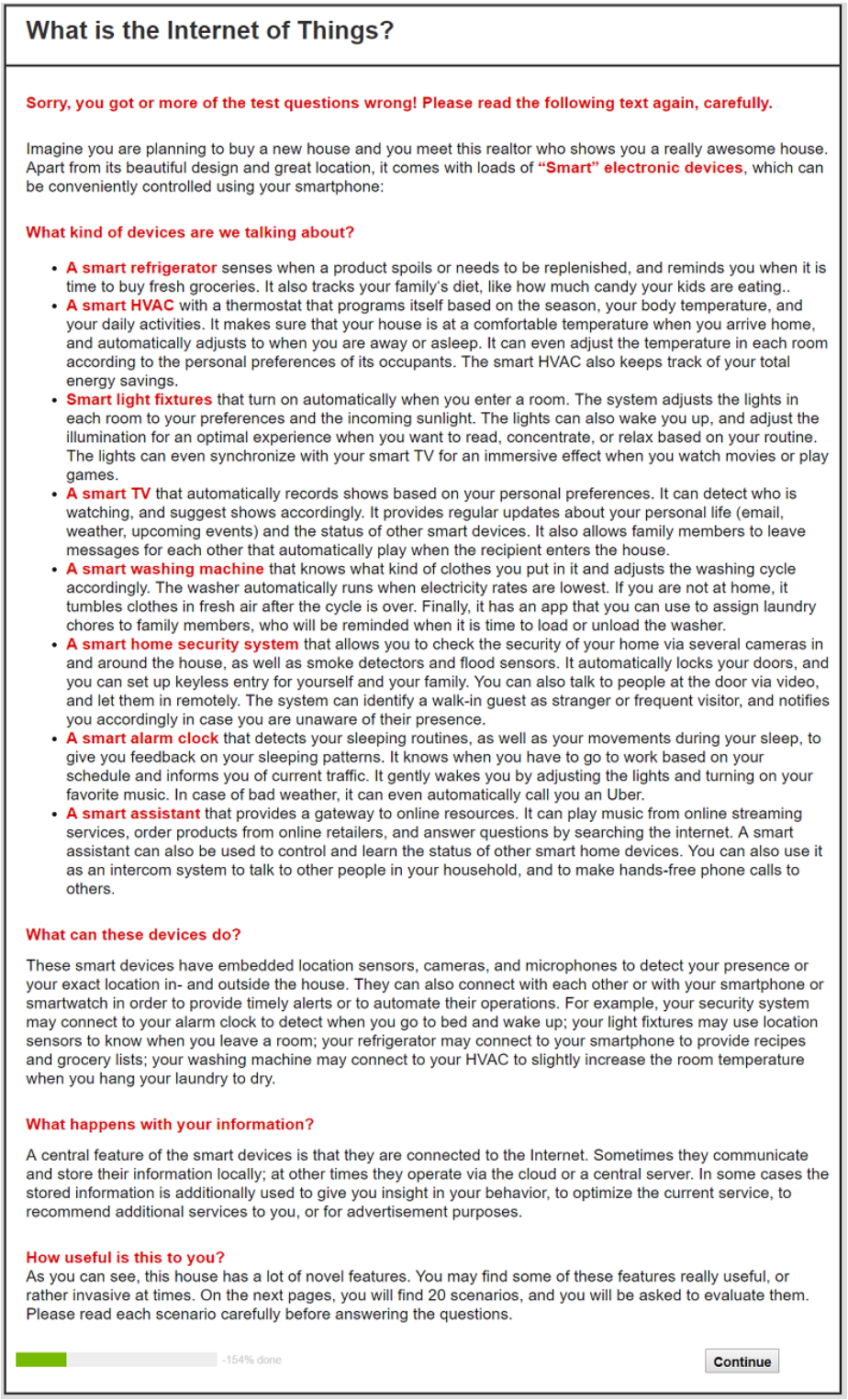
completed with an average accuracy greater than 95%). Participants were paid $2.00 upon successful completion of the study. The participants were warned about not getting paid in case they failed attention checks.

The study participants represented a wide range of ages, with 9 participants less than 20 years old, 130 aged 20-25, 273 aged 25-30, 418 aged 30-40, 175 aged 40-50, 80 aged 50-60, and 43 participants over 60 years old (5 participants did not disclose their age).

Each participant was first shown a video with a brief introduction to various smart home devices, which also mentioned various ways in which the different appliances would cooperate and communicate within a home. After the video, participants were asked to answer three attention check questions, shown in Figure 5.2. If they got any of these questions wrong, they would be asked to read the transcript of the video and re-answer the questions. The transcript is shown in Figure 5.3

After the introduction video, each participant was presented with 12 information-sharing scenarios (and a 13th control scenario, not considered in this paper). These scenarios were selected from the available 4608 scenarios using fractional factorial design[1] that balances the within- and between-subjects assignment of each parameter's main effect, and creates a uniform exposure for each participant to the various parameters (i.e., to avoid "runs" of near-similar scenarios). Participants were asked to carefully read the scenario and then answer all questions about it. Two of the

[1]The scenario assignment scheme is available at `https://www.usabart.nl/scenarios.csv`



What is the Internet of Things?

Sorry, you got or more of the test questions wrong! Please read the following text again, carefully.

Imagine you are planning to buy a new house and you meet this realtor who shows you a really awesome house. Apart from its beautiful design and great location, it comes with loads of **"Smart" electronic devices**, which can be conveniently controlled using your smartphone:

What kind of devices are we talking about?

- **A smart refrigerator** senses when a product spoils or needs to be replenished, and reminds you when it is time to buy fresh groceries. It also tracks your family's diet, like how much candy your kids are eating..
- **A smart HVAC** with a thermostat that programs itself based on the season, your body temperature, and your daily activities. It makes sure that your house is at a comfortable temperature when you arrive home, and automatically adjusts to when you are away or asleep. It can even adjust the temperature in each room according to the personal preferences of its occupants. The smart HVAC also keeps track of your total energy savings.
- **Smart light fixtures** that turn on automatically when you enter a room. The system adjusts the lights in each room to your preferences and the incoming sunlight. The lights can also wake you up, and adjust the illumination for an optimal experience when you want to read, concentrate, or relax based on your routine. The lights can even synchronize with your smart TV for an immersive effect when you watch movies or play games.
- **A smart TV** that automatically records shows based on your personal preferences. It can detect who is watching, and suggest shows accordingly. It provides regular updates about your personal life (email, weather, upcoming events) and the status of other smart devices. It also allows family members to leave messages for each other that automatically play when the recipient enters the house.
- **A smart washing machine** that knows what kind of clothes you put in it and adjusts the washing cycle accordingly. The washer automatically runs when electricity rates are lowest. If you are not at home, it tumbles clothes in fresh air after the cycle is over. Finally, it has an app that you can use to assign laundry chores to family members, who will be reminded when it is time to load or unload the washer.
- **A smart home security system** that allows you to check the security of your home via several cameras in and around the house, as well as smoke detectors and flood sensors. It automatically locks your doors, and you can set up keyless entry for yourself and your family. You can also talk to people at the door via video, and let them in remotely. The system can identify a walk-in guest as stranger or frequent visitor, and notifies you accordingly in case you are unaware of their presence.
- **A smart alarm clock** that detects your sleeping routines, as well as your movements during your sleep, to give you feedback on your sleeping patterns. It knows when you have to go to work based on your schedule and informs you of current traffic. It gently wakes you by adjusting the lights and turning on your favorite music. In case of bad weather, it can even automatically call you an Uber.
- **A smart assistant** that provides a gateway to online resources. It can play music from online streaming services, order products from online retailers, and answer questions by searching the internet. A smart assistant can also be used to control and learn the status of other smart home devices. You can also use it as an intercom system to talk to other people in your household, and to make hands-free phone calls to others.

What can these devices do?

These smart devices have embedded location sensors, cameras, and microphones to detect your presence or your exact location in- and outside the house. They can also connect with each other or with your smartphone or smartwatch in order to provide timely alerts or to automate their operations. For example, your security system may connect to your alarm clock to detect when you go to bed and wake up; your light fixtures may use location sensors to know when you leave a room; your refrigerator may connect to your smartphone to provide recipes and grocery lists; your washing machine may connect to your HVAC to slightly increase the room temperature when you hang your laundry to dry.

What happens with your information?

A central feature of the smart devices is that they are connected to the Internet. Sometimes they communicate and store their information locally; at other times they operate via the cloud or a central server. In some cases the stored information is additionally used to give you insight in your behavior, to optimize the current service, to recommend additional services to you, or for advertisement purposes.

How useful is this to you?

As you can see, this house has a lot of novel features. You may find some of these features really useful, or rather invasive at times. On the next pages, you will find 20 scenarios, and you will be asked to evaluate them. Please read each scenario carefully before answering the questions.

-154% done

Continue

Figure 5.3: Transcript of video shown to participants if they failed attention checks.

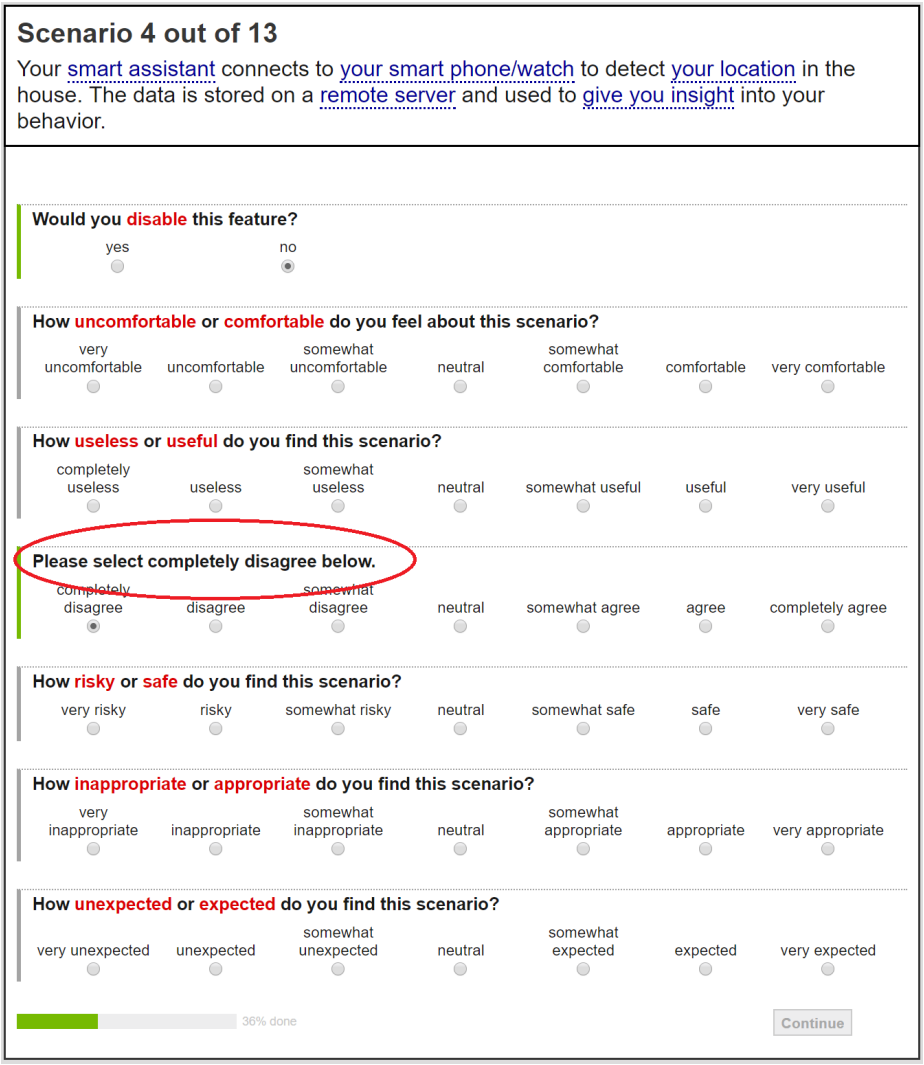


Figure 5.4: Attention check question shown while participants are answering questions per scenario.

13 scenarios had an additional attention check question (e.g., "Please answer this question with Completely Agree", see Figure 5.4), and there was an additional attention check question asking participants about the remaining time to finish the study (which was displayed right there on the same page, see 5.5). Participants rushing through the experiment and/or repeatedly failing the attention check questions were removed from the dataset.

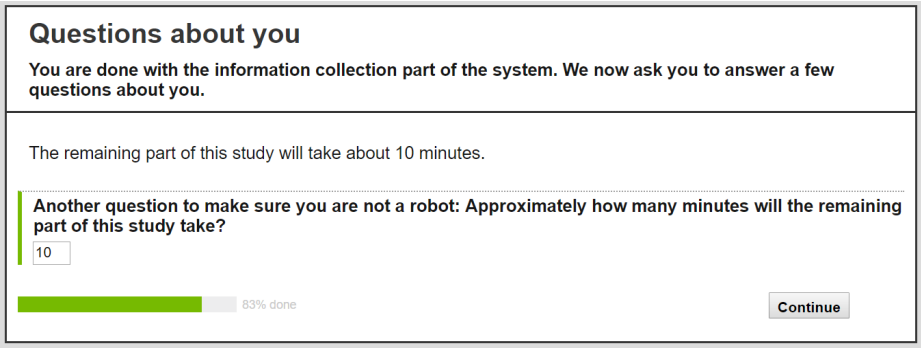


Figure 5.5: Attention check question asked to participants.

5.3 Statistical Analysis

Our statistical analysis [2] shows that unlike results from [11], all parameters had a significant effect. Particularly, where the information is stored and if/how it is shared with third parties ('Storage' parameter) has the strongest impact on users' decision, followed by 'What', 'Who' and 'Purpose' (all similar) and finally 'Action'. Moreover, substantial two-way interaction effects were observed between 'Who', 'What', and 'Purpose', which suggest that when users decide on one parameter, they inherently take another parameter into account. Based on these results, we designed an interface, for users to manually change their privacy settings, which separated 'Device/Sensor Management' and 'Data Storage & Usage'.

We also analyze the effects of defaults and framing [10]. As outlined in section 5.2.3, the framing and default of the Decision question in our study were manipulated between-subjects at three levels each: positive, negative, or neutral framing; combined with a positive, negative, or no default. The analysis shows that defaults and framing have direct effects on disclosure: Participants in the negative default condition are less likely to enable the functionality, while participants in the positive default condition are more likely to enable the scenario (a traditional default effect). Likewise, participants in the negative framing condition are more likely to enable the functionality (a loss aversion effect).

Moreover, there are interaction effects between defaults/framing and attitudes on disclosure: the effects of attitudes are generally weaker in the positive and negative default conditions than in the no default condition, and they are also weaker in the negative framing condition.

[2]The statistical analysis were conducted by my co-author Paritosh Bahirat. These endeavors are presented in summarized form since they are not an official part of this dissertation. For more details, please refer to [48].

Importantly, there are no interaction effects between defaults/framing and parameters on attitude or disclosure. Hence, the main findings in this section regarding the structure and relative importance of the effects of parameters remain the same, regardless of the effects of defaults and framing.

5.4 Privacy-Setting Prototype Design

Our dataset presents a simplified version of possible scenarios one might encounter in routine usage of smart home technology. Still it is a daunting task to design an interface, even for these simplified scenarios: We want to enable users to navigate their information collection and sharing preferences across 12 different sources (*What*), 7 different devices trying to access this information (*Who*) for 4 different *Purposes*. Additionally, this information is being stored/shared in 3 ways (*Storage*) and being used for 4 different secondary uses (*Actions*).

Based on our statistical analysis in 5.3, we developed an intuitive interface that gives users manual control over their privacy settings. We split our settings interface into two separate sections: 'Device/Sensor Management' and 'Data Storage & Use'. The landing page of our design (screen 1 in Figure 5.6) gives users access to these two sections. The former section is based on *Who*, *What* and *Purpose* and allows users to "Manage device access to data collected in your home" (screen 2-3). The latter section is based on *Storage* and *Action*, and allows users to "Manage the storage and long-term use of data collected in your home" (screen 4). Both sections are explained in more detail below.

Device/Sensor Management: This screen (Figure 5.6, screen 2) allows users to control the *Purposes* for which each device (*Who*) is allowed to access data collected by itself, other devices, and the smart home sensors installed around the house (*What*). This screen has a collapsible list of data-collecting devices and sensors (*What*). For each device/sensor, the user can choose what devices can access the collected data (*Who*; in rows), and what it may use that data for (*Purpose*; in columns).

In the example of Figure 5.6, the user does not give the 'Refrigerator' access to information collected by the 'Smart Assistant' for any of the four purposes, while they give the 'Smart TV' access to this data for the purpose of giving 'timely alerts'. In this example the 'Smart Assistant' is allowed to use its own data to 'automate operations' and to 'know your location in your home'.

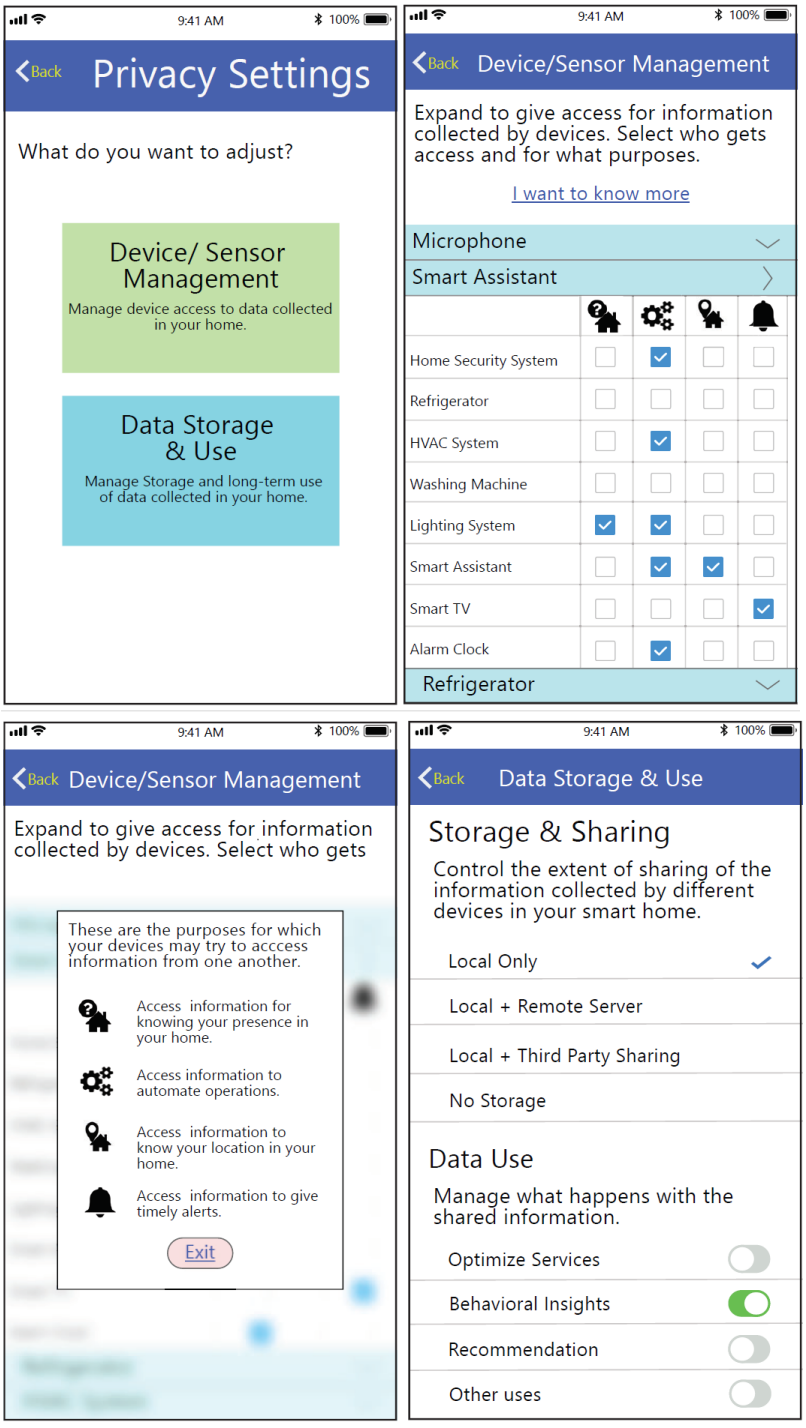


Figure 5.6: Privacy-Setting Interfaces Prototype

Showing *Who*, *What* and *Purpose* at the same time allows users to enable/disable specific combinations of settings—the significant interaction effects between these parameters suggest that this is a necessity. The icons for the *Purpose* requirement allow this settings grid to fit on a smartphone or in-home control panel. We expect that users will quickly learn the meaning of these icons, but they can always click on 'I want to know more' to learn their meaning (see Figure 5.6, screen 3).

Data Storage & Use: This screen (Figure 5.6, screen 4) allows users to control how their data is stored and shared (*Storage*), as well as how stored data is used (*Action*). These settings are independent from each other and from the Device/Sensor Management settings.

For 'Storage & Sharing', users can choose to turn storage off altogether, store data locally, store data both locally and on a remote server, or store data locally and on a remote server *and* allow the app to share the data with third parties. Note that the options for *Storage* are presented as ordered, mutually exclusive settings. Our scenarios did not present them as such (i.e., participants were free to reject local storage but allow remote storage). However, the *Storage* parameter showed a very clear separation of levels, so this presentation is justified. For 'Data Use', the users can choose to enable/disable the use of the collected data for various secondary purposes: behavioral insights, recommendations, service optimization, and/or other purposes.

In the subsequent sections we describe the results from our machine learning analysis and further explain how these results impact the designs presented in this section. For this purpose, Section 5.6 revisits the interface designs presented here.

5.5 Predicting users' behaviors (original work)

In this section we predict participants' *enable/disable* decision using machine learning methods. We do not attempt to find the best possible solution; instead we make a conscious trade-off between parsimony and prediction accuracy.

Our prediction target is the participants' decision to *enable* or *disable* the data collection described in each scenario. The scenario parameters serve as input attributes. Using Java and Weka's Java library [133] for modeling and evaluation, we implement progressively sophisticated methods for predicting participants' decisions. After discussing naive (enable/disable all) solutions and One Rule Prediction, we first present a cross-validated tree learning solution that results in a

Table 5.2: Comparison of clustering approaches (highest parsimony and highest accuracy)

Approach	Inital clusters	Final # of profiles	Complexity (avg. tree size/profile)	Accuracy
Naive (enable all)	1	1	1	46.74%
Naive (disable all)	1	1	1	53.26%
One Rule (Fig. 5.7)	1	1	3	61.39%
Overall	1	1	8	63.32%
(Fig. 5.10)	1	1	264	63.76%
Attitude-based clustering (Fig. 5.13)	2	2	2	69.44%
	2	2	121.5	72.66%
	3	3	2.67	72.19%
	3	3	26.67	73.47%
	5	4	3	72.61%
	5	4	26	73.56%
Agglomerative clustering (Fig. 5.16)	1133	4	2	79.4%
	1133	5	2.4	80.35%
	1133	6	3.17	80.60%
Fit-based clustering (Fig. 5.20)	2	2	2	74.43%
	2	2	151.5	76.72%
	3	3	7	79.80%
	3	3	65.33	80.81%
	4	4	9.25	81.88%
	4	4	58.25	82.41%
	5	5	4.2	82.92%
	5	5	51.4	83.35%

single "smart default" setting that is the same for everyone. Subsequently, we discuss three different procedures that create a number of "smart profiles" by clustering the participants and creating a separate cross-validated tree for each cluster. For each procedure, we try various numbers of clusters and pruning parameters. The solutions with the most parsimonious trees and the highest accuracies of each approach are reported in Table 5.2; more detailed results of the parsimony/accuracy trade-off are presented in Figures 5.10, 5.13, 5.16 and 5.20 throughout the paper, and combined in Figure 5.24.

5.5.1 Naive Prediction Model

We start with the naive or "information-less" predictions. Compared to our previous work in Chapter 4, our current dataset shows that it is even less amenable to a 'simple' default setting: it contains 6335 *enable* cases and 7241 *disable* cases, which means that predicting *enable* for every setting gives us a 46.74% prediction accuracy, while making a *disable* prediction for every setting gives us an accuracy of 53.26%. In other words, if we disable all information collection by default, only 53.26% users will on average be satisfied with this default settings. Moreover, such a default

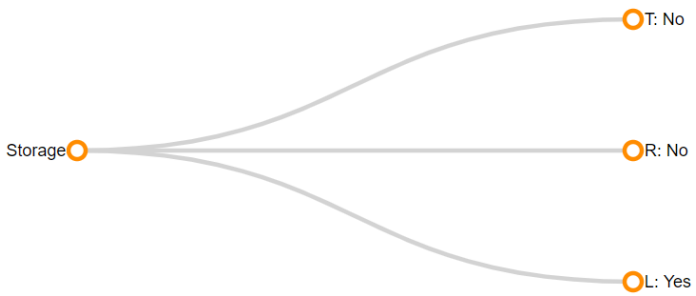


Figure 5.7: A "smart default" setting based on the "One Rule" algorithm.

Table 5.3: Confusion matrix for the One Rule prediction

Observed	Prediction		Total
	Enable	Disable	
Enable	5085 (TP)	1270 (FN)	6355
Disable	3262 (FP)	3979 (TN)	7241
Total	7192	6404	13596

setting disallows any 'smart home' functionality by default—arguably not a solution the producers of smart appliances can get behind.

5.5.2 One Rule Prediction

Next, we use a "*One Rule*" (OneR) algorithm to predict users' decision using the simplest prediction model possible. OneR is a very simple but often surprisingly effective learning algorithm [51]. It creates a frequency table for each predictor against the target, and then find the best predictor with the smallest total error based on the frequencies.

As shown in Figure 5.7 (parameter value abbreviations correspond to the "code" column in Table 5.1), the OneR model predicts users' decision solely based on the **Storage** parameter with an accuracy of 61.39%. Based on this model, if we enable all information-sharing *except* with third parties, we will on average satisfy 61.39% of users' preferences—a 15.3% improvement[3] over the naive "disable all" default. Note, though, that this default setting is overly permissive, with 3262 false positive predictions (see Table 5.3).

[3] 61.39 / 53.26 = 1.153

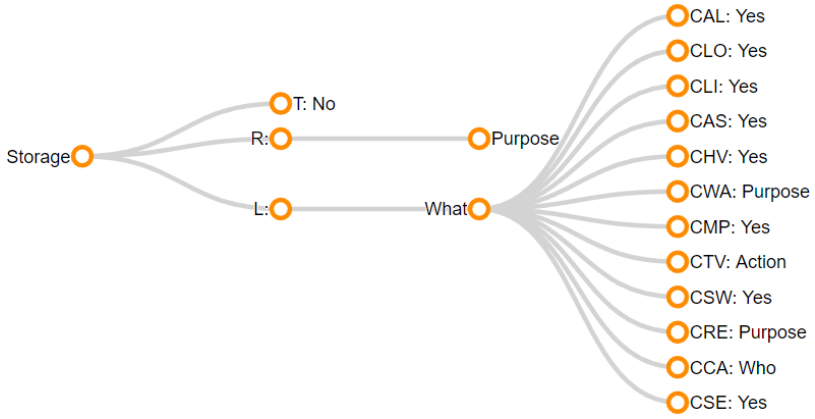


Figure 5.8: A "smart default" setting with 264 nodes with 63.76% accuracy.

5.5.3 Overall Prediction

Moving beyond a single parameter, we create a "smart default" setting by predicting the *enable/disable* decision with all scenario parameters using the J48 decision tree algorithm. The resulting tree has an accuracy of 63.76%. As shown in Figure 5.8, this model predicts users' decision on **Storage** first. It predicts *disable* for every scenarios with collected data stored on a remote server and shared with third party. For scenarios that store collected data on remote server without sharing, the default settings will depend on the 'purpose' of information sharing. There is a further drill down based on 'who' and 'what'. For scenarios that store collected data locally, the default settings will depend on the 'what'. There is a further drill down based on 'who', 'what', and 'action'. With this default setting, users would on average be satisfied with 63.76% of these settings—a 19.7% improvement over the naive "disable all" default.

On the downside, this "smart default" setting is quite complex—the "smart default" in our previous work [11] contained only 49 nodes, whereas the "smart default" for our current dataset has 264 nodes. Compared to *One Rule* algorithm, which only has 4 nodes in its decision tree and is thus much easier to explain, the accuracy improvement of Smart Default is only 3.8%. This highlights the trade-off between parsimony and prediction accuracy that we have to make when developing "smart default" settings. On the upside, though, the prediction of the J48 decision tree algorithm is more balanced, with a roughly equal number of false positives and false negatives (see Table 5.4).

To better understand the parsimony/accuracy trade-off, we vary the degree of model pruning to investigate the effect of increasing the parsimony (i.e., more trimming) on the accuracy of the resulting "smart default" setting. The parameter used to alter the amount of post-pruning performed

Table 5.4: Confusion matrix for the overall prediction

Observed	Prediction		Total
	Enable	Disable	
Enable	4753 (TP)	2488 (FN)	7241
Disable	2439 (FP)	3916 (TN)	6355
Total	7192	6404	13596

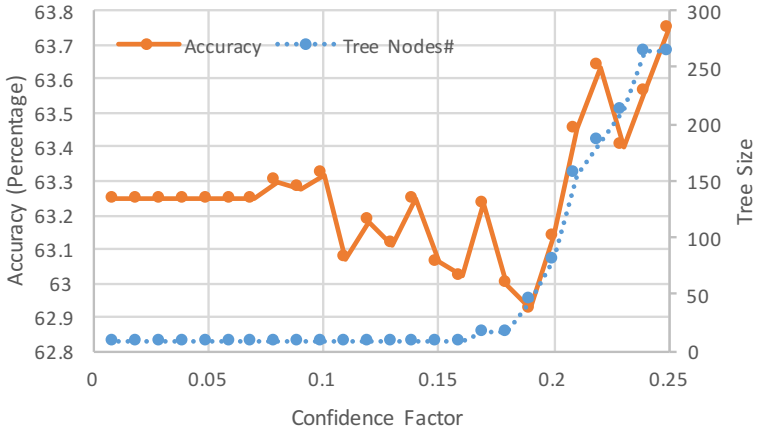


Figure 5.9: Accuracy and parsimony (tree size) of the smart default change as a function of Confidence Factor

on the J48 decision trees is called Confidence Factor (CF) in Weka, and lowering the Confidence Factor will incur more pruning. We tested the J48 classifier with a Confidence Factor ranging from 0.01 to 0.25 (the default setting in Weka) with an increments of 0.01.

Figure 5.9 displays the accuracy and the size of the decision tree as a function of the Confidence Factor. The X-axis represents the Confidence Factor; the left Y-axis and the orange line represent the accuracy of the smart default setting; the right Y-axis and the dotted blue line represent the size of the decision tree for that setting. The highest accuracy, 63.75%, is achieved with the 264-node decision tree produced by $CF = 0.25$. The lowest accuracy, 62.9%, is achieved with the 44-node decision tree produced by $CF = 0.19$. When $CF \leq 0.16$, the decision tree contains only 8 nodes. The 8-node profile with the highest accuracy is produced by $CF = 0.10$ with an accuracy of 63.32%.

Figure 5.10 summarizes accuracy as a function of parsimony. The X-axis represents the number number of nodes in the decision tree (more = lower parsimony); the Y-axis represents the accuracy of the decision tree. The figure shows the most accurate J48 solution for any given tree size, and includes the One Rule and Naive predictions for comparison. Reducing the tree from 264 to

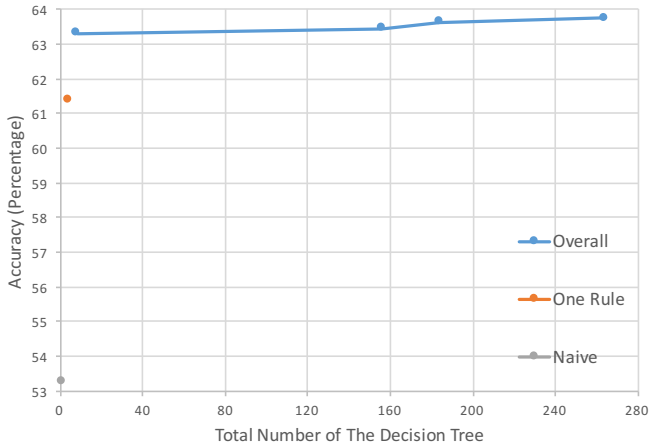


Figure 5.10: Parsimony/accuracy comparison for Naive, One Rule, and Overall Prediction

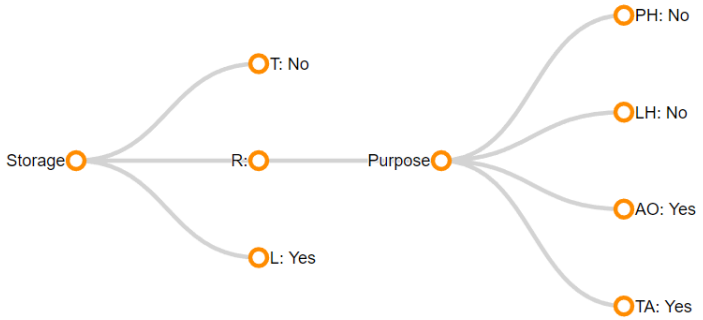


Figure 5.11: A "smart default" setting with only 8 nodes 63.32% accuracy.

8 nodes incurs a negligible 0.67% reduction in accuracy. This decision tree is shown in Figure 5.11, and is still 3.1% better than the One Rule prediction model and 18.9% better than the naive "disable all" default. This more parsimonious "smart default" setting can easily be explained to users as follows:

- All sharing with third parties will be disabled by default.
- Remote storage is allowed for automation and alerts, but not for detecting your presence or location in the house.
- Local storage is allowed for all purposes.

While the "smart default" setting makes a considerable improvement over a naive default, there is still a lot of room for improvement—even our best prediction model only correctly models on average 63.76% of the user's desired settings. This should come at no surprise, as one of the

most consistent findings in the field of privacy is that people differ substantially in their privacy preferences [65]. As a result, our "one-size fits all" default setting—smart as it may be—is not very accurate. Therefore, in Chapter 4 we moved beyond "smart default" settings by clustering participants with similar privacy preferences and creating a set of "smart profiles" covering each of the clusters [11]. The idea is that the accuracy of the tree for each cluster will likely exceed the accuracy of our overall prediction model.

In the remainder of this section we apply existing and new clustering methods with the aim of creating separate "smart profiles" for each cluster. As our goal is to develop simple, understandable profiles, we keep the parsimony/accuracy trade-off in mind during this process.

5.5.4 Attitude-Based Clustering

Our statistical results indicate that the effects of scenario parameters on users' decisions are mediated by their attitudes (Risk, Comfort, Appropriateness, Expectedness and Usefulness), as shown in Figure 5.12. Therefore, our first attempt to develop "smart profiles" is to cluster participants with similar attitudes towards the 12 scenarios they evaluated. We averaged the values per attitude across each participant's 12 answers, and ran a *k-means* clustering algorithm to divide them into 2, 3, 4, 5, and 6 clusters. We then added the participants' cluster assignments back to our original dataset, and ran the J48 decision tree algorithm on the dataset with this additional *Cluster* attribute for each number of clusters, varying the Confidence Factor from 0.01 to 0.25 with increments of 0.01. The results are summarized in Figure 5.13, which displays the most accurate solution for any given tree size and number of clusters.

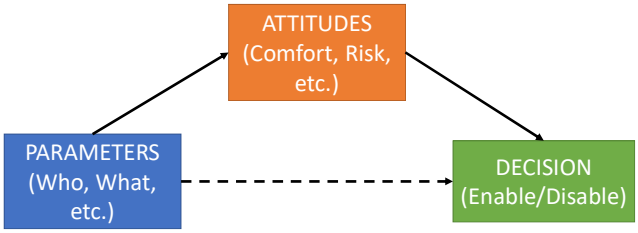


Figure 5.12: Different tests conducted for mediation analysis

All of the resulting decision trees have *Cluster* as the root node. This justifies our approach, because it indicates that the *Cluster* parameter is a very effective for predicting users' decisions. It

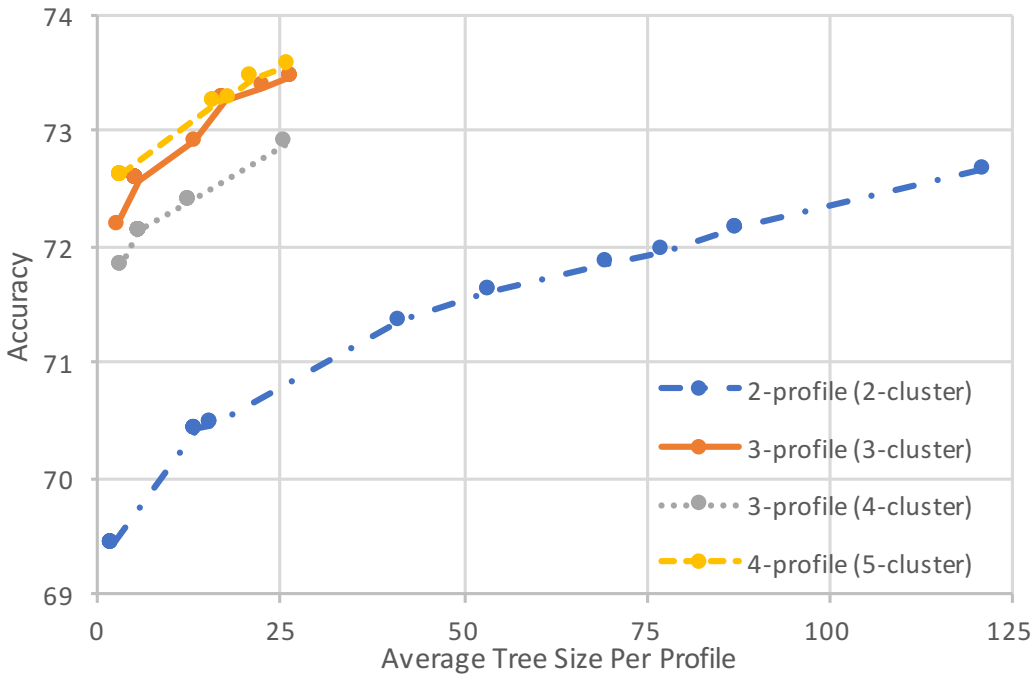


Figure 5.13: Parsimony/accuracy comparison for attitude-based clustering

also allows us to split the decision trees at the root node, and a create different "smart profile" for each subtree/cluster. Note that for some solutions two clusters end up with the same decision tree, which effectively reduces the number of profiles by 1.

For the 2-cluster solutions (the blue line in Figure 5.13), the highest accuracy is 72.66%, which is a 14.0% improvement over the best single "smart default" setting. However, this tree has an average of 121.5 nodes per profile. In comparison, the most parsimonious solution has only 1 node ("disable all") for one of the clusters, and 3 nodes ("disable sharing with third parties") for the other cluster (see Figure 5.14). This solution still has an accuracy of 69.44%, which is still an 8.9% increase over the best single "smart default" setting.

For the 3-cluster solutions (the orange line in Figure 5.13), the highest accuracy of 73.47% is achieved by a set of trees with 26.67 nodes on average (a minimal improvement of 1.1% over the best 2-cluster solution, but with simpler trees), while the most parsimonious solution has a "disable all" and an "enable all" tree, plus a tree that is the same as the most parsimonious smart default setting (see Figure 5.11). This solution has an accuracy of 72.19%, which is a 4.0% increase over the most parsimonious 2-cluster solution.

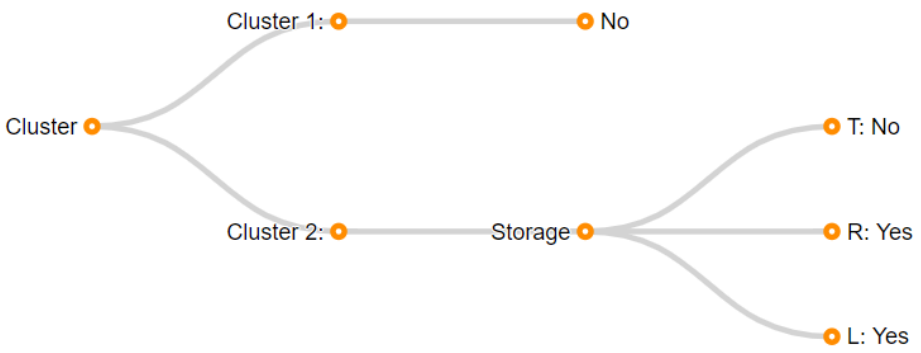


Figure 5.14: The most parsimonious 2-profile attitude-based solution.

The 4-cluster solutions (the grey line in Figure 5.13) all result in "over-clustering": all solutions based on the 4-cluster *Cluster* parameter result in two profiles with the same subtree, effectively resulting in a 3-profile solution. The accuracy of these solutions is actually lower than the accuracy of similar 3-cluster solutions, so we will not discuss them here.

The 5-cluster solutions (the yellow line in Figure 5.13) are also "over-clustered", resulting in 4 profiles. The highest accuracy of 73.56% is achieved by a set of trees with 26 nodes—this is about the same accuracy and parsimony as the most accurate 3-cluster solution. The same holds for the most parsimonious 5-cluster solution, which has a similar accuracy and parsimony as the most parsimonious 3-cluster solution.

The accuracy of the 6-cluster solutions (which result in either 4- or 5-profile solutions) is lower than the accuracy of similar 5-cluster solutions. Therefore, we will not further discuss these results.

Reflecting upon the attitude-based clustering results, we observe in Figure 5.13 that there is indeed a trade-off between accuracy and parsimony: the most parsimonious results are less accurate, but the most accurate results are more complex. Moreover, the 2-profile solutions are about 5% less accurate than the 3-profile solutions at any level of complexity. The 4-profile solutions do not improve the solution much further, though.

The 3-profile solution with an average of 18.33 nodes per profile and 73.26% accuracy provides a nice compromise between accuracy and parsimony. Part of this decision tree is shown in Figure 5.15: it contains one "disable all" profile, one "enable all" profile, and a more complex profile with 55 nodes that disallows sharing with third parties and allows remote and local storage depending on the purpose (not further shown).

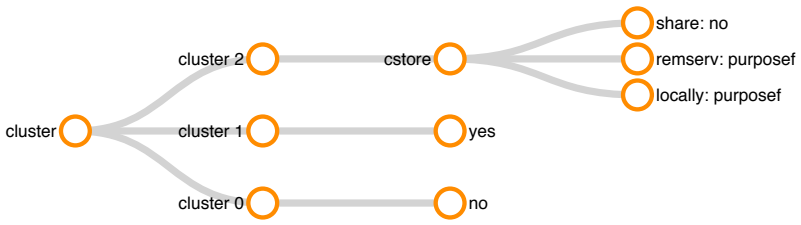


Figure 5.15: A 3-profile solution example of attitude-based clustering.

5.5.5 Agglomerative Clustering

The attitude-based clustering approach requires knowledge of users' attitudes towards the household IoT information-sharing scenarios, which may not always be available. We developed an alternative method for finding "smart profiles" that follows a hierarchical bottom-up (or agglomerative) approach, using users' decisions only. This method first fits a separate decision tree for each participant, and then iteratively merges these trees based on similarity. In our previous work [11] only 10 out of the 200 users in the dataset had unique trees fitted to them (all others had an "enable all" or "disable all" tree), making the merging of trees a rather trivial affair. Our current dataset has many more participants, and is more complex, making the agglomerative clustering approach more challenging but also more meaningful.

In the first step, 283 participants' decision trees predict "enable all", 414 participants' decision trees predict "disable all", while the remaining 436 participants have a multi-node decision tree.

In the second step, a new decision tree is generated for each possible pair of participants in the "multi-node group". The accuracy of the new tree is compared against the weighted average of the accuracies of the original trees. The pair with smallest reduction in accuracy is merged, leaving 435 clusters for the next round of merging. If two or more candidate pairs have the same smallest reduction in accuracy, priority is given to the pair with the most parsimonious resulting tree (i.e., with smallest number of nodes). If there are still multiple pairs that tie on this criterion, the first pair is picked. The second step is repeated until it reaches the predefined number of clusters, and the entire procedure is repeated with 20 random starts to avoid local optima.

To fit the trees, we use the J48 classifier with a Confidence Factor ranging from 0.01 to 0.25 with increments of 0.01. Surprisingly, smaller tree sizes result in a *higher* accuracy for agglomerative clustering (see Figure 5.16). This suggests that without extensive trimming, our agglomerative

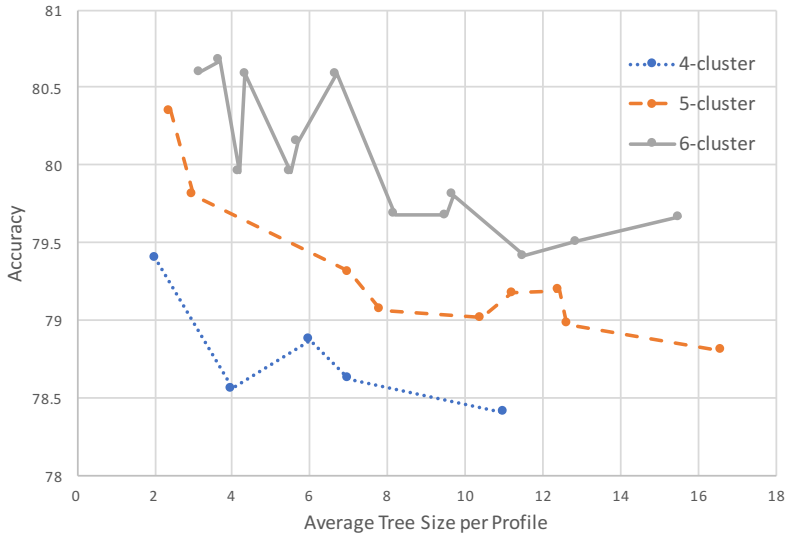


Figure 5.16: Parsimony/accuracy comparison for agglomerative clustering

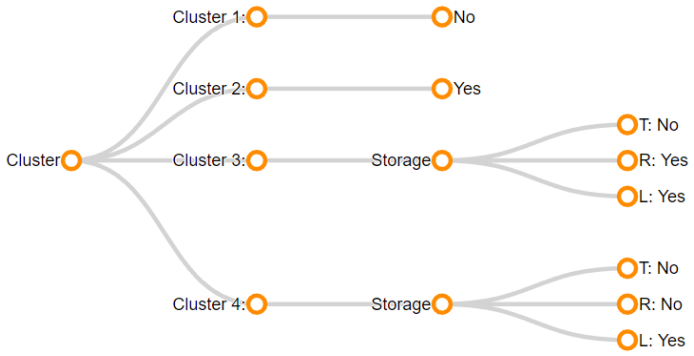


Figure 5.17: The best 4-profile agglomerative clustering solution.

approach arguably overfits the data, resulting in a lower level of cross-validated accuracy.

The best 4-cluster solution has an average of 2 nodes per profile and an accuracy of 79.40%—a 24.53% improvement over the "smart default", and a 7.9% increase over the most accurate 5-cluster/4-profile attitude-based clustering solution. The decision trees are shown in Figure 5.17[4]: aside from the "enable all" and "disable all" profiles, there is a "disable sharing with third parties" profile and a "local storage only" profile.

The best 5-cluster solution has an average of 2.4 nodes per profile and an accuracy of 80.35%—a 26.02% improvement over the "smart default", but only a 1.2% improvement over the

[4]T: Data will be stored at the remote servers and will be shared with Third Parties; R: Data will be stored at the remote servers without sharing; L: Data will be stored locally. These are the same with the following figures in this chapter

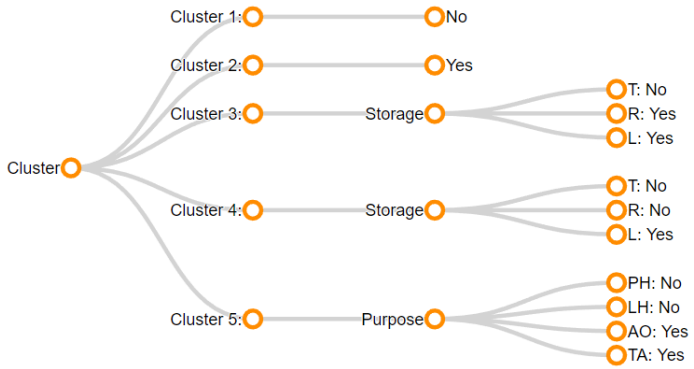


Figure 5.18: The best 5-profile agglomerative clustering solution.

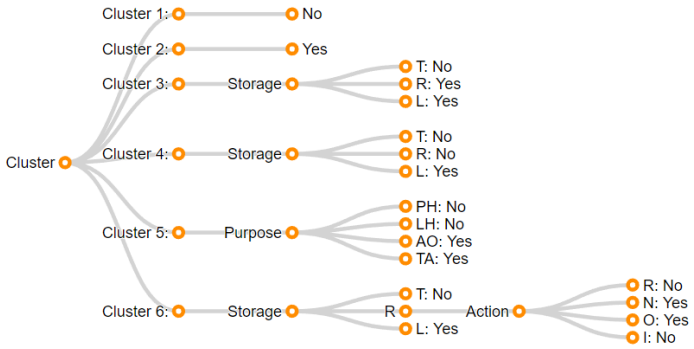


Figure 5.19: The best 6-profile agglomerative clustering solution.

4-cluster agglomerative solution. The decision trees are shown in Figure 5.18: it has the same profiles as the 4-cluster solution, plus an "allow automation and alerts, but don't track my presence or location in the house" profile.

Finally, the best 6-cluster solution[5] has an average of 3.17 nodes per profile and an accuracy of 80.68%—a 26.54% improvement over the "smart default", but no substantial improvement over the 5-cluster agglomerative solution. The decision trees are shown in Figure 5.19: it has the same profiles as the 5-cluster solution, plus a profile that allows local storage for anything, plus remote storage for any reason except for user profiling (i.e., to recommend other services or to give the user insight in their behavior).

[5]There is another solution with slightly fewer nodes per profile (2.67) and a slightly lower accuracy (80.60%).

5.5.6 Fit-Based Clustering

We now present a "fit-based" clustering approach that, like the agglomerative approach, clusters participants without using any additional information. Instead, it uses the fit of the tree models to bootstrap the process of sorting participants into different clusters. The process of our algorithm is similar as the one we used in previous chapter shown in Figure 4.5. The detailed steps are as follows:

- **Random starts:** We randomly divide participants into k separate groups, and learn a tree for each group. This is repeated until a non-trivial starting solution (i.e., with distinctly different trees per group) is found.
- **Iterative improvements:** Once each of the k groups has a unique decision tree, we test for each participant which of the k trees best represents their 12 decisions. If this is the tree of a different group, we switch the participant to this group. Once all participants are evaluated and put in the group of their best-fitting tree, the tree in each group is re-learned with the data of the new group members. This then prompts another round of evaluations, and this process continues until no further switches are performed.
- **Repeat**: Since this process is influenced by random chance, it is repeated 1,000 times in its entirety to find the optimal solution. Cross-validation is performed in the final step to prevent over-fitting.

We perform this approach to obtain 2-, 3-, 4-, and 5-cluster solutions. To fit the trees, we use the J48 classifier with a Confidence Factor ranging from 0.01 to 0.25 with increments of 0.01. The best results are summarized in Figure 5.20.

For the 2-cluster solutions (the blue line in Figure 5.20), the highest accuracy is 76.72%—a 20.33% improvement over the "smart default" setting and a 5.6% improvement over the most accurate 2-cluster attitude-based solution. However, this tree has an average of 151.5 nodes per profile. The most parsimonious solution is exactly the same as the most parsimonious 2-cluster attitude-based solution (see Figure 5.14), but with a higher accuracy (74.43%).

For the 3-cluster solutions (the orange line in Figure 5.20), the highest accuracy of 80.81% is achieved by a set of trees with 65.33 nodes on average. This is a 26.74% improvement over the "smart default", a 10.0% improvement over the most accurate 3-cluster attitude-based solution (but

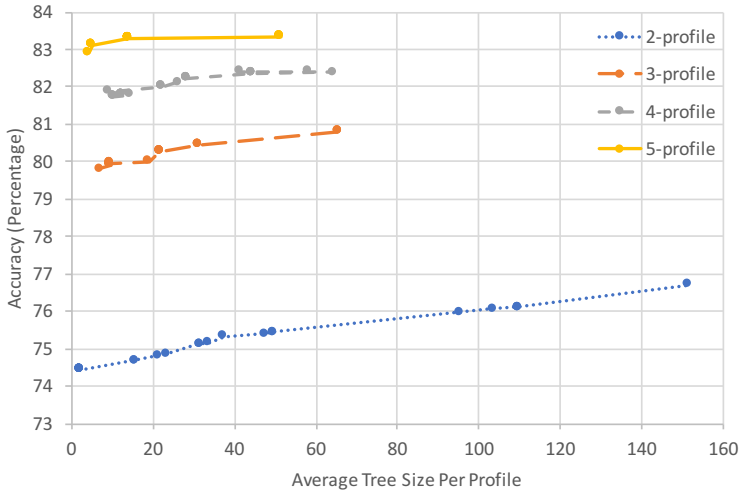


Figure 5.20: Parsimony/accuracy comparison for fit-based clustering

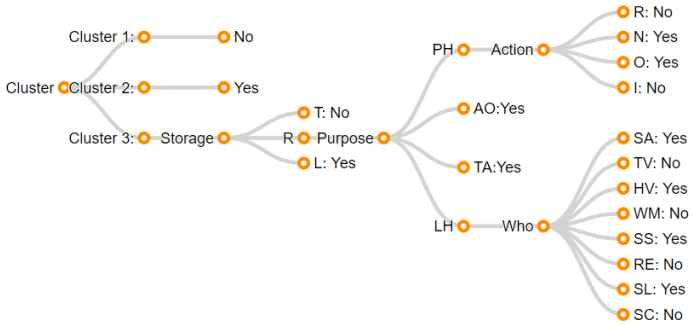


Figure 5.21: The most parsimonious 3-profile fit-based solution.

at a cost of lower parsimony), and a 5.2% improvement over the best 2-cluster fit-based solution. The most parsimonious solution, on the other hand, has 7 nodes on average, with an accuracy of 79.80%, thereby still outperforming all other 3-profile solutions. The decision trees for this solution are shown in Figure 5.21.

For the 4-cluster solutions (the grey line in Figure 5.20), the highest accuracy of 82.41% is achieved by a set of trees with 58.25 nodes on average. This is a 29.25% improvement over the "smart default", a 3.8% improvement over the 4-cluster agglomerative solution (but at a cost of lower parsimony), and a 2.0% improvement over the best 3-cluster fit-based solution. The most parsimonious solution, on the other hand, has 9.25 nodes on average, with an accuracy of 81.88%. It still outperforms all other 4-profile solutions, but the agglomerative solution is more parsimonious. The decision trees for this solution are shown in Figure 5.22.

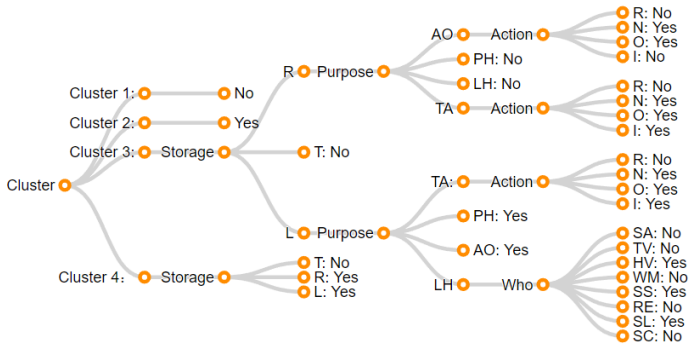


Figure 5.22: The most parsimonious 4-profile fit-based solution.

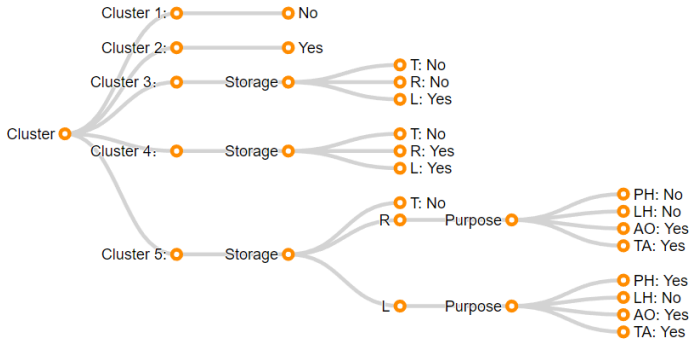


Figure 5.23: The most parsimonious 5-profile fit-based solution.

For the 5-cluster solutions (the yellow line in Figure 5.20), the highest accuracy of 83.35% is achieved by a set of trees with 51.4 nodes on average. This is a 30.05% improvement over the "smart default", a 3.8% improvement over the 5-cluster agglomerative solution (but at a cost of lower parsimony), and a 1.1% improvement over the best 4-cluster fit-based solution. The most parsimonious solution, on the other hand, has 4.2 nodes on average, with an accuracy of 82.92%. It still outperforms the 5-profile agglomerative solution, but it is slightly less parsimonious. The decision trees for this solution are shown in Figure 5.23.

5.5.7 Discussion of machine learning results

Figure 5.24 shows a comparison of the presented approaches. The X-axis represents the parsimony (higher average tree size per profile = lower parsimony); the Y-axis represents the accuracy. While the "smart default" setting makes a significant 15.3% improvement over the naive default setting ("disable all"), we observe that having multiple "smart profiles" substantially increases the

prediction accuracy even further. The fit-Based clustering algorithm performs the best out of all the approaches, followed by agglomerative clustering and attitude-based clustering.

The most parsimonious 2-profile fit-based solution (with an accuracy of 74.43%) is the *simplest* of all "smart profile" solutions: one profile is simply "disable all", while the other profile is the same as our OneR solution: "disable sharing with third parties". In fact, these profiles are so simple, that one might not even want to bother with presenting them to the user: in our current interface (see Figure 5.6) these defaults are incredibly easy for users to implement by themselves.

The same is true for the 4-profile agglomerative clustering solution (see Figure 5.17) and the 5-profile agglomerative clustering solution (see Figure 5.18): these profiles involve little more than a single high-level setting, which users can likely easily make by themselves.

The 5-profile fit-based solution is the *most accurate* of all "smart profile" solutions. The most parsimonious 5-profile fit-based clustering solution (Figure 5.23) has an accuracy of 82.92%. It has the following five profiles:

- Enable all
- Enable local and remote storage, but disable third-party sharing
- Enable local storage only
- Enable local storage for everything except location-tracking, enable remote storage for everything except location- and presence-tracking, and disable third-party sharing
- Disable all

The fourth profile in this list specifies an interaction between between **Storage** and **Purpose**—something that is not possible in our current manual settings interface (which only allows interactions between **Who**, **What**, and **Purpose**). The next section will present a slightly altered interface that accommodates these profiles.

There is another 5-profile fit-based solution with a slightly higher accuracy (83.11%) and a reasonably simple tree (5 nodes/profile on average). This solution is shown in Figure 5.25. In this solution, the third profile ("enable local storage only") is replaced by a slightly more complex profile ("enable local storage only, but not to recommend other services"). This profile specifies an additional interaction between **Storage** and **Action**. The next section will present a settings interface that accommodates this profile as well.

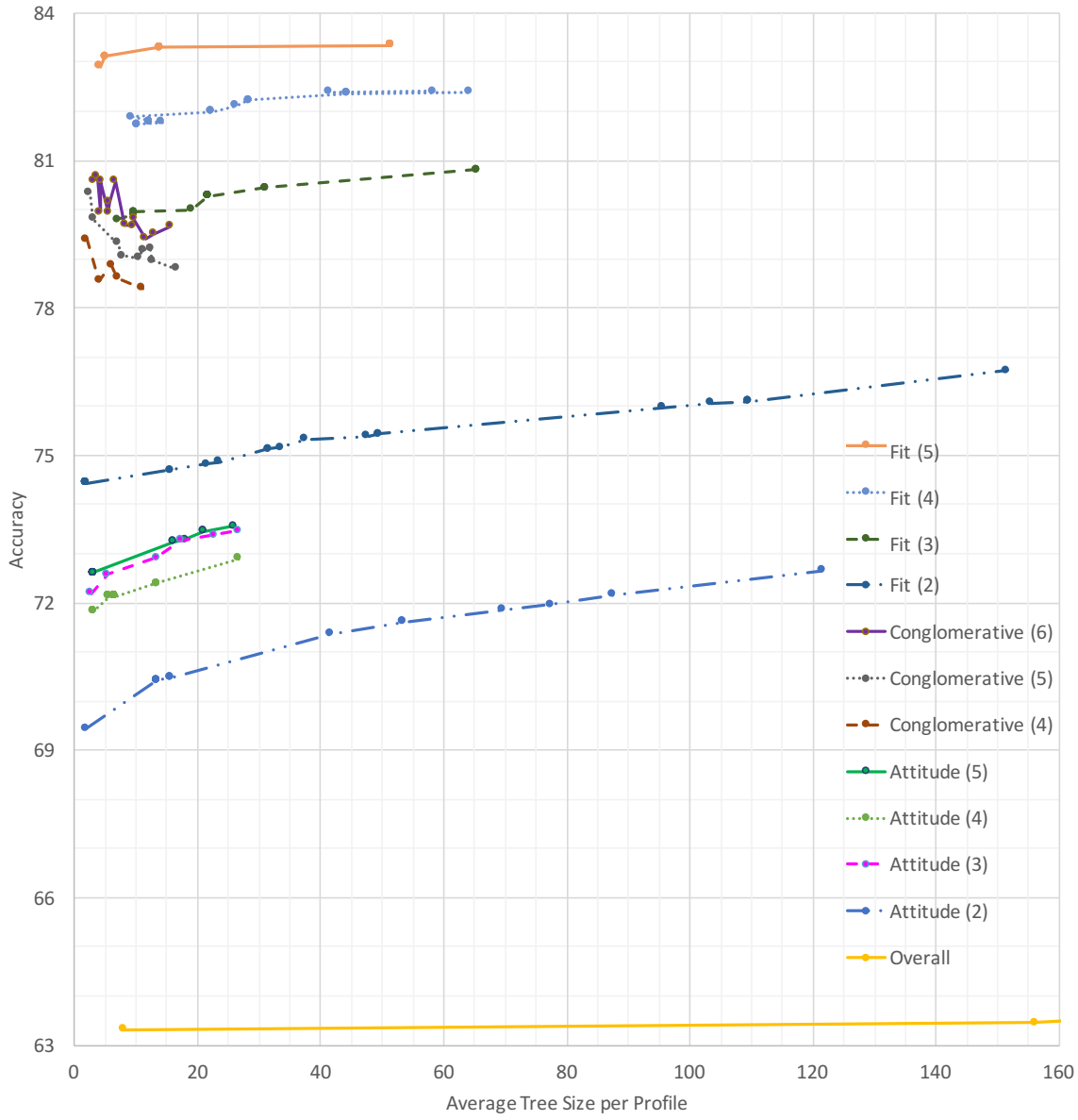


Figure 5.24: Summary of All our Approaches

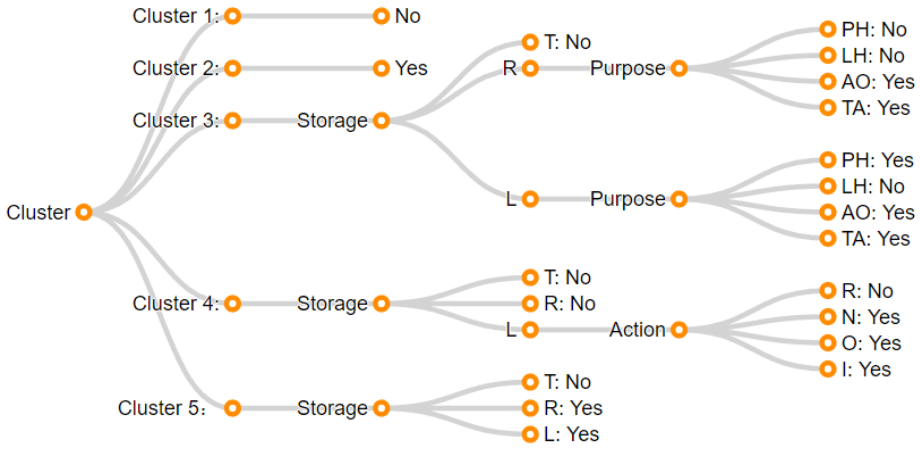


Figure 5.25: A good 5-profile fit-based clustering solution.

Other usable solutions are the 3-profile fit-based solution (Figure 5.21) or the 4-profile fit-based solution (Figure 5.22. However, like almost all of the less parsimonious solutions, these profiles involve higher-order interaction effects, e.g. between **Storage**, **Purpose**, and **Action**; and between **Storage**, **Purpose**, and **Who**. Consequently, a rather more complex interface is needed to accommodate these default profiles.

5.6 Privacy-Setting Prototype Design Using Machine Learning Results (original work)

In Section 5.4 we developed a prototype interface that household IoT users can use to manually set their privacy settings (see Figure 5.6). Our machine learning analysis (Section 5.5) resulted in a number of interesting solutions for "smart profiles" that would allow users of this interface to set their privacy settings with a single click (i.e., a choice of profile). While some of these profiles can be integrated in our prototype (e.g., the most parsimonious 2-profile fit-based solution and the 4-profile and 5-profile agglomerative solutions) other profiles have an interaction effect between variables that are modeled as independent in our current prototype interface (e.g., the two 5-profile fit-based solutions presented in Figures 5.23 and 5.25).

In this section we therefore present two modified prototypes that are designed to be compatible with these two 5-profile solutions. These two solutions are not the most accurate, but they produce a parsimonious set of profiles that require only minimal alterations to our interface design.

They thus provide the optimal trade-off between reduction accuracy, profile parsimony, and interface complexity.

5.6.1 Interface for the 5-profile fit-based solution with an accuracy of 82.92%

This machine learning solution (Figure 5.23) requires an interaction between the *Storage* parameter and the *Purpose* parameter—two parameters that are controlled independently in the prototype in Figure 5.6. Our solution is to slightly alter the interface, and add the profile selection page at the beginning of the interface. As shown in Figure 5.26, from top left, screen 1 is the profile selection page, screen 2 is the slightly altered landing page of our manual settings interface, screen 3 is the slightly altered Data Storage page, screen 4 (bottom left) is the Device/Sensor Management page, and screen 5 is the Data Use page.

- **Screen 1:** On this screen users choose their most applicable default profile. For some users, the selected profile accurately represents their preferences, while others may want to adjust the individual settings manually.
- **Screen 2:** After clicking 'Next', users are given the option to select 'Storage/Sharing & Device/Sensor Management' or 'Data Use'.
- **Screen 3:** When users select either 'Storage/Sharing & Device/Sensor Management' they first get to set their sharing preferences for 'local storage', 'remote server' and 'third party sharing' (*Storage*). Each of these can independently be set to *enabled* or *disabled*, but users can also click on 'More'.
- **Screen 4:** When users select 'More', they can manage *Who-What-Purpose* combinations for that particular storage/sharing option.
- **Screen 5:** When users select 'Data Use' on screen 2, they get to enable/disable the use of the collected data for various secondary purposes (*Action*).

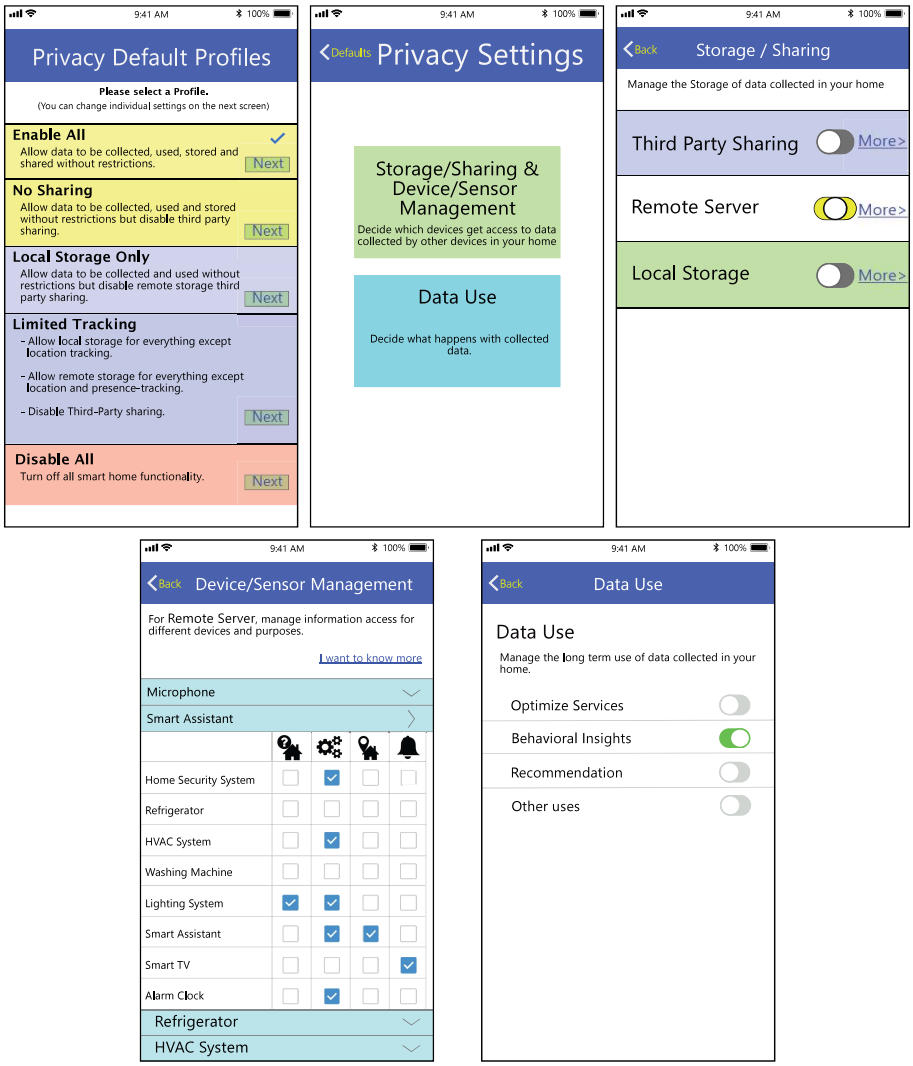


Figure 5.26: Design for 5-Profile solution presented in Section 5.6.1.

5.6.2 Interface for the 5-profile fit-based solution with an accuracy of 83.11%

The alternative machine learning solution presented in Figure 5.25 requires an additional interaction between the *Storage* parameter and the *Action* parameter. This requires us to slightly alter the interface again. As shown in Figure 5.27, from top left, screen 1 is the profile selection page, screen 2 is the slightly altered Data Storage page, screen 3 follows the 'More' button to offer access to screen 4 (bottom left, the Data Use page) and screen 5 (bottom right, the Device/Sensor Management page)

- **Screen 1:** The profile selection screen remains unchanged, with the exception that the 'Local storage only' profile is replaced by the more complex 'Local Storage & No Recommendations' profile.
- **Screen 2:** After clicking 'Next', users first get to set their sharing preferences for 'local storage', 'remote server' and 'third party sharing' (*Storage*). Each of these can independently be set to *enabled* or *disabled*, but users can also click on 'More'.
- **Screen 3:** When users select 'More', they are given the option to select either 'Device/Sensor Management' or 'Data Use'.
- **Screen 4:** When users select 'Device/Sensor Management' they can manage *Who-What-Purpose* combinations for that particular storage/sharing option.
- **Screen 5:** When users select 'Data Use' they get to enable/disable the use of the collected data for various secondary purposes (*Action*) for that particular storage/sharing option.

5.6.3 Reflection on design complexity

The interfaces presented in this section have an additional 'layer' compared to the original interface presented in Section 5.4. This additional layer makes setting the privacy settings manually more difficult, but it is necessary to accommodate the complexity of the smart profiles uncovered by our machine learning analysis. On the one hand, this demonstrates the value of developing a parsimonious machine learning model—the more accurate but more complex profiles that comprise some of the solutions in Section 5.5 are not only more difficult to explain to the user, they also contain

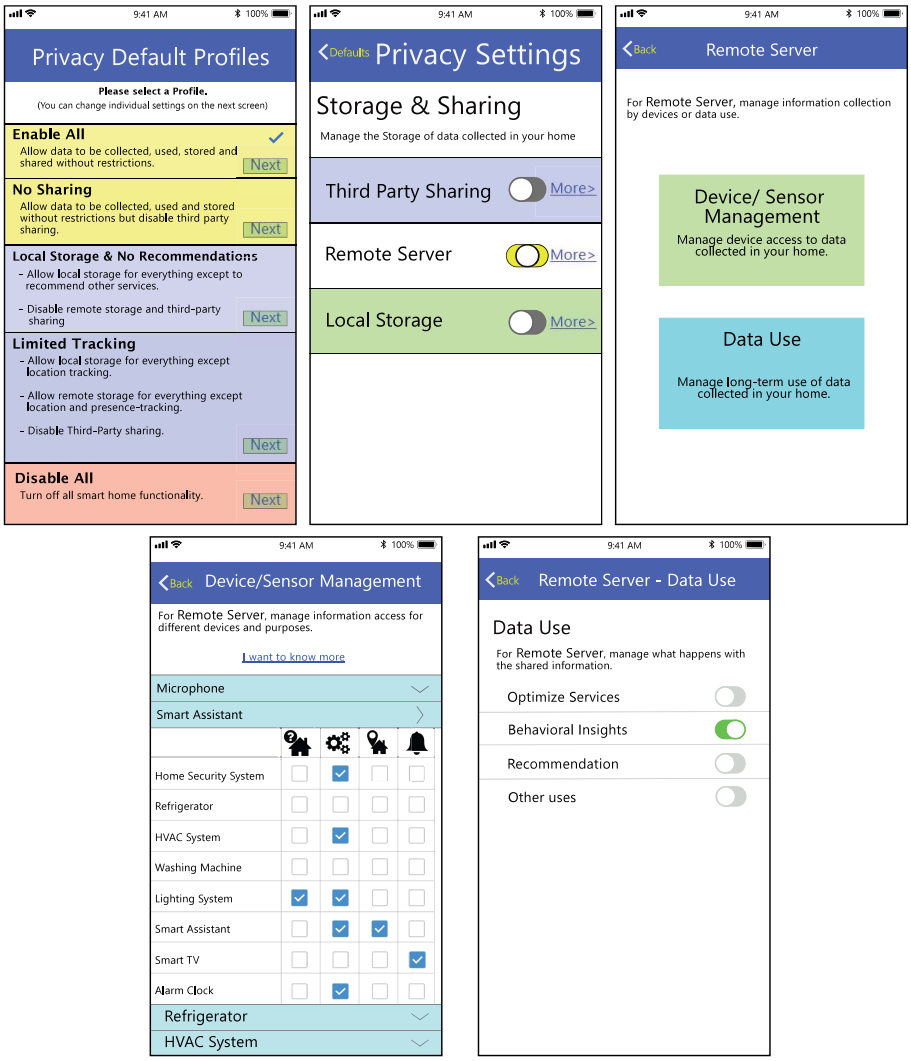


Figure 5.27: Design for 5-Profile solution presented in Section 5.6.2.

more complex interactions between decision parameters, forcing the manual settings interface to become even more complex. A simple smart profile solution avoids such complexity in the interface.

On the other hand, one should not over-simplify the profiles, lest they become overly generic and inaccurate in representing users' privacy preferences. Indeed, when we make our smart profile solutions more accurate, fewer users will need to make any manual adjustments at all, so we can allow some additional complexity in the interface.

5.7 Limitations

In this section, we discuss the limitations of our work, our plans to evaluate the presented interfaces.

We note that participants in our study made decisions about hypothetical rather than "real life" scenarios. However, compared to most other privacy studies, our study asks participants about very specific IoT scenarios, measuring their attitudes and behaviors in the context of these scenarios. The hypothetical nature of the scenarios is thus a conscious trade-off here: it is impossible to measure privacy in 4000+ scenarios without presenting them on a screen.

A limitation regarding our machine learning approach is that it assumes a perfect assignment of users to profiles. However, in our current approach, users of the profile-based interface make their own choice as to which profile they want to apply. If they do not make the correct choice, then this introduces additional uncertainty, and the accuracy of our approach will be substantially lower than described in our paper. This limitation highlights the importance of the parsimony/accuracy tradeoff: Users benefit from parsimony in the context of our study, because parsimony makes for simpler profiles, which are easier to understand and hence easier to choose from. At the same time, though, these more parsimonious profiles are likely going to be less accurate, which means that users need to make more manual adjustments to the profile-based settings.

Our biggest limitation is that we did not test any of the presented interfaces, so we do not know what level of complexity (in term of both the complexity of the user interfaces and the profiles) is most suitable. I will address this limitation in my final study (Chapter 7).

5.8 Summary

In this chapter, we have presented the following:

- Using an intricate mixed fractional factorial study design, we collected a dataset of 1133 participants making 13596 privacy decisions on 4608 scenarios.
- We performed statistical analysis on this dataset to develop a layered IoT privacy-setting interface. As our analysis shows more complex decision patterns than our previous work, we presented guidelines to translate our statistical results into a more sophisticated settings interface design.
- We performed machine learning analysis on our dataset to create a set of "smart profiles" for our IoT privacy-setting interface. Beyond our work in Chapter 4, we conducted a deeper analysis regarding the trade-off between parsimony and accuracy of our prediction models, leading to a better-informed selection of smart profiles.
- Aside from the privacy-setting interface and the smart profiles, we made specific design recommendations for household IoT devices that can help to minimize users' privacy concerns.

In the next chapter, we discuss our work applying data-driven approach in the fitness IoT context.

Chapter 6

Recommending Privacy Settings for Fitness IoT

6.1 Introduction

In Chapter 4 and 5, we have discussed how we apply the data-driven approach to the general/public IoT and household IoT contexts, respectively. We developed corresponding IoT privacy-setting interface prototypes that integrated with smart defaults/profiles by predicting users' privacy decisions. In this chapter, we present the work we did in the domain of fitness IoT. We further test the previously-developed data-driven approach to design privacy-setting interfaces for users of fitness IoT devices. Note that moving the context from general/public IoT to household IoT, now to fitness IoT, the context that we are focusing is becoming more narrow. The change of environment brought more challenge. For example, for fitness IoT, there is no contextual scenario, which we focused on in Chapter 4 and 5. Considering almost all the current fitness IoT devices require corresponding mobile Apps to be used together and the mobile Apps are usually the ones who are take charge of users' privacy information, we focus on the privacy permissions asked by the mobile Apps. In this Chapter, we first collect users permission decisions to fitness IoT permissions[1]. Then we apply our data-driven approach to classify users into groups based on their permission decisions, and create permission profiles for each group. This allows new users to answer very few

[1] unlike previous chapters, for fitness IoT you have multiple profiles per user, namely one for each type of data.

questions before getting a recommendation of a set of permission profiles, which simplifies users' task of setting every permission for fitness IoT devices.

6.2 Data Model

As discussed in Section 6.1, the mechanism that most modern fitness trackers use to guide their user to manage privacy settings is by asking users various permission questions. We first investigate the questions asked by mainstream fitness trackers, and then adapt those questions for the use of our data model in this study.

As shown in Figure 6.1, we examined the permission questions asked by the mainstream fitness trackers (Fitbit, Garmin, Jawbone, and Misfit) and categorized these questions into 3 groups – *Smartphone Persmission*, *In-app Requests*, and *Fitness Data*,.

6.2.1 Smartphone Permissions (S set)

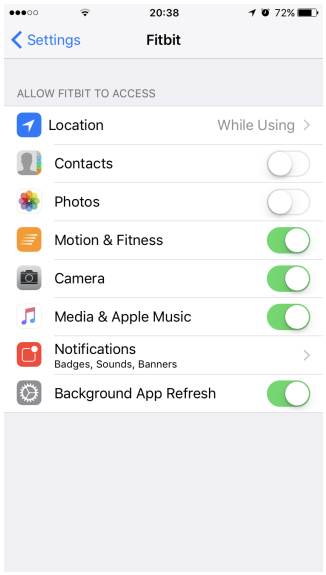
The first group of permissions are the smartphones permissions, which are requested during the installing or the first use of the mobile application. The requested smartphone permissions differs by the brands of the fitness trackers as well as the mobile Operation System of the smartphones. As shown in Figures 6.2a and 6.2b, even for the mobile application from the same manufacturer (Fitbit), the requested smartphone permissions are different between the iOS version and the Android version. We summarize all the requested smartphone permissions by popular brands of fitness trackers' mobile application across different mobile Operating Systems (i.e. iOS, Android, and Windows Mobile).

6.2.2 In-App Requests (A set)

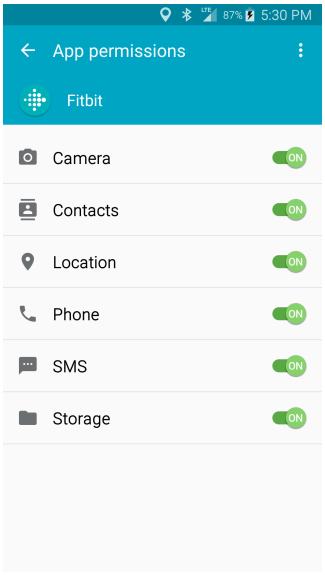
Fitness tracks also intend to collect user's data in their mobile applications. For example, Fitbit asks users to provide their *First Name*, *Last Name*, *Gender*, *Height*, *Weight*, *Birth Date*, as shown in Figure 6.3 when signing up an account during the first-time using the mobile App. Note that these data are mandatory for all fitness trackers in Figure 6.1; the only optional piece of information is Misfit's request on users' occupation. Figure 6.3 shows the *A set* for the Fitbit app (other apps are similar).

	Fitbit	Garmin	Jawbone	Misfit	Our Data Model
(S Set) Smartphone Permissions	• Identity • Contacts • Location • SMS • Camera • Bluetooth • Storage • Device & Call Inf. • Photos/ Media/Files	• Identity • Calendar • Contacts • Location • Phone • Camera • SMS • Device & Call Inf. • Photos/ Media/Files • WiFi Inf. • Storage	• Identity • Contacts • Location • SMS • Microphone • Phone • Storage • Device & Call Inf. • Photos/ Media/Files	• Identity • Contacts • Location • SMS • Camera • Phone • Storage • Device & Call Inf. • Photos/ Media/Files	• Identity • Contacts • Location • Phone • Camera • Storage • Media & Music • Photos • Motion & Fitness • SMS • Bluetooth • Mobile Data
(A set) In-app Requests	• First Name • Last Name • Gender • Height • Weight • Birth date	• Full Name • Display Name • Birth date • Gender • Height • Weight	• First Name • Last Name • Gender • Height • Weight • Birth date	• Full name • Gender • Weight • Height • Birth date • Occupation (optional)	• First Name • Last Name • Gender • Height • Weight • Birth date
(F Set) Fitness Data	• Activity & Exercise – steps – distance – elevation – floors – activity minutes – calories activity • Weight • Sleep • Heartrate • Food & Water Logs • Devices & Settings • Location & GPS • Friends • Profile	• Full data • Location • Sync Device	• Basic Info • Extended Info • Heartrate • Meals • Moves • Sleep • Friends list	• Profile • Goal • Device • Summary – steps – calories – activity calories – distance • Session • Sleep	• steps • distance • elevation • floors • activity minutes • calories activity • weight • Sleep • Heartrate • Food & Water Logs • Location • Devices & Settings • Friends • Profile
(G Set) GDPR Permissions					Entity Types • SN (public) • SN (friends only) • health/fitness apps • other apps • corp. fitness programs • gov't. fitness programs Purposes • safety • health • social • commercial • convenience • Frequency • Retention

Figure 6.1: Comparison of permissions asked by Fitness Trackers and the fitness IoT Data Model used for this study.



(a) The interface of smartphone permissions of Fitbit iOS App



(b) The interface of smartphone permissions of Fitbit Android App

Figure 6.2: Interface examples of Smartphone Permissions requests for Fitbit trackers (S set)

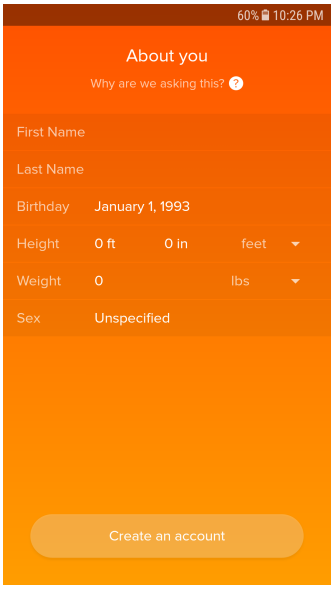


Figure 6.3: Interface example of In-App Permissions requests in Fitbit Android App (A set)

6.2.3 Fitness Data Permissions (F set)

F set contains fitness-related data that is either automatically collected by the fitness tracker or manually input by the users, such as food and water logs, friend list. As shown in Figure 6.1, we follow Fitbit's permission model for F set but give users more fine-grained control over *Activity and Exercise* data by breaking these permissions down into steps, distance, elevation, floors, activity minutes, and calories activity. A total of 14 permissions are included in the F set for our study.

6.2.4 GDPR-based Permissions (G set)

As of May 25, 2018, the European Union (EU) enforce the General Data Protection Regulation (GDPR) [112] which applies to the storage, processing and use of the subject's personal data from the third parties which may or may not have been established in the EU as long as they operate in an EU market or acess data of EU residents. It requires users to provide explicit consent to privacy options expressed by third parties. The G set includes permissions that are based on GDPR requirements. The purpose of data collection, *hasReason*, includes *safety*, *health*, *social*, *commercial* and *convenience*. The frequency of data access, *hasPersistence*, includes *continuous access*, *continuous access but only when using the app*, and *separate permissions for each workout*. For the retention period of collected data, *hasMaxRetentionPeriod*, permissions include *retain until no longer necessary*, *retain until the app is uninstalled*, and *retain indefinitely*. We did not include the *hasMethod* property since it involves technical background.

The types of third parties (instances of *EntityType*) that can request access to the user's Fitness data include *health/fitness apps*, *Social Network (SN) apps* (*public* or *friends* only), *other apps on the user's phone*, and *corporate* and *government fitness programs*.

6.3 Dataset

The dataset we use in this study was collected by my colleague Odnan. 310 participants were asked to set up a new account using a fitness tracker mobile App similar to Fitbit. They were then asked the 4 groups of questions that we discussed in our data model. For each question, the answer will be either "Allow" or "Deny", meaning the participants are either willing to provide information for that permission or not. After answering these questions, participants were then asked to fill our a survey questionnaire measuring their privacy-related attitudes (i.e. Trust, Privacy

concerns, Perceived surveillance and intrusion, and Concerns about the secondary use of personal information), the negotiability of their privacy settings, their social behaviour (social influence and sociability), exercise tendencies (a proxy for their attitude and knowledge about fitness tracking), and demographic information.

As shown in Figure 6.4, participants intend to have a higher disclose rate for their demographics information (A set), which is in line with the results of other studies [64].

For the smartphone permissions (S set), participants are more likely to allow motion, location, bluetooth, and mobile data, which are usually the minimum permissions required for a fitness mobile App to work. In S set, the access to contacts and photos are the least allowed permissions.

Regarding the G set, participants seem most open to data collection for health (the main purpose of a fitness tracker) and safety (another popular purpose often advertised by the manufacturers). On the other hand, users are less likely to agree to data collection with an indefinite retention period, and they prefer not to share data with government fitness programs or publicly on social media.

6.4 Predicting users' Preference (partial original work)

We predict participants' *allow*/*deny* decision using machine learning methods. Our dataset shows considerable variability between participants' privacy preferences—a finding that is broadly reflected in the privacy literature [65]. Using clustering, one can capture the preferences of various users with a higher level of accuracy. Hence, the goal of this section is to find a concise set of profiles, clusters, that can represent the variability of the permission settings among our study participants.

We cluster participants' permissions with Weka[2] using the K-modes clustering algorithm with default settings. The K-modes algorithm follows the same principles as the more common K-means algorithm, but it is more suitable for the nominal variables in our dataset.

6.4.1 Overall Prediction

In our first clustering attempt we tried to find a set of profiles by clustering the full dataset, including the A, F, S, and G subsets. A drawback of this method is that, assume we cluster the users into n clusters, this method will only provide n possible profiles to be used for recommendations to

[2] `https://www.cs.waikato.ac.nz/ml/weka/`

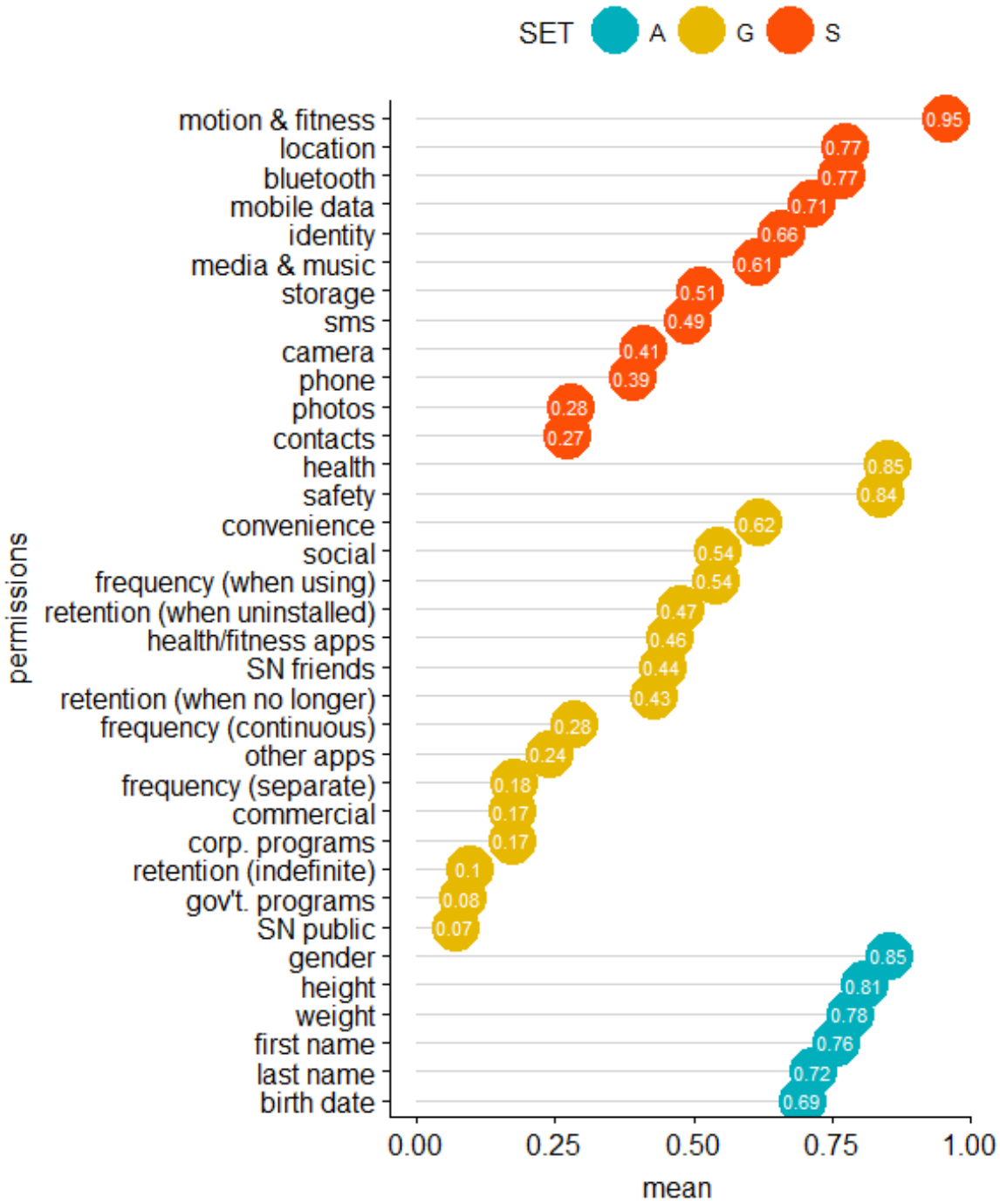
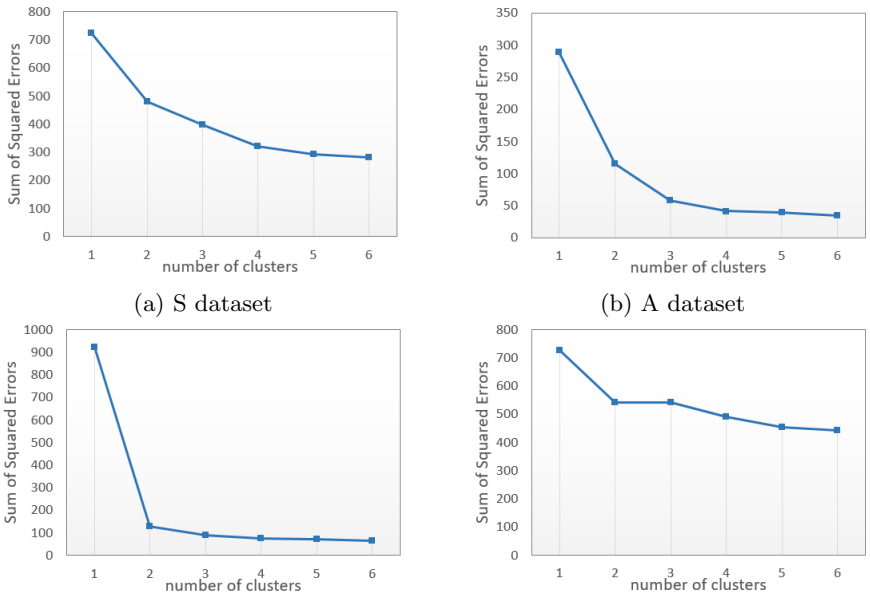


Figure 6.4: Average values of each privacy permissions (1-allow, 0-deny).



(a) S dataset (b) A dataset

(c) F dataset (d) G dataset

Figure 6.5: Evaluation of different numbers of clusters for each set.

the users. A further drawback of clustering based on the full set of 45 permissions is that it has high error rates (e.g., the sum of squared error for the viable 4-cluster solution is 1435 and 1688 for 2-cluster solution). In addition, the profile provided will be complicated since all the settings from four different sets are presented in a single profile, making it difficult to explain to the users.

If we instead generate a separate set of n "subprofiles" for each of the four datasets (A, F, S, and G), n^4 different combinations of profiles can be used for recommendation, providing finer-grained privacy-setting controls to the users compared to clustering the full set. In addition, error rates are lower when clustering each set separately, as shown in Figure 6.5. For example, with only 2 clusters per set, the sum of squared error reduces to 1277 (a 24.3% reduction). An additional benefit is that the profiles for each set can be investigated in more detail.

In our dataset the fitness data permissions (F set) are specified repeatedly for each Entity Type (part of the G set). We tried to cluster these combinations, taking into account all 98 features (i.e., 14 fitness data per 7 entity types). This analysis resulted in two profiles: one that had "allow all" for health and SN public entities (and "deny all" for all other entities), and one that had"deny all" for all entities. This means that: a) very similar results can be obtained by considering the fitness data permissions separately from the Entity Type, and b) as expected, the "who" parameter (Entity Type) is more important than the "what" parameter (fitness data permissions).

Attribute	Full Data (265.0)	Cluster# 0 (165.0)	1 (100.0)
identity	1	1	1
contacts	0	0	1
location	1	1	1
sms	0	0	1
storage	1	0	1
camera	0	0	1
bluetooth	1	1	1
photos	0	0	1
phone	0	0	1
motion & fitness	1	1	1
media & music	1	0	1
mobile data	1	1	1

(a) S dataset

Attribute	Full Data (265.0)	Cluster# 0 (99.0)	1 (166.0)
first name	1	0	1
last name	1	0	1
gender	1	1	1
birth date	1	0	1
height	1	1	1
weight	1	1	1

(b) A dataset

Attribute	Full Data (265.0)	Cluster# 0 (177.0)	1 (88.0)
steps	1	1	0
distance	1	1	0
elevation	1	1	0
floors	1	1	0
activity minutes	1	1	0
calories activity	1	1	0
weight	1	1	0
sleep	1	1	0
heartrate	1	1	0
food & water logs	1	1	0
friends	1	1	0
profile	1	1	0
location	1	1	0
devices & settings	1	1	0

(c) F dataset

Attribute	Full Data (265.0)	Cluster# 0 (143.0)	1 (122.0)
social network (public)	0	0	0
social network (friends)	0	1	0
health/fitness apps	0	1	0
other apps in phone	0	0	0
corp.fitness program	0	0	0
gov't.fitness program	0	0	0
health (purpose)	1	1	1
safety (purpose)	1	1	1
social (purpose)	1	1	0
commercial (purpose)	0	0	0
convenience (purpose)	1	1	0
frequency	2	2	2
retention	2	3	2

(d) G dataset

Figure 6.6: Privacy profiles from the two clustering methods: 1-cluster results (full data) and 2-clusters results (privacy subprofiles) for each dataset(allow=1, deny=0, except for frequency & retention)

In the following, we will discuss our method that generates subprofiles for each of the four datasets.

6.4.2 2-Cluster Solution

We first investigate the optimal number of clusters by running the K-modes algorithm for 1-6 clusters with a 70/30 train/test ratio, using the sum of squared errors of the test set for evaluation. The results are shown in Figure 6.5. Using the elbow method [69], we conclude that 2 is the optimal number of clusters for each dataset[3].

The final cluster centroids of the 2-cluster solution for each dataset are shown in Figure 6.6, together with the results of the 1-cluster solution. We describe the subprofiles of each set in the subsections below.

[3]We obtain similar results using other clustering algorithms, such as Hierarchical Clustering.

6.4.2.1 The *S* Set

- **Minimal** (cluster 0): this subprofile allows the minimum permissions needed to effectively run a fitness app. This includes identity, location, bluetooth, motion & fitness, and mobile data permissions.
- **Unconcerned** (cluster 1): this subprofile allows all permissions in this dataset.

6.4.2.2 The *A* Set

- **Anonymous** (cluster 0): this subprofile shares only users' gender, height and weight information but not their birth date or first and last name.
- **Unconcerned** (cluster 1): this subprofile shares all data requested in this dataset.

6.4.2.3 The *F* Set

- **Unconcerned** (cluster 0): this subprofile shares all fitness data with third parties.
- **Strict** (cluster 1): this subprofile does not share any fitness data with third parties.

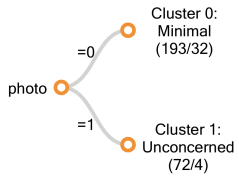
6.4.2.4 The *G* Set

- **Socially-active** (cluster 0): this subprofile shares data with health/fitness apps and social network friends, but not with other recipients. Sharing is allowed for health, safety, and social purposes but not for commercial purposes.
- **Health-focused** (cluster 1): this subprofile does not allow sharing with any third parties. Sharing is allowed only for health and safety purposes.

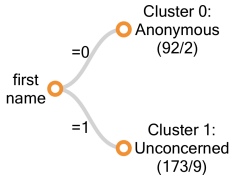
6.5 Profile Prediction (partial original work)

Now that we have identified two privacy "subprofiles" per dataset, the next step is to find predictors for the profiles and predict which subprofiles each participant belongs to.

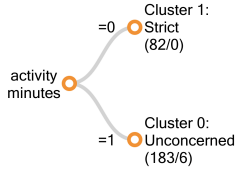
Recommender systems usually ask users to evaluate a few items before giving recommendations regarding all remaining items. Likewise, in our system, we might be able to identify certain permission items inside each privacy subprofile that—when answered by the user—could drive the



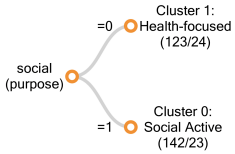
(a) S set (86.42%)



(b) A set (95.85%)



(c) F set (97.74%)



(d) G set (82.26%)

Figure 6.7: The permission drivers for the privacy subprofiles and their respective prediction accuracies.

prediction. Since the items are the permission preferences included in the subprofiles, we define this as the "direct predicition" approach.

Additionally, we also explored whether the items from our questionnaire could drive the predicition. Since these items are not part of the privacy subprofiles, we define this as the "indirect prediction" approach. For each approach and for each subset of data (S, A, F, and G sets), we develop decision trees that will enable us to predict which subprofile best describes a user. The trees contain the subprofile items (direct prediction) or questionnaire items (indirect prediction) that can be asked to classify each user into their correct subprofile.

We developed our decision trees using the J48 decision tree learning algorithm and evaluated the resulting decision tree using cross validation.

6.5.1 Direct Prediction Questions

In our direct prediction approach, the aim is to ask users to answer certain permission items from each subset as a means to classify them into the correct subprofile (thereby providing a recommendation for the remaining items in that subset). For this approach, we thus classify users using the items in the subset as predictors.

Our results for this approach are reported in Figure 6.7. It shows for each subset the question that best classifies our study participants into the correct subprofile.

When running tree-based algorithms, a trade-off has to be made between the parsimony and the accuracy of the solution. Parsimony prevents over-fitting and promotes fairness and can be

accomplished by pruning the decision trees. In our study, while multi-item trees may provide better predictions, the increase in accuracy is not significant compared to the single-item trees presented in Figure 6.7. These single-item solutions already obtained a high accuracy, and their parsimony prevents over-fitting and minimizes the number of questions that will need to be asked to the users in order to provide them accurate recommendations. The resulting solution involves a 4-question input sequence—one question for each subset.

For the S set, the Photo permission is the best subprofile predictor. This is one of the least-shared permissions (see Figure 6.4), and 94% of participants who give this permission are correctly classified into the "Unconcerned" subprofile, while 83% of participants who do not give this permission are correctly classified into the "Minimal" subprofile.

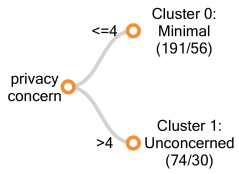
For the A set, First name is the best predictor. Again, 94% of participants who share their first name are correctly classified into the "Unconcerned" subprofile, while 98% of participants who do not share their first name are correctly classified into the "Anonymous" subprofile.

For the F set, Activity minutes permission is the best predictor. This is one of the most-shared permissions. 97% of participants who give this permission are correctly classified into the "Unconcerned" subprofile, while 100% of participants who do not give this permission are correctly classified into the "Strict" subprofile.

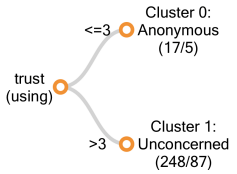
Finally, for the G set, the best predictor is whether the participants allows data collection for Social purposes. If so, participants are correctly classified into the "Socially active" subprofile with 84% accuracy, otherwise they are classified into the "Health-focused" subprofile with 80% accuracy.

6.5.2 Indirect Prediction Questions

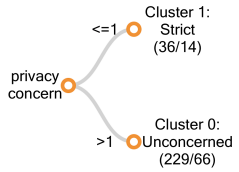
A similar procedure was applied to the questionnaire data concerning the following categories of user traits: privacy attitude, social behavior, negotiability, exercise tendencies and user demographics (cf. Table **??** in Appendix). As will be shown below, the indirect prediction approach has a lower accuracy than the direct approach presented in Section 6.5.1. This is expected since the questionnaire items about user traits have no direct relationship with the permission settings in the privacy profiles. These results are still interesting, though, since they allow the user to avoid making any specific privacy settings. Moreover, the resulting predictors show interesting semantic relationships with the datasets they predict. We discuss these results in more detail below.



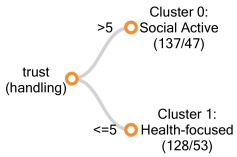
(a) S set (66.04%)



(b) A set (65.28%)



(c) F set (69.81%)



(d) G set (62.26%)

Figure 6.8: The attitude drivers for the privacy subprofiles and their respective prediction accuracies.

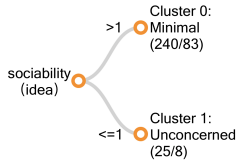
6.5.2.1 Privacy Attitudes

We first attempted to use privacy attitudes as predictors of users' subprofiles. The resulting trees for this indirect prediction are shown in Figure 6.8.

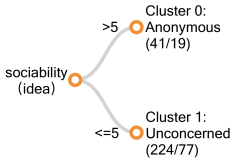
Among all the privacy attitude questions, "trust" and "privacy concern" are found to be predicting factors of user subprofiles. Interestingly, there is a single privacy concern question ("I believe other people are too concerned with online privacy issues") that predicts the user's S and F subprofiles. Those who agree that people are just too concerned about privacy issues belong to "Unconcerned" subprofile, while those who have higher concerns tend to be in the "Minimal" subprofile. The same goes for the F set where those who strongly disagree, (1) on a 7pt scale, thinking that it is a major concern belong to the "Strict" subprofile. Otherwise they are classified as "Uncocerned".

For the trust question, "I believe the company is honest when it comes to using the information they provide", it can be used to predict users' subprofile for the A set. Participants are assigned to the "Anonymous" subprofile if they answer this question with "somewhat disagree" (3) or below. Those who indicate higher levels of trust are assigned to the "unconcerned" subprofile. The A set concerns information provided directly to the fitness app, so it makes sense that trust is a significant predictor of users' willingness to provide such information.

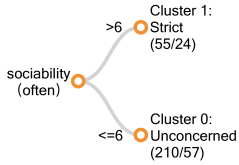
For the G set, those users who agree (6) or extremely agree (7) with the question "I believe the company providing this fitness tracker is trustworthy in handling my information" are classified in the "Socially active" subprofile, while the remaining users are classified in the "Health-focused"



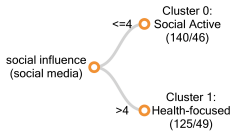
(a) S set (65.66%)



(b) A set (61.89%)



(c) F set (69.43%)



(d) G set (61.89%)

Figure 6.9: The social behavior drivers for the privacy subprofiles and their respective prediction accuracies.

subprofile. The question really fits the G set since GDPR permissions are mostly about handling the user information by the third parties. Particularly, it makes sense that users who do not trust the fitness app in handling their information would be assigned to the "Health-focused" profile, since this profile prevents the app from sharing their data to any other entity and only allows data collection for the purpose of health and/or safety.

The result shows that we managed to capture some semantically relevant relationships between users' attitudes and their assigned privacy profiles. The S and F sets share the same predictor question which makes the final solution a 3-question input sequence that is one less question to the users compared to the direct questions in Section 6.5.1.

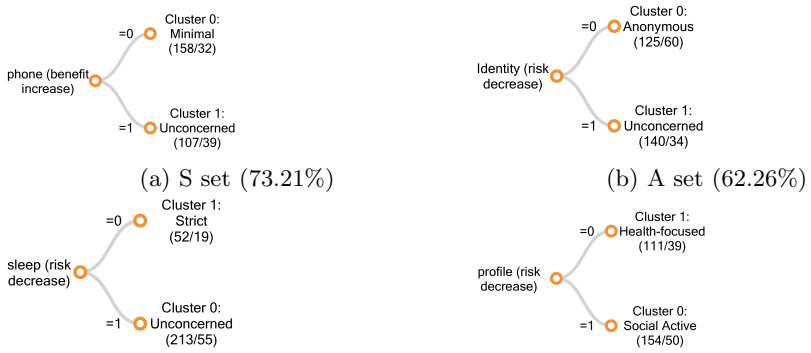
6.5.2.2 Social Behavior

We also tried to find predictors among the questions about social influence and sociability. The resulting trees for this indirect prediction are shown in Figure 6.9.

A single sociability question can be used to predict subprofiles for both the S and A sets. For the S set, users who are completely open (1) to the idea of meeting new friends when they exercise are classified in the "Unconcerned" subprofile, otherwise they are classified in the "Minimal" subprofile.

For the A set, users who are likely not (6) or definitely not (7) open to meeting new friends are classified in the "Anonymous" subprofile, otherwise they are classified in the "Unconcerned" subprofile.

For the F set, users who have never (7) met any new friends while exercising are classified



(a) S set (73.21%) (b) A set (62.26%)

(c) F set (72.08%) (d) G set (66.41%)

Figure 6.10: The user negotiability drivers for the privacy subprofiles and their respective prediction accuracies.

into the "Strict" subprofile, while others are classified into the "Unconcerned" subprofile. This, as well as the findings regarding the S and A sets, seem to suggest that users' disclosure of personal information is likely to be related with their tendency to socialize while using fitness apps.

For the G set, users who are influenced to do exercise if their social media friends also exercise (i.e., "definitely yes" to "neutral" (1-4)) are classified into the "Socially active" subprofile, otherwise they are classified into the "Health-focused" subprofile.

Again, we found interesting semantic relationships between social influence and sociability while exercising and users' privacy-related behaviors: users who are more prone to reap social benefits from exercising are more likely to give the app more widespread permissions. Similar to privacy attitudes, these predictors only involve a 3-question input sequence.

6.5.2.3 Negotiability of Privacy Settings

We also attempted to use the negotiability of users' privacy settings as input for the subprofile prediction. Figure 6.10 shows the tree-learning solutions for this approach.

For the S set, users who are willing to give the Phone permission (access phone calls and call settings) if the benefits increase are classified into the "Unconcerned" subprofile, while users who refuse to share the Phone permission even if the benefits increase are classified into the "Minimal" subprofile. In other words, the privacy preferences of the latter group are not negotiable; they will still share only the minimum permissions needed to run the tracker, even if the benefits increase.

For the A set, users who are willing to give the Identity permission (account and/or profile information) if the risks decrease are classified into the "Unconcerned" subprofile, otherwise they

are classified into the "Anonymous" subprofile. Interestingly, the Identity permission is part of the S set rather than the A set, but it semantically coincides with the items in the A set, which include the user's name and birth date (i.e., identifying information). As such, it makes sense that users who are unwilling to share their phone's identifier even when the risks decrease are also unwilling to share their personal identity information.

For the F set, users who share their Sleep fitness data with other third parties if the risks decrease are classified into the "Unconcerned" subprofile, otherwise they are classified into the "Strict" subprofile. Users in the latter subprofile will not share their fitness data with any other third parties, even if the risk decreases.

For the G set, users who share their fitness app Profile with other third parties if the risks decrease are classified into the "Socially active" subprofile, otherwise they are classified into the "Health-focused" subprofile. Even though Profile is a permission from the F set, it semantically coincides with the subprofiles of the G set: users in the "Socially active" subprofile tend to have permissions that allow them to connect to others while exercising, and sharing one's fitness app Profile is indeed a potential way to connect to other users. As such, it makes sense that users in this subprofile are more willing to share their fitness app Profile if the risks of doing so decrease.

The classification accuracy of the negotiability questions is the highest among all "indirect prediction" approaches. The most predictive questions also have understandable semantic relationships with the datasets they predict.

6.5.2.4 Exercise Tendencies and User Demographics

We applied J48 learning algorithms to the group of exercise tendency questions and user demographics as well, but we found no significant predictors among these questions. While other studies have found user demographics to be significant predictors of privacy behaviors [64], in this particular study we were not able to find any significant predictors among the group of user demographics.

6.5.3 Tree Evaluation

Figure 6.11 shows the root mean square error of all the trees produced by the J48 classifier. The evaluation has been executed with k-fold cross validation with $k = 10$.

As expected, the "direct prediction" approach results in lower error rates than the various

"indirect prediction" approaches, since in the former approach the items are a direct part of the privacy settings that constitute the subprofiles. Among the "indirect prediction" approaches, the *negotiability of privacy settings* has slightly lower error rates. This is not surprising, since it is at least partially related to the privacy settings (yet evaluates whether those settings will change under certain conditions). The prediction accuracies of each tree are reported on the branches in their respective figures (Figure 6.7 to 6.10), and take the form of (# assigned / # incorrect).

6.6 Privacy-setting Recommendations (partial original work)

In this section, we describe different types of guided privacy-setting approaches for fitness Iot users that are based on the previous clustering and machine learning results.

6.6.1 Manual Setting

The baseline privacy settings interface is one where users have to manually set their settings (see Figure 6.12). If users do this correctly these manual settings should match their privacy preferences 100%. However, the process of manually setting one's privacy settings can be very burdensome for the user; our system has a total of 45 permissions that are required to be managed. Under such burden, users are likely going to make mistakes [82], so the 100% accuracy may not be achieved through manual settings.

The next strategies exploit the results of the analysis in the previous section to provide *interactive recommendations* that simplify the task of privacy permission setting, with different levels and type of user intervention.

6.6.2 Single Smart Default Setting

One way to reduce the burden of privacy management is with single "smart" default setting. Rather than having the user set each permission manually, this solution already selects a default setting for each permission. Users can then review these settings and change only the ones that do not match their preferences.

The optimal "smart" default is a set of settings that is aligned with the preferences of the majority of users. Hence, we can calculate these setting by using the cluster centroid of the 1-cluster solution (i.e., the full dataset "single cluster" in Figure 6.6). Figure 6.13 shows the resulting default

values for each dataset. If the user is unhappy with these settings, he/she can still make specific changes. Otherwise, he/she can keep them without making any changes.

6.6.3 Pick Subprofiles

The single smart default setting works best when most users have preferences similar to the average. However, our dataset shows considerable variability in participants' privacy preferences—a finding that is broadly reflected in the privacy literature [65]. This bring us to our clustering solutions, which create *separate* default settings (in the form of subprofiles) for distinct groups of users.

Our first approach in this regard is to have users manually select which privacy subprofiles they prefer. Figure 6.14 shows the subprofile selection interface for the S set. Users can choose either the "Minimal" or "Unconcerned" subprofile. Similar interfaces are provided for the F, A, and G sets.

The subprofiles provided by this approach have a higher overall accuracy than the single "smart" default described in Section 6.6.1, meaning that the user could possibly spend less effort changing the settings. However, the user *will* have to select a subprofile for each dataset. This highlights the importance of having a small number of subprofiles and making these subprofiles easy to understand. That said, even with only two subprofiles per dataset, this can be a challenging task. In the next two subsections, we address this problem by automatically selecting subprofiles based on users' answers to specific subprofile items ("direct prediction") or questionnaire items ("indirect prediction").

6.6.4 Direct Prediction

For the direct prediction approach, we devise an interactive 4-question input sequence as shown in Figure 6.15. Each screen asks the user to answer a specific permission question, which guides the subprofile classification processes as outlined in Section 6.5.1. In effect, each question informs the system about the user's subprofile of one of the four datasets, which means that users no longer have to manually pick the correct subprofiles. Specifically, users will be asked if they agree to share their First name (for the A set recommendation), Activity (for the F set), Photos (for the S set), and whether they allow their data to be used for Social purposes (for the G set). This

4-question interaction will aid the users in setting all of the 45 permissions in the system. Depending on the answer to these questions, the user will subsequently see the settings screens with the defaults set to the predicted profile. Users can still change specific settings if their preferences deviate from the selected profile.

6.6.5 Indirect Prediction

For the indirect prediction approach, we take a similar approach, but the interactive 4-question input sequence is based on the analysis of questionnaire items rather than permission settings.

As shown in Figure 6.16, we selected 4 questions that yield the highest accuracy for each permission set: a negotiability question for Phone permissions for the S set, a negotiability question for the permission to share Sleep data for the F set, A question about sociability for the A set, and a trust question for the G set. Negotiability and attitude have almost the same accuracy for G set, so we chose attitude for diversity.

The benefit of the indirect prediction approach is that the user does not have to answer any permission questions, not even the four needed to give a subprofile recommendation. Instead, the user has to answer four questionnaire items.

6.7 Validation

We conducted a validation of these different approaches by running the recommendation strategies on the 30 users in our holdout dataset. The resulting recommended privacy subprofiles are then compared with their actual privacy preference. Figure 6.17 shows the average accuracies of each of the presented approaches.

The *Pick Profile* approach reaches an 84.74% accuracy. This approach has the highest accuracy, because only the error from the difference between the privacy profile and the users' settings is counted, omitting the errors introduced by the user classification. This assumes that users can classify themselves with perfect accuracy—this is likely an incorrect assumption.

Among recommendation approaches, the *direct prediction* approach is the most accurate, averaging 83.41%. It almost yields no additional classification error compared to the *Pick subprofile* approach. The *indirect prediction* approach has a significantly lower accuracy of 73.9%.

Finally, the *single smart default* approach uses only a single "profile", circumventing the need for classification. The default profile settings are shown in the 'full data' column of Figure 6.6. The accuracy of this setting is lower than the accuracy of the subprofile solutions, but it does not lose accuracy on classification. Hence, its accuracy is a respectable 68.7%, which is not much lower than the *indirect prediction* approach.

The details about accuracies are provided in Table A1 in Appendix.

6.8 Summary

In this chapter, we have presented the following:

- The dataset we used and Data modeling to fitness IoT permissions.
- Using a data-driven approach to developing user permission profiles
- A series of recommendation strategies that we developed for privacy management including direct prediction and more interestingly, indirect prediction using some user traits (users' privacy attitudes, the negotiability of their preferences, and social influence).

One limitation of this work is that we have not tested the suitability of the recommendation strategies from the user's perspective. Specifically, we have conjectured that profile-based approaches reduce the hassle of making privacy settings but that the manual selection of a privacy profile might be difficult for a user. These conjectures should be evaluated in a user study, which we are currently working on.

In the next chapter, we discuss the evaluation study for our household IoT privacy-setting interface prototype.

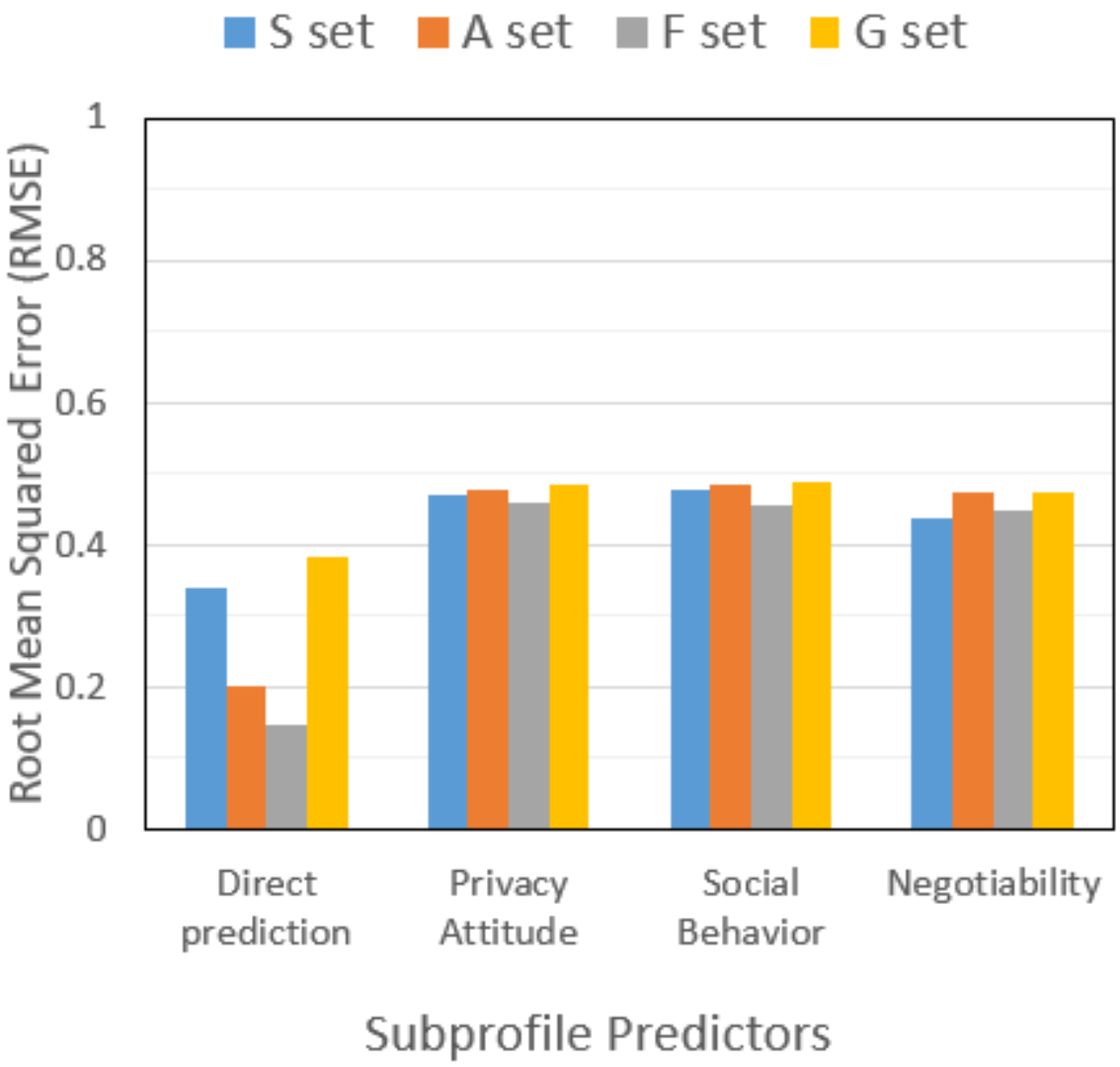
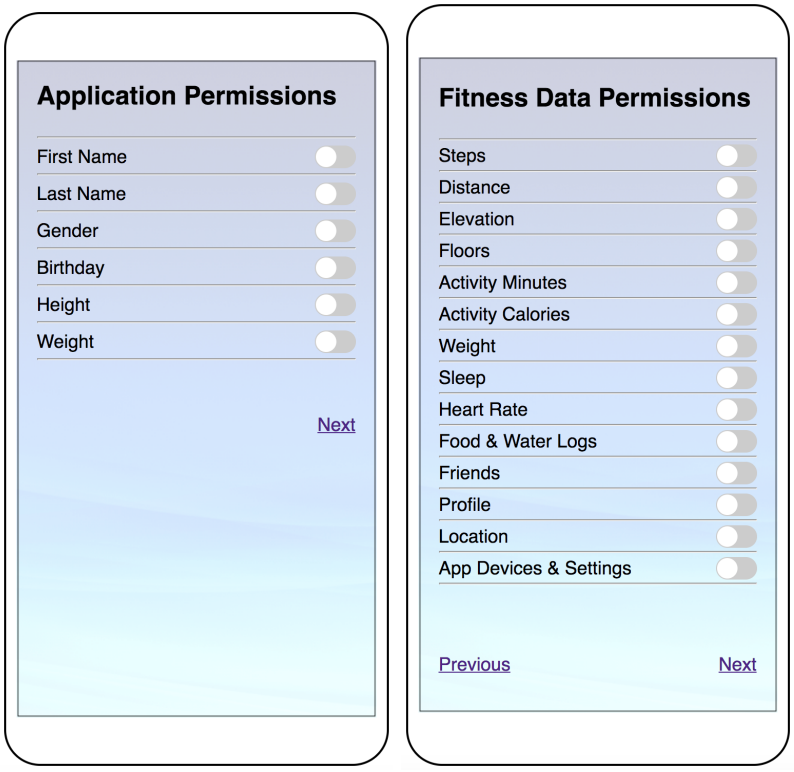


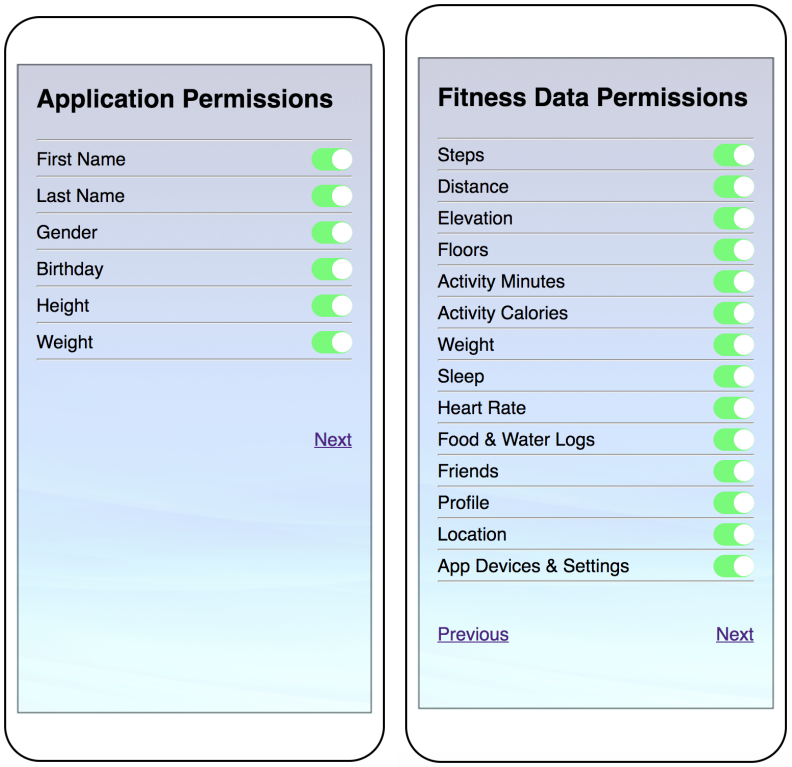
Figure 6.11: Tree evaluation. Root mean square error for each J48 tree algorithm.



(a) A set (b) F set

(c) S set (d) G set

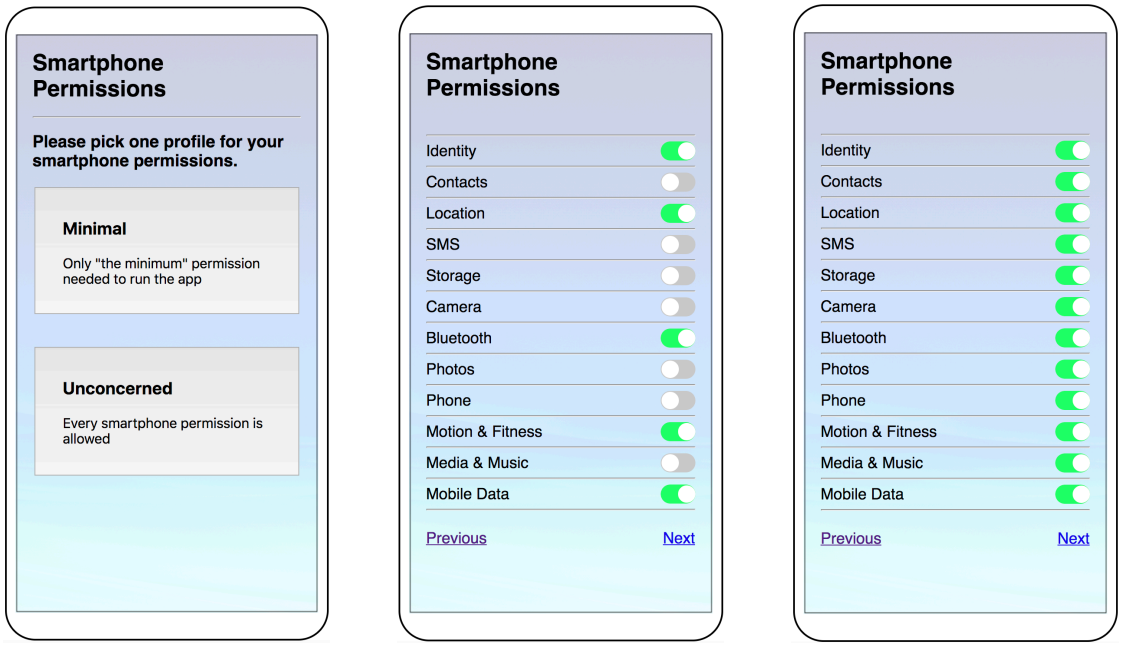
Figure 6.12: Manual settings



(a) A set (b) F set

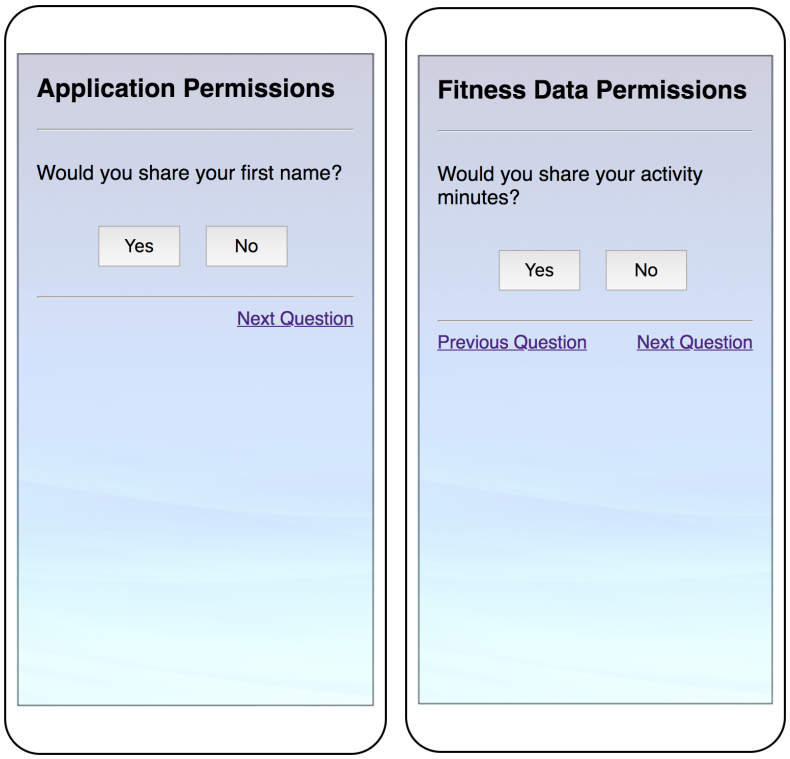
(c) S set (d) G set

Figure 6.13: Smart Single settings.



(a) S set subprofiles (b) The "Minimal" subprofile (c) The "Unconcerned" subprofile

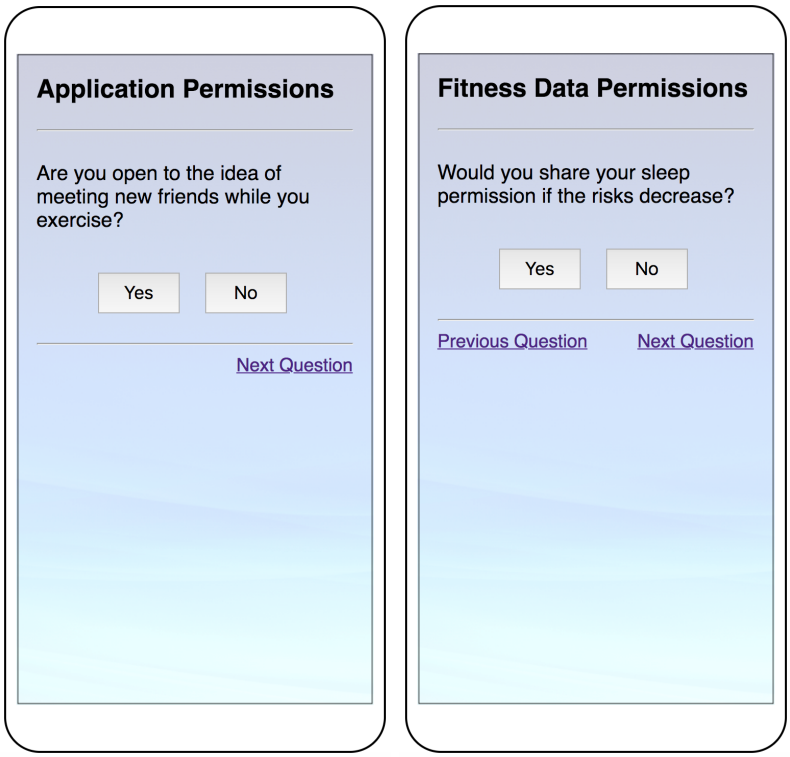
Figure 6.14: Interaction for picking a subprofile for the S set.



(a) A set (b) F set

(c) S set (d) G set

Figure 6.15: Direct Prediction questions.



(a) A set (b) F set

(c) S set (d) G set

Figure 6.16: Indirect Prediction questions.

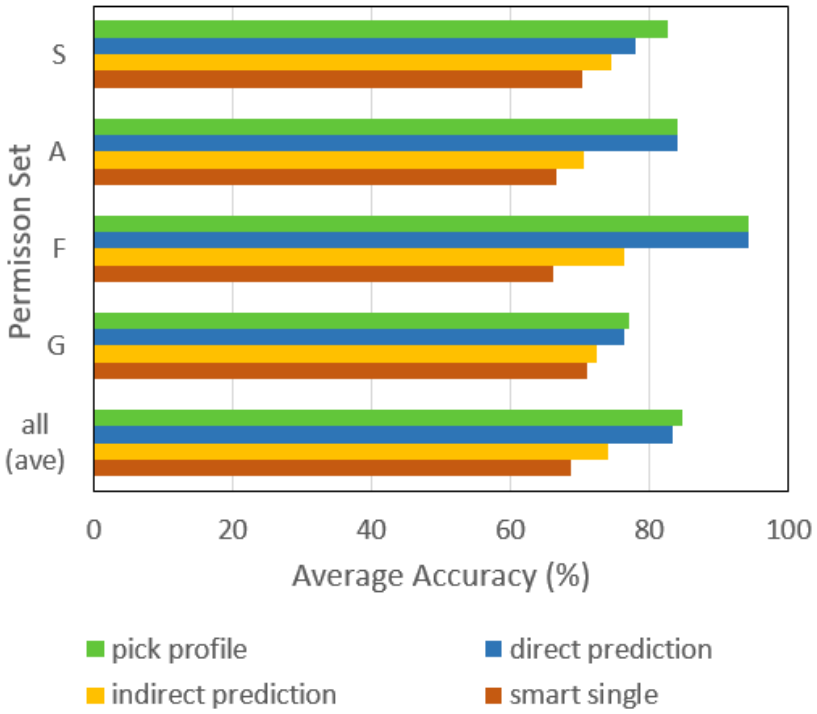


Figure 6.17: Average accuracies of the recommender strategies on the holdout 30 users.

Chapter 7

Evaluate the Household IoT Privacy-setting Profiles and User Interfaces

7.1 Introduction

In the previous chapters, we have described the three studies on recommending privacy settings for general/public IoT, household IoT, and fitness IoT, respectively. A "data-driven" approach has been used in all three studies, to gain the underlying insights of IoT users' privacy decision behavior, and to design a set of User interfaces (UI) to incorporate the "smart" privacy default/profiles created based on the insights. Users can apply these smart defaults/profiles by either a single click or by answering a few related questions. When applying this approach on the household IoT dataset in Chapter 5, we explored the trade-off between parsimony and accuracy when creating the "smart" privacy defaults/profiles. We manipulate the pruning parameter for the decision trees of the C4.5 algorithm, which impacted the complexity of the generated profiles based on the decision trees. Accuracy is important to ensure that users' privacy preferences are accurately captured and/or need only few manual adjustments, while parsimony, on the other hand, prevents overfitting and promotes fairness. In Chapter 5, we noticed that more complex models tended to increase overall accuracy by predicting a few users' preferences more accurately, with no effect on other users. Parsimony also

makes the associated default setting easier to understand for the user.

The biggest limitation of our work so far is that we did not test any of the proposed UIs, so we do not know what level of complexity (both in terms of the user interface and the in terms of the profiles) is most suitable. Thus, to further test this trade-off between accuracy and parsimony in a real usage environment and test the user experience of using the interfaces that we designed in Chapter 5, in this chapter, I address this limitation by discussing our final study on evaluating the new interface prototypes of recommending privacy-settings for household IoT. The main purpose of this study is to test the user experience of the privacy-setting profiles interfaces and defaults/profiles.

7.2 Study Design

In this chapter, we present the design our study, including the dependent variables and manipulations.

7.2.1 Dependent Variables

To test the user experience of our privacy-setting interfaces, the Dependent Variable of our study will be their **satisfaction to the system**, **and the trust to the company**, and several subjective system aspects, including **perceived usefulness**, **perceived ease of use**, **perceived privacy threats**, **perceived control**, **perceived privacy helpfulness**. As shown in Table 7.1, all the scales of these dependent variable are adapted from previous work.

7.2.2 Manipulations

7.2.2.1 Interface complexity

In Chapter 5, we first designed a set of interfaces, as shown in Figure 5.6, based on the results from our statistical analysis (**UI1**). Further, we modified these interfaces to integrate the "smart defaults/profiles" generated from our machine learning results. This modification separated the Storage and sharing modules from the Data usage, leading a slightly more complex interface design (**UI2**). For our study, we need to test these two groups of interfaces (UI1 vs UI2) in terms of interface complexity. Compared to UI1, UI2 has more granularity when setting on different storage. In UI1, users can only configure all the privacy-settings to be the same for the three different types

of storage (Local, Remote, and Third-party sharing), while they can configure those setting for each type of storage differently in UI2.

7.2.2.2 Profile complexity

In terms of the complexity of "smart defaults/profiles", we consider 4 different experimental conditions as follows:

- **Everything-On**: With all the data access and usage being turned on, this is considered as the open default settings. This profile also means nothing has been done for the users. They have to make every change for themselves.
- **Everything-Off**: With all the data access and usage being turned off, this is considered as the most conservative default settings. In our previous studies, this is also the profile that more than 50% participants want to use.
- **Smart Default**: One single "smart profile" will be provided to the users. This is considered as the experimental condition with intermediate complexity.
- **Smart Profiles**: Multiple "smart profiles" will be provided to the users. This is considered as the most sophisticated settings with high complexity in "smart profiles".

These different default/profile conditions map to users' "preference fit", where smart profiles and smart defaults conditions have better "preference fit" than the two baseline conditions. In addition, smart profiles condition have more preference options for users to choose than smart default. Thus, we expect smart profile to have the best fit/user satisfaction or other subject system aspects, followed by smart defaults and the two baseline conditions.

From above, we have 2 different levels of interface complexity, and 4 different levels of profile complexity. Hence, 4x2 = 8 total experimental conditions (i.e., user interfaces) will be presented to the participants.

7.2.2.3 Profile/Interface Selection

Everything-Off and **Everything On** profiles can easily be implemented on both our designed interfaces (UI1 and UI2).

For **Smart Default** and **Smart Profiles** selection, note that, when applying our machine learning algorithms in Chapter 5, we have manipulated the pruning parameter to create different "smart defaults/profiles". This manipulation results in a set of smart profiles with different weight in accuracy and parsimony. The more the decision tree is pruned, the less complex the resulting "smart" profile will be, leading lower accuracy and high parsimony, and vice versa. Since we can only choose one "smart default/profile" to test the interface, this selection needs to be done carefully.

Smart Default: In section 5.5.2, we have applied a one-rule algorithm to our dataset. The resulting "smart default" in shown in Figure 5.7. This is the simplest "smart default" settings across all the different "smart defaults" settings with lowest accuracy (61.39%) but highest parsimony. In addition, this "smart default" can be easily integrate into both the **UI1** and **UI2**. Thus, we choose this "smart default" as the target interface for experimental conditions **UI1:Smart Default** and **UI2:Smart Default**.

Smart Profiles: For "smart profiles" selection, we want this interface differ as much as possible comparing the "smart default", so we search across all the "smart profiles" with large number of clusters. In addition, the "smart profiles" should be easily integrated into UI1 or UI2. Figure 5.18 is considered for UI1 because it has 5 clusters with a high accuracy of 80.35%. And it has no interaction between **Storage** and other parameters. This is suitable for our UI1 design, serving as the target interface profiles for experimental condition — **UI1:Smart Profiles**. We have separated the Data Storage and Data Usage modules in UI2. Thus, we choose Figure 5.25 for UI2 because it has 5 clusters, a close to highest accuracy of 83.11%. In addition, in the cluster 3, it has a 2-way interaction between **Storage** and **Purpose**; in cluster 4, it has a 2-way interaction between **Storage** and **Action**. It does not have an 3-way interaction between any of these parameters in any of its clusters. Thus, we choose this set of "smart profiles" as the target interface profiles for experimental condition — **UI2:Smart Profiles**. We implemented above 8 different sets of user interfaces using HTML, PHP, CSS, and SQL.

7.2.3 Research Questions

Compared to UI1, UI2 has more granularity when setting on different storage. In UI1, users can only configure all the privacy-settings to be the same for the three different types of storage (Local, Remote, and Third-party sharing), while they can configure those setting for each type of storage differently in UI2. Brandimarte et al. demonstrate that users perceive more control

when privacy controls are more granular [15]. But this control can at times be an illusion. More granular controls allow users to set their privacy settings to a level that better reflects their privacy preferences, this additional control may increase the perceived usefulness [109, 4]. Similarly, more fine-grained control may reduce users' perceived privacy threats. Tang et al. (2012) found that users of a finer-grained settings interface were more comfortable with their privacy settings. Research has also shown that increasing the control often introduces choice overload issues [54, 103, 2, 3], which makes it more difficult and time-consuming for users to accurately their privacy settings [82, 101].

Therefore, here are our first research question:

RQ 1a *Is there any significant difference between UI1 and UI2 on users experience and other subjective system aspects when using our system?*

In term of profile complexity, we have four different levels of experimental conditions. These different default/profile conditions map to users' "preference fit". "Smart profiles" provide the users more pre-configured options for users to choose from, leading to a better preference fit than the "smart default" with only single "smart" option provided, which in turn has a better fit than Everything-Off/Everything-On defaults. This additional freedom of choice and possible increased preference fit may increase the perceived control and perceived usefulness. Similarly, the increased preference fit may increase the level that the pre-configured profiles better reflect the users' privacy preferences, which may reduce the perceived privacy threats. The additional options in "smart profiles" may introduce choice overload compared to the "smart default" and Everything-Off and Everything-On defaults. This may lead to a low perceived ease of use for "smart profiles". Compared to Everything-Off and Everything-On defaults, "smart defaults" are generated from machine learning analysis results. The higher accuracy of "smart defaults" can arguably result in fewer a lower manual changes that users would make to the system, leading to a higher perceived ease of use compared to Everything-Off and Everything-On defaults. Therefore, Here is our second research question:

RQ 2a *Is there any significant difference between the 4 experimental conditions on users experience and other subjective system aspects when using our system?*

7.3 Experimental setup

In this section, we discuss the Experimental setup of our user study. This user study will be a between-subject study, which takes about 15 – 20 minutes to finish. All participants will be recruited via Amazon Mechanical Turk.

7.3.1 Participants and Procedures

Based on the power analysis results, to collect our dataset, 504 adult U.S.-based participants were recruited through Amazon Mechanical Turk. Participation was restricted to Mechanical Turk workers with a high reputation (at least 50 completed tasks, average accuracy of $> 96\%$). Participants were paid \$1.50 upon successful completion of the study. The participants were warned about not getting paid in case they failed attention checks (see below). The study participants represented a wide range of ages, with 44 aged 18-24, 298 aged 25-34, 116 aged 35-44, 29 aged 45-54, 12 aged 55-64, and 5 participants over 65 years old.

During the study [1], the participants were first welcomed with a brief introduction of the experimental instructions. We explicitly introduce that the goal of this study is to test a new setting interfaces for Smart Home Users.

Then each participant was shown a video with a brief introduction to various smart home devices, which also mentioned various ways in which the different appliances would cooperate and communicate within a home. After the video, participants were asked to answer two attention check questions depicted in Figure A1 in the Appendix.

After the introduction video, each participant was shown the basics of our UI and usage instructions, shown in Figure A2 in the Appendix. Then each participant was presented with one privacy-setting user interface for household IoT that was randomly choosen from the previous lydiscussed 8 different experimental conditions. Participants were asked to set all the privacy-settings to best fit their own privacy preferences. They were required to spend at least 25 seconds before they can leave the UI page and will be warned if they spent too little time on the UI page.

Finally, a post-test survey questionnaire was shown to each participant, asking their user experience using our privacy-setting interfaces. The questionnaire included three groups of questions – *experience* (i.e. satisfaction with the system); *Subjective System Aspects* (SSA), including

[1] The user study url can be found here: http://iot.usabart.nl/yang

Perceived usefulness, Perceived ease of use, perceived privacy threats, perceived control); and *personal/situational characteristics* (General privacy concerns, Data Collection Concerns, Knowledge, Rational Decision Style, and Emotional Decision Style). All items were adapted from previous published studies with minor modifications in wording to accommodate the IoT privacy-setting context. Each item was measured on five-point Likert scales with 1 being "strongly disagree" to 7 being "strongly agree". All the items of the questionnaire are shown in Appendix.

7.4 Results

In this section, I present the statistical analysis results. I first discuss the confirmatory factor analysis that I conducted to clean up the survey question items. Then I discuss the structural equation model (SEM) that I used to analyze the effect of the independent variables on the subjective systems aspects and user experience. And finally, I present the effect of personal/situational characteristics on the subjective systems aspects and user experience.

7.4.1 Confirmatory Factor Analysis

I conducted a Confirmatory Factor Analysis (CFA) and examined the validity and reliability scores of the constructs measured in the study. I started with the saturated model, as shown in Figure 7.1. Upon inspection of the CFA model, I removed items that have lowest R-square value since this means that this item explains the least percentage of the scale.

During this process, th6 (low communality 0.121), e2 (low communality 0.221), e7 (low communality 0.237), th5 (low communality 0.222), s8 (low communality 0.233), th2 (low communality 0.278), u4 (low communality 0.291), e4 (low communality 0.330), e5 (low communality 0.341), e9 (low communality 0.311), tr2 (low communality 0.365), tr4 (low communality 0.353) tr8 (low communality 0.209), tr3 (low communality 0.295), tr1 (low communality 0.246), s4 (low communality 0.317), s3 (low communality 0.274), s6 (low communality 0.298), e1 (low communality 0.308), e10 (low communality 0.184), u2 (low communality 0.368), u7 (low communality 0.346), s5 (low communality 0.383), s7 (low communality 0.327) were removed. Interestingly, after removing e10, I removed h4 (communality 0.612) instead of h2 (low communality 0.227), because if h2 was removed, both h1 and h3 need to be removed, leaving only one item in that scale. While if h4 was removed, h1, h2, and h3 can all be kept in the model.

```
model <- "satisf=~s1+s2+s3+s4+s5+s6+s7+s8+s9+s10
      usef=~u1+u2+u3+u4+u5+u6+u7
      ease=~e1+e2+e3+e4+e5+e6+e7+e8+e9+e10
      helpf=~h1+h2+h3+h4
      threat=~th1+th2+th3+th4+th5+th6+th7
      control=~c1+c2+c3+c4
      trust=~tr1+tr2+tr3+tr4+tr5+tr6+tr7+tr8"
```

Figure 7.1: CFA Saturated Model.

```
model <- "satisf=~s1+s2+s9+s10
      usef=~u1+u3+u5+u6
      ease=~e3+e6+e8
      helpf=~h1+h2+h3
      threat=~th1+th3+th4+th7
      control=~c1+c2+c3+c4
      trust=~tr5+tr6+tr7"
```

Figure 7.2: Trimmed CFA Model.

And at the end, I also checked that no item has high cross-loadings with other factors. The remaining scale items with their R-square value of the trimmed model are shown in Table 7.1. The final trimmed model is shown in Figure 7.2.

Also, to ensure the convergent validity of constructs, I examined the average variance extracted (AVE) of each construct. The AVEs were all higher than the recommended value of 0.50, indicating adequate convergent validity. To ensure discriminant validity, we ascertained that the square root of the AVE for each construct was higher than the correlations of the construct with other constructs. As shown in Figure 7.3[2], trust, satisfaction, perceived privacy threat, perceived ease of use, and perceived control all have high correlation with each other (at least 0.746). Out of them, perceived privacy threat and perceived ease of use have the lowest AVE but with the highest correlation with other constructs. And if these two constructs are removed from the model, the square root of the AVE for other construct will be higher than their correlations with the left constructs, which indicates the discriminant validity. Thus, we removed perceived privacy threat and perceive ease of use from the final model. The model has a following model fit:

[2]on the diagonal is the sqrt(AVE)

Table 7.1: Factor Items in Trimmed CFA Model[1]

Construct	Item	Loading
System satisfaction [53, 137, 136]	The system has no real benefit to me.	0.584
	Using the system is annoying.	0.700
	Using the system is a pleasant experience.	
	Using the system makes me happy.	
	Overall, I am satisfied with the system.	
	I would recommend the system to others.	
	I would use this system if it were available.	
	I would pay a monthly fee to use this system.	
	I would quickly abandon using this system.	0.755
	It would take a lot of convincing for me to use this system.	0.709
Trust [55, 84]	I believe the company providing this software is trustworthy in handling my information.	
	I believe this company tells the truth and fulfills promises related to the information I provide.	
	I believe this company is predictable and consistent regarding the usage of my information.	
	I believe this company is honest when it comes to using the information I provide.	
	I think it is risky to give my information to this company.	0.634
	There is too much uncertainty associated with giving my information to this company.	0.750
	Providing this company my information would involve many unexpected problems.	0.709
	I feel safe giving my information to this company.	
Perceived Usefulness [25]	Based on what I have seen, the system is useful.	0.741
	The system helps me more effectively set my privacy preferences.	
	The system gives me more control over my Smart home devices.	0.483
	The privacy setting task would be easier to finish with the help of this system.	
	The system saves me time when I use it.	0.527
	The system meets my needs.	0.580
	The system does everything that I expect it to do.	
Perceived Ease of Use [25, 66]	It is convenient to set my preferences in the system.	
	It requires the fewest mouse-clicks possible to set my privacy preferences with the system.	
	It takes too many mouse-clicks to set my privacy preferences with the system.	0.500
	I was able to quickly set my privacy-setting preferences in the system.	
	I feel setting my privacy preferences within the system is easy.	
	I feel setting my preferences in the system was unnecessarily complex.	0.676
	I can set my privacy-setting preferences without written instructions.	
	I felt lost using the system's privacy settings.	0.774
	I felt this privacy-setting interface is designed for all levels of users.	
	I can use the Privacy-setting interface successfully every time.	
Perceived privacy Helpfulness [124]	The system helped me to decide what information I should disclose.	0.626
	The system explained how useful providing each piece of information was.	0.561
	The system helped me to make a tradeoff between privacy and usefulness.	0.629
	I felt clueless about what information to disclose.	
Perceived Privacy Threat [66]	I am afraid that I am sharing my personal information too freely, due to my privacy settings.	0.602
	I am comfortable with amount of data that is used/shared based on my settings.	
	Due to the system, the manufacturer will know too much about me.	0.557
	Due to the system, third-parties will know too much about me.	0.612
	I made sure only information that I am comfortable with will be used or shared.	
	My privacy settings are spot on; I am not disclosing too much to anyone.	
	I fear that I have been too liberal in selecting my privacy settings.	0.668
Perceived Control [138]	I had limited control over the way this system made privacy settings.	0.630
	The system restricted me in my choice of settings.	0.809
	Compared to how I normally configure privacy settings, the system was very limited.	0.731
	I would like to have more control over the recommendations.	0.500

[1] Grayed out items were removed during trimming

Satisfaction	0.829						
Usefulness	-0.583	0.763					
Trust	0.799	-0.391	0.835				
Ease of use	0.815	-0.370	0.830	0.806			
Helpfulness	-0.005	0.611	-0.042	0.079	0.778		
Threat	0.746	-0.302	0.879	0.850	0.057	0.780	
Control	0.785	-0.252	0.801	0.850	0.200	0.864	0.817
	Satisfaction	Usefulness	Trust	Ease of use	Helpfulness	Threat	Control

Figure 7.3: Factor Correlation Matrix (on the diagonal is the sqrt(AVE)).

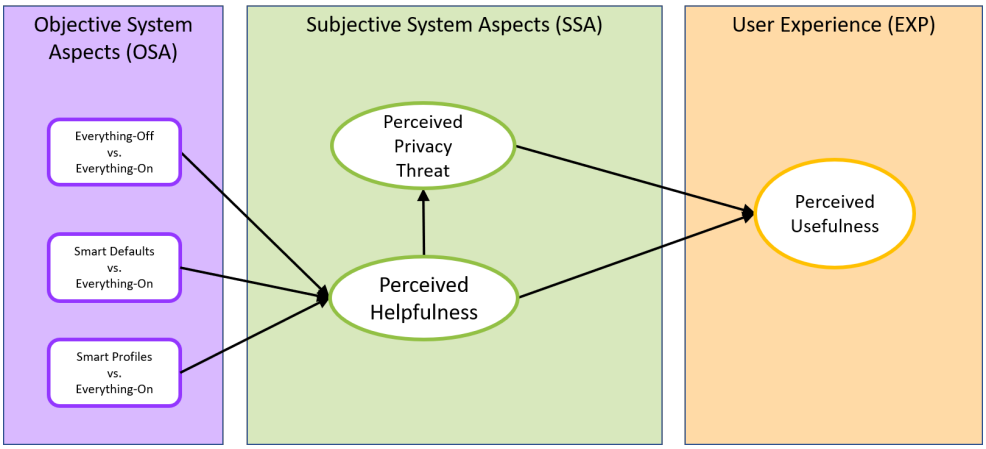


Figure 7.4: Preliminary SEM Model with perceived privacy threats

$\chi^2(125) = 298.507, p = .0000; RMSEA = 0.067, 90\%CI : [0.058, 0.077], CFI = 0.975, TLI = 0.970.$

7.4.2 Structural Equation Modeling

I tried many different SEM models. Figure 7.4 shows a model which contains perceived privacy threat, perceived helpfulness, and perceived usefulness. This model has a good model fit. However, the user experience variables — satisfaction and trust are both removed from the model due to the high covariance between them and perceived privacy threat. Thus, this model was not chosen.

As shown in Figure 7.5, I also tried another model with hypothesizing that there will be

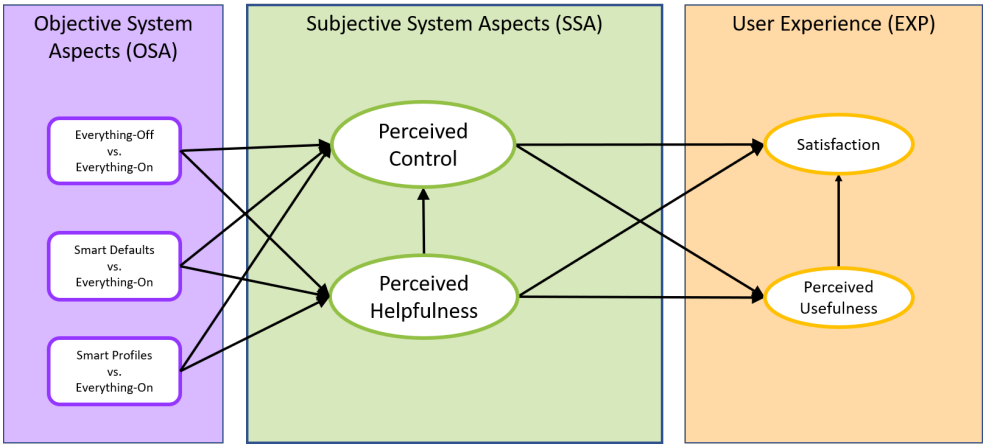


Figure 7.5: Preliminary SEM Model with effect from manipulations to perceived control

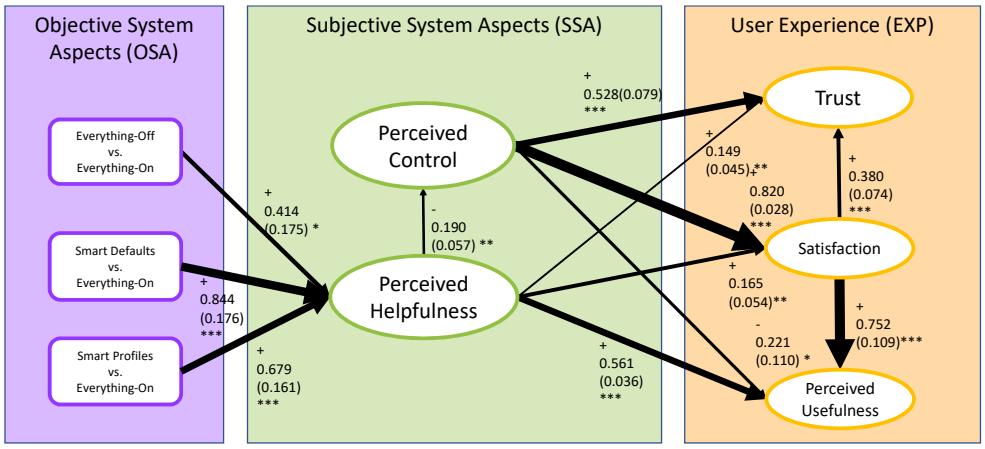


Figure 7.6: Trimmed structural equation model. $*p < .05, **p < .01, ***p < .001$.

significant effect from objective system aspects (experimental conditions/manipulations) to perceived control since. Compared to the previous preliminary model, this model kept satisfaction and perceived usefulness. Both of these factors are mediated by the perceived control and perceived helpfulness. However, no significant effect from the manipulations to the perceived control was found.

Finally, as shown in Figure 7.6, we subjected the remaining 5 factors (Trust, Satisfaction, Perceived Usefulness, Perceived Control, and Perceived Helpfulness) and the experimental conditions to structural equation modeling, which simultaneously fits the factor measurement model and the structural relations between factors and other variables. The model has following model fit: $\chi^2(176) = 284.160, p = .0000; RMSEA = 0.045, 90\%CI : [0.035, 0.054], CFI = 0.986, TLI = 0.983$.

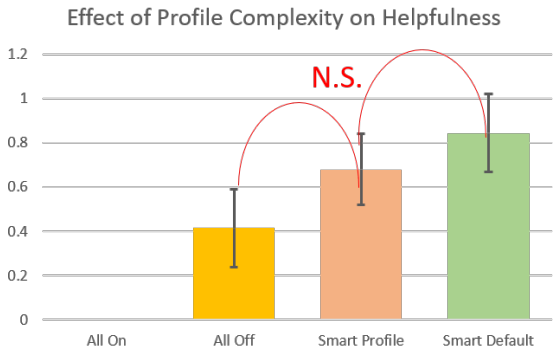


Figure 7.7: Effects of profile complexity on perceived helpfulness

The model answers the two first two research questions — smart defaults/profiles manipulation has a significant effect on the helpfulness of the system: Participants in Everything-Off, Smart Defaults, and Smart Profiles conditions perceived more helpfulness than the Everything-On condition. The two different UIs, however, do not have a significant effect on anything.

Figure 7.7 shows the effect of profile complexity on perceived helpfulness. Both Everything-On and Everything-Off have been used as the baseline to test the significance of the effect. The results shows that only the difference between pair (Everything-off – smart profiles) and pair (smart profiles — smart defaults) are not significant. The effect between all other manipulations are significant.

The helpfulness is in turn related to users' perceived control. Here we see that perceived helpfulness has a negative effect on users' perceived control. This indicates an interesting debate between perceived control and perceived helpfulness from the users. More details about this debate will be discussed in the next section. Figure 7.8 shows the total effects of profile complexity on perceived control. All the effects are significant, which indicates that the effect of profile complexity on perceived control is mediated by perceived helpfulness.

Both the perceived control and perceived helpfulness have a positive significant effect on users' satisfaction with the system. Figure 7.8 shows the total effects of profile complexity on satisfaction. No significant effect was found. This, in the other hand, also proofs that the debating between perceived control and perceived helpfulness are canceling the effect from the manipulations on satisfaction.

Perceived control, Perceived helpfulness, and the satisfaction all have significant positive effects on users' trust in the company. Figure 7.8 shows the total effects of profile complexity on trust. No significant effect was found. Thus, the effect from the manipulations on trust were also

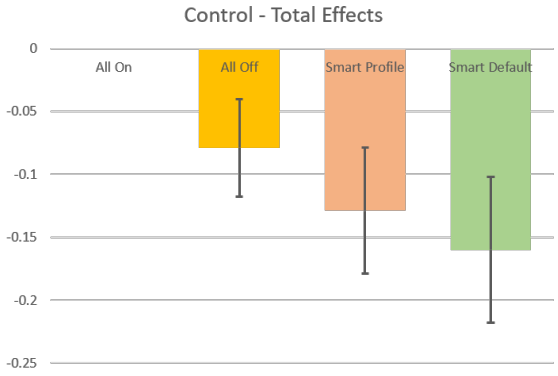


Figure 7.8: Total Effects of profile complexity on perceived control

Figure 7.9: Total Effects of profile complexity on satisfaction

being canceled by the debating between perceived control and perceived helpfulness.

Perceived control, Perceived helpfulness, and the satisfaction all determine perceived usefulness. Both satisfaction and perceived helpfulness have a positive significant effect on perceived usefulness. Perceived control has a negative significant effect on perceived usefulness. Less perceived control indicates there were more perceived helpfulness. And more perceived helpfulness could lead to more perceived usefulness. Figure 7.8 shows the total effects of profile complexity on perceived usefulness. All the effects are significant. This may be due to the effect from perceived helpfulness on perceived usefulness is strong and the effect from perceived control is weak. Also, the covariance between perceived helpfulness and perceived usefulness is

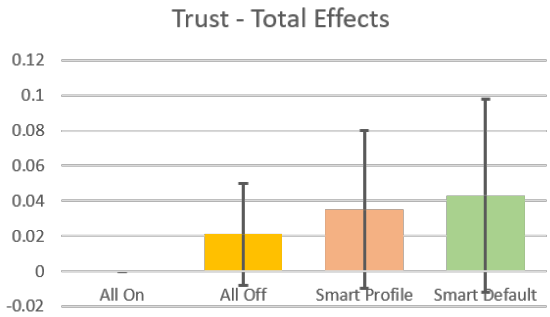


Figure 7.10: Total Effects of profile complexity on trust

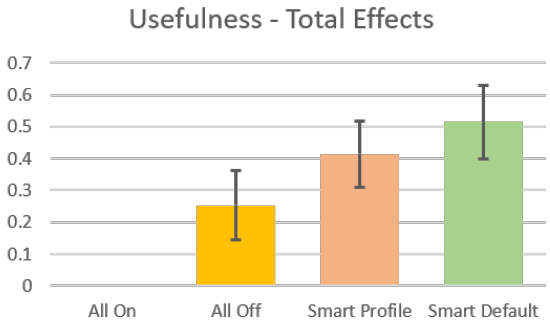


Figure 7.11: Total Effects of profile complexity on usefulness

7.5 Discussion

In this chapter we conducted a systematic evaluation of the effect of several design parameters of a household IoT privacy settings interface on users' evaluation of the system. In terms of managerial implications, we find that it is useful to utilize the data-driven approach to develop "smart defaults" and "smart profiles", and corresponding setting interfaces to improve users' experience and satisfaction. We did not find significant difference between the two UIs. A possible explanation for this is that design differences between the UIs were very subtle.

Regarding the negative effect from perceived helpfulness on perceived control, there are a few possible explanations: i) It is possible that participants in "smart defaults" and "smart profiles" condition found their privacy-settings have already been set by defaults. Thus, they found those "smart defaults" and "smart profiles" generated from previous study are helpful. However, in the other hand, users may feel that their choice of settings have been limited due to these helpful pre-settings. ii) It is also possible that users feel as though the pre-set settings are helpful but also

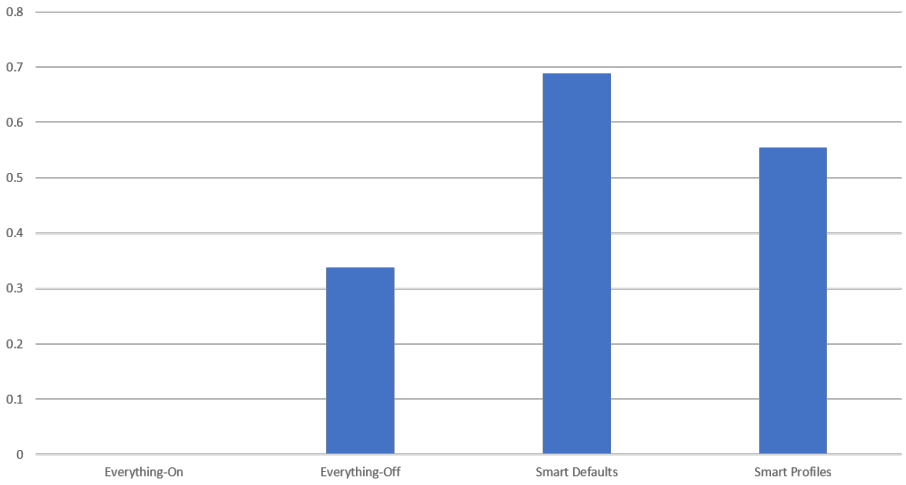


Figure 7.12: Effect size of average time spent on different UI pages

complicated. They feel they have less control over these settings. These are also corresponding to our previous discussion on the trade-off between accuracy and parsimony. A more parsimonious profile would be easier to explain to the users and also make them less worried about the pre-defined settings. So users are debating between the benefit brought by the "smart defaults" and "smart profiles" and the control they like to have over these privacy settings of their household IoT devices. iii) We also revisit the perceived scale that we used. It appear that all the items in that scale are reversed framed and related to the spirit of "losing control" and having limited control when using the system. One example is question C4, "I would like to have more control over the recommendations". Our system is all about make privacy setting recommendations. While we are making the right recommendation about the IoT privacy settings for users, they might still want more control and configure these settings by themselves, leading less control perceived.

Another interesting point is that the lack of difference between smart default and smart profiles in the effect on the user experience and subjective system aspects. We first investigated the time spent on the two conditions. Figure 7.12 shows the effect size of average time spent on different UI pages. Although the average time spent on smart defaults is higher than the smart profiles condition, the effect is not significant. So this could not be explained by the lack of interaction due to less time spent on the smart profiles than the smart defaults.

The finding is still interesting since users are expected to spend less time on smart profiles. And these lack of difference between smart defaults and smart profiles could be due to following

reasons:

i) **Laziness?** Since in our smart profiles conditions for both interfaces, there are detailed description about the profile being showed. Thus, users would know what the setting will be like for smart profile condition. Users would have to spend more cognitive effort to individually go ahead and change the smart default settings provided, which means one would have to spend more time and effort to get the settings to their preference. Here, people are not entirely confident whether the recommended defaults are matching their preferences and hence have to go in manually anyway to do so. Thus, this could lead more time spent on the smart defaults UI page and possible better user experience.

ii) **Accuracy?** The second possible reason could be that the accuracy of the smart profiles are better than the smart defauls that we used. The higher accuracy the pre-settings are, the more likely users would make less changes and leave the settings as is, leading less time spent on the smart profiles UI page.

ii) **Endowment effect?** Since the smart defaults are provided by the system, while in the smart profile condition, users have to choose their own profile by reading the description of the profile. So it is highly likely that they would try to stick to their choice as changing it now would call for expending additional cognitive effort and would rather avoid it. Thus, they might think the profile that they chose fits their preference the best and would not take a deeper look or give more careful review on the settings in that profile.

There are several limitations to our work. First of all, our sample is not large enough to carefully examine 2- or 3-way interaction effects in M-plus. We examined the effect of personal characteristics on the user experience individually, and did not find any significant effect. A larger sample is needed to test these effects and assure the robustness of our results. Second, we planned to examined the behavior data that how users make the changes to the pre-defined settings. However, due to the coding problem, we were not able to access data. This should be improved in the next user study since users' setting behavior could give us more hints to explain our previous findings.

From the results of this study, we encourage privacy researchers, policy-makers, and industry executives to consider the effects of privacy settings interfaces on privacy outcomes. This study shows that subtle changes in the design of such interfaces can have important subjective and behavioral consequences. Careful design of these systems can help users better setting their IoT devices.

Chapter 8

Conclusion

In this dissertation, we first present three studies on recommending privacy settings for different IoT environments, namely general/public IoT, household IoT, and fitness IoT, respectively. We developed and utilized a "data-driven" approach in these three studies—We first use statistical analysis and machine learning techniques on the collected user data to gain the underlying insights of IoT users' privacy decision behavior, and then create a set of "smart" privacy defaults/profiles based on these insights. Finally, we design a set of interfaces to incorporate these privacy default/profiles. Users can apply these smart defaults/profiles by either a single click or by answering a few related questions. To address the limitation of lacking evaluation to the designed interfaces, we conducted a user study to evaluate the new interfaces of recommending privacy-settings for household IoT users The results shows that by using smart defaults and smart profile can significantly improve users' experience, including satisfaction with the system, trust to the company. Our research can benefit the IoT users, manufacturers, and researchers, privacy-setting interface designers and anyone who wants to adopt IoT devices.

The main contribution of my dissertation are:

- User testing is often used to inform the development of user interfaces. Since the interface needs to be developed for the IoT system does not yet exists, we developed a data-driven approach to designing IoT privacy-setting interfaces for three different IoT environments, namely general IoT, household IoT, and fitness IoT.

- Prior research has shown that the decision-making of IoT users are heavily depending on the

contextual parameter of the IoT usage scenario. Thus, we investigated the effect of IoT scenario parameters on IoT users' decision and attitudes to find out which contextual parameter is more important in users' decision making process. And based on the importance of the different contextual parameters, we created a set of privacy-setting interfaces.

- Setting privacy-settings in these interfaces can still be complicated. To solve this problem, we used decision tree algorithm to create smart defaults and developed several clustering algorithm to group the users and created corresponding smart profiles for each group.
- During the process of creating smart defaults and smart profiles, we found that when the decision tree of the smart defaults/profiles become complex, this smart defaults/profiles will be difficult to explain to the users, leading bad decision making when choosing from provided options. We explored the trade-off between accuracy and parsimony when creating smart defaults/profile by manipulating the degree of pruning to the decision tree. We striked the balance between higher accuracy and better explainability of the smart defaults/profiles.
- In Fitness IoT domain, we also created a series of strategies to recommend "smart profiles" for users.
- Finally, we conducted a study to evaluate the designed interfaces in terms of interface complexity and profile complexity. The results show that smart defaults and smart profiles integrated in our privacy-setting interfaces have significantly improved users experience compared to the baseline condition.

This research can benefit the IoT users, manufacturers, and researchers, privacy-setting interface designers and anyone who wants to adopt IoT devices. I suggest the designers of future IoT privacy-setting interface to make use of our data-driven approach and carefully consider the trade-off between "smart defaults" and "smart profiles". "smart profiles" and "smart defaults" can be the viable route for designing future IoT privacy-setting interface. When designing their own setting interfaces and smart defaults/profiles, the effect of interface complexity and profile complexity should be carefully investigated based on their own user groups, dataset, and contexts.

Bibliography

[1] Alessandro Acquisti and Ralph Gross. Imagined communities: Awareness, information sharing, and privacy on the facebook. In *International workshop on privacy enhancing technologies*, pages 36–58, 2006.

[2] Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. *IEEE security & privacy*, 3(1):26–33, 2005.

[3] Alessandro Acquisti and Jens Grossklags. What can behavioral economics teach us about privacy. *Digital privacy: theory, technologies and practices*, 18:363–377, 2007.

[4] Adai Mohammad Al-Momani, Moamin A Mahmoud, and S Ahmad. Modeling the adoption of internet of things services: A conceptual framework. *International Journal of Applied Research*, 2(5):361–367, 2016.

[5] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 787–796. ACM, 2015.

[6] Denise Anthony, Tristan Henderson, and David Kotz. Privacy in location-aware computing environments. *IEEE Pervasive Computing*, (4):64–72, 2007.

[7] Kevin Ashton et al. That 'internet of things' thing. *RFID journal*, 22(7):97–114, 2009.

[8] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[9] Naveen Farag Awad and M. S. Krishnan. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly*, 30(1):13–28, March 2006.

[10] Paritosh Bahirat and Yangyang He. Exploring defaults and framing effects on privacy decision making in smarthomes. In *Proceedings of the SOUPS 2018 Workshop on the Human aspects of Smarthome Security and Privacy (WSSP)*, 2018.

[11] 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*, IUI '18, pages 165–176, Toyko, Japan, 2018. ACM.

[12] Hans H Bauer, Tina Reichardt, Stuart J Barnes, and Marcus M Neumann. Driving consumer acceptance of mobile marketing: A theoretical framework and empirical study. *Journal of electronic commerce research*, 6(3):181, 2005.

[13] Michael Benisch, Patrick Gage Kelley, Norman Sadeh, and Lorrie Faith Cranor. Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing*, 15(7):679–694, 2011.

[14] Alastair R Beresford, Andrew Rice, Nicholas Skehin, and Ripduman Sohan. Mockdroid: trading privacy for application functionality on smartphones. In *Proceedings of the 12th workshop on mobile computing systems and applications*, pages 49–54. ACM, 2011.

[15] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, 4(3):340–347, 2013.

[16] Ajay Brar and Judy Kay. *Privacy and security in ubiquitous personalized applications*. School of Information Technologies, University of Sydney, 2004.

[17] C Brodie, CM Karat, and J Karat. How personalization of an e-commerce website affects consumer trust. *Designing Personalized User Experience for eCommerce, Karat, J., Ed. Dordrecht, Netherlands: Kluwer Academic Publishers*, pages 185–206, 2004.

[18] Supriyo Chakraborty, Chenguang Shen, Kasturi Rangan Raghavan, Yasser Shoukry, Matt Millar, and Mani B Srivastava. ipshield: A framework for enforcing context-aware privacy. In *NSDI*, pages 143–156, 2014.

[19] Amir Chaudhry, Jon Crowcroft, Heidi Howard, Anil Madhavapeddy, Richard Mortier, Hamed Haddadi, and Derek McAuley. Personal data: thinking inside the box. In *Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives*, pages 29–32. Aarhus University Press, 2015.

[20] Ramnath K. Chellappa and Raymond G. Sin. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6(2-3):181–202, 2005.

[21] Shanzhi Chen, Hui Xu, Dake Liu, Bo Hu, and Hucheng Wang. A vision of iot: Applications, challenges, and opportunities with china perspective. *IEEE Internet of Things journal*, 1(4):349–359, 2014.

[22] 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.

[23] Mary J Culnan. " how did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS quarterly*, pages 341–363, 1993.

[24] Nigel Davies, Nina Taft, Mahadev Satyanarayanan, Sarah Clinch, and Brandon Amos. Privacy Mediators: Helping IoT Cross the Chasm. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*, HotMobile '16, pages 39–44, New York, NY, USA, 2016. ACM.

[25] Fred D Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pages 319–340, 1989.

[26] Fred D Davis, Richard P Bagozzi, and Paul R Warshaw. User acceptance of computer technology: a comparison of two theoretical models. *Management science*, 35(8):982–1003, 1989.

[27] 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.

[28] Julia Brande Earp, Annie I Antón, Lynda Aiman-Smith, and William H Stufflebeam. Examining internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, 52(2):227–237, 2005.

[29] Nathan Eddy. Gartner: 21 billion iot devices to invade by 2020. *InformationWeek, Nov*, 10, 2015.

[30] Serge Egelman, Janice Tsai, Lorrie Faith Cranor, and Alessandro Acquisti. 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*, pages 319–328. ACM, 2009.

[31] Opher Etzion and Fabiana Forunier. On the personalization of event-based systems. In *Proceedings of the 1st ACM International Workshop on Human Centered Event Understanding from Multimedia*, pages 45–48. ACM, 2014.

[32] 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.

[33] NK Fantana, Till Riedel, Jochen Schlick, Stefan Ferber, Jürgen Hupp, Stephen Miles, Florian Michahelles, and Stefan Svensson. Iot applications—value creation for industry. *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*, page 153, 2013.

[34] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security*, pages 1–14. ACM, 2012.

[35] Denis Feth, Andreas Maier, and Svenja Polst. A User-Centered Model for Usable Security and Privacy. In Theo Tryfonas, editor, *Human Aspects of Information Security, Privacy and Trust*, Lecture Notes in Computer Science, pages 74–89. Springer International Publishing, 2017.

[36] forbes. Iot: Don't forget privacy and security while racing to the price bottom, 2017. [Online; accessed 1-Feb-2019].

[37] Huiqing Fu, Yulong Yang, Nileema Shingte, Janne Lindqvist, and Marco Gruteser. A field study of run-time location access disclosures on android smartphones. *Proc. Usable Security (USEC)*, 14:10–pp, 2014.

[38] Steven Furnell. Managing privacy settings: lots of options, but beyond control? *Computer Fraud & Security*, 2015(4):8–13, 2015.

[39] Lingling Gao and Xuesong Bai. A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pacific Journal of Marketing and Logistics*, 26(2):211–231, 2014.

[40] David Gefen, Elena Karahanna, and Detmar W Straub. Trust and tam in online shopping: An integrated model. *MIS quarterly*, 27(1):51–90, 2003.

[41] Hemant Ghayvat, S.C. Mukhopadhyay, Jie Liu, Arun Babu, Md Alahi, and Xiang Gui. Internet of things for smart homes and buildings: Opportunities and challenges. *Australian Journal of Telecommunications and the Digital Economy*, 3:33–47, 12 2015.

[42] Susan E Gindin. Nobody reads your privacy policy or online contract: Lessons learned and questions raised by the ftc's action against sears. *Nw. J. Tech. & Intell. Prop.*, 8:1, 2009.

[43] 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.

[44] ACQUITY GROUP et al. The internet of things: The future of consumer adoption. *ACQUITY GROUP*, 2014.

[45] Dominique Guinard, Vlad Trifa, Friedemann Mattern, and Erik Wilde. From the internet of things to the web of things: Resource-oriented architecture and best practices. In *Architecting the Internet of things*, pages 97–129. Springer, 2011.

[46] Mark Hall, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, and Ian H Witten. The weka data mining software: an update. *ACM SIGKDD explorations newsletter*, 11(1):10–18, 2009.

[47] Moeen Hassanalieragh, Alex Page, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo Mateos, Burak Kantarci, and Silvana Andreescu. Health monitoring and management using internet-of-things (iot) sensing with cloud-based processing: Opportunities and challenges. In *2015 IEEE International Conference on Services Computing*, pages 285–292. IEEE, 2015.

[48] Yangyang He, Paritosh Bahirat, Abhilash Menon, and Bart P Knijnenburg. A data driven approach to designing for privacy in household iot. *Transactions on Interactive Intelligent Systems*, 2018.

[49] Alexander Henka, Lukas Smirek, and Gottfried Zimmermann. Personalizing smart environments. In *Proceedings of the 6th International Conference on the Internet of Things*, pages 159–160. ACM, 2016.

[50] Shuk Ying Ho and Kar Tam. Understanding the Impact of Web Personalization on User Information Processing and Decision Outcomes. *MIS Quarterly*, 30(4):865–890, December 2006.

[51] Robert C. Holte. Very simple classification rules perform well on most commonly used datasets. *Machine Learning*, 11(1):63–90, Apr 1993.

[52] Kai-Lung Hui, Bernard C. Y. Tan, and Chyan-Yee Goh. Online information disclosure: Motivators and measurements. *ACM Transactions on Internet Technology*, 6(4):415–441, November 2006.

[53] Kai-Lung Hui, Bernard CY Tan, and Chyan-Yee Goh. Online information disclosure: Motivators and measurements. *ACM Transactions on Internet Technology (TOIT)*, 6(4):415–441, 2006.

[54] Sheena S Iyengar and Mark R Lepper. When choice is demotivating: Can one desire too much of a good thing? *Journal of personality and social psychology*, 79(6):995, 2000.

[55] Sirkka L Jarvenpaa, Noam Tractinsky, and Lauri Saarinen. Consumer trust in an internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication*, 5(2):JCMC526, 1999.

[56] Prem Prakash Jayaraman, Xuechao Yang, Ali Yavari, Dimitrios Georgakopoulos, and Xun Yi. Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation. *Future Generation Computer Systems*, 76:540–549, November 2017.

[57] 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.

[58] Xiaolin Jia, Quanyuan Feng, Taihua Fan, and Quanshui Lei. Rfid technology and its applications in internet of things (iot). In *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on*, pages 1282–1285. IEEE, 2012.

[59] Patrick Kelley, Sunny Consolvo, Lorrie Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. A conundrum of permissions: installing applications on an android smartphone. *Financial cryptography and data security*, pages 68–79, 2012.

[60] Sean Dieter Tebje Kelly, Nagender Kumar Suryadevara, and Subhas Chandra Mukhopadhyay. Towards the implementation of iot for environmental condition monitoring in homes. *IEEE Sensors Journal*, 13(10):3846–3853, 2013.

[61] Bart P. Knijnenburg. *A user-tailored approach to privacy decision support.* Ph.D. Thesis, University of California, Irvine, Irvine, CA, 2015.

[62] Bart P Knijnenburg. Privacy? i can't even! making a case for user-tailored privacy. *IEEE Security & Privacy*, 15(4):62–67, 2017.

[63] Bart P. Knijnenburg. Privacy? I Can't Even! Making a Case for User-Tailored Privacy. *IEEE Security & Privacy*, 15(4):62–67, 2017.

[64] Bart P Knijnenburg and Alfred Kobsa. Helping users with information disclosure decisions: potential for adaptation. In *Proceedings of the 2013 international conference on Intelligent user interfaces*, pages 407–416. ACM, 2013.

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

[66] Bart Piet Knijnenburg and Alfred Kobsa. Increasing sharing tendency without reducing satisfaction: finding the best privacy-settings user interface for social networks. 2014.

[67] Alfred Kobsa, Ramnath K Chellappa, and Sarah Spiekermann. Privacy-enhanced personalization. In *CHI'06 extended abstracts on Human factors in computing systems*, pages 1631–1634. ACM, 2006.

[68] Alfred Kobsa, Hichang Cho, and Bart P. Knijnenburg. The Effect of Personalization Provider Characteristics on Privacy Attitudes and Behaviors: An Elaboration Likelihood Model Approach. *Journal of the Association for Information Science and Technology*, 67:2587–2606, February 2016.

[69] Trupti M Kodinariya and Prashant R Makwana. Review on determining number of cluster in k-means clustering. *International Journal*, 1(6):90–95, 2013.

[70] Robert S Laufer and Maxine Wolfe. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues*, 33(3):22–42, 1977.

[71] Mihai T Lazarescu. Design of a wsn platform for long-term environmental monitoring for iot applications. *IEEE Journal on emerging and selected topics in circuits and systems*, 3(1):45–54, 2013.

[72] 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.

[73] Wonjun Lee and Seungjae Shin. An empirical study of consumer adoption of internet of things services. *INTERNATIONAL JOURNAL OF ENGINEERING AND TECHNOLOGY INNOVATION*, 9(1):1–11, 2019.

[74] Woojin Lee, Lina Xiong, and Clark Hu. The effect of facebook users' arousal and valence on intention to go to the festival: Applying an extension of the technology acceptance model. *International Journal of Hospitality Management*, 31(3):819–827, 2012.

[75] Xu Li, Rongxing Lu, Xiaohui Liang, Xuemin Shen, Jiming Chen, and Xiaodong Lin. Smart community: an internet of things application. *IEEE Communications Magazine*, 49(11), 2011.

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

[77] Jiunn-Woei Lian. Critical factors for cloud based e-invoice service adoption in taiwan: An empirical study. *International Journal of Information Management*, 35(1):98–109, 2015.

[78] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I Hong. Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 199–212, 2014.

[79] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun (Aerin) Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In *Proceedings of the 2016 Symposium on Usable Privacy and Security*, 2016.

[80] Franco Loi, Arunan Sivanathan, Hassan Habibi Gharakheili, Adam Radford, and Vijay Sivaraman. Systematically Evaluating Security and Privacy for Consumer IoT Devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, IoTS&P '17, pages 1–6, New York, NY, USA, 2017. ACM.

[81] Chris Lu. Overview of security and privacy issues in the internet of things, 2014.

[82] Michelle Madejski, Maritza Johnson, and Steven M Bellovin. A study of privacy settings errors in an online social network. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, pages 340–345. IEEE, 2012.

[83] Carlo Maria Medaglia and Alexandru Serbanati. An overview of privacy and security issues in the internet of things. In *The Internet of Things*, pages 389–395. Springer, 2010.

[84] Miriam J Metzger. Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of computer-mediated communication*, 9(4):JCMC942, 2004.

[85] George R Milne and Mary J Culnan. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of interactive marketing*, 18(3):15–29, 2004.

[86] Monika Mital, Victor Chang, Praveen Choudhary, Armando Papa, and Ashis K Pani. Adoption of internet of things in india: A test of competing models using a structured equation modeling approach. *Technological Forecasting and Social Change*, 136:339–346, 2018.

[87] Helen Nissenbaum. Privacy as Contextual Integrity Symposium - Technology, Values, and the Justice System. *Washington Law Review*, 79:119–158, 2004.

[88] 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.

[89] 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.

[90] Yangil Park and Jengchung V Chen. Acceptance and adoption of the innovative use of smartphone. *Industrial Management & Data Systems*, 107(9):1349–1365, 2007.

[91] Charith Perera, Ciaran McCormick, Arosha K. Bandara, Blaine A. Price, and Bashar Nuseibeh. Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms. In *Proceedings of the 6th International Conference on the Internet of Things*, IoT'16, pages 83–92, New York, NY, USA, 2016. ACM.

[92] Andreas Pfitzmann and Marit Köhntopp. Anonymity, unobservability, and pseudonymity—a proposal for terminology. In *Designing privacy enhancing technologies*, pages 1–9. Springer, 2001.

[93] Joseph Phelps, Glen Nowak, and Elizabeth Ferrell. Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, 19(1):27–41, 2000.

[94] Tero Pikkarainen, Kari Pikkarainen, Heikki Karjaluoto, and Seppo Pahnila. Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet research*, 14(3):224–235, 2004.

[95] Michael E Porter and James E Heppelmann. How smart, connected products are transforming competition. *Harvard business review*, 92(11):64–88, 2014.

[96] Gil Press. Internet of things by the numbers: Market estimates and forecasts, 2014.

[97] 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.

[98] Rupak Rauniar, Greg Rawski, Jei Yang, and Ben Johnson. Technology acceptance model (tam) and social media usage: an empirical study on facebook. *Journal of Enterprise Information Management*, 27(1):6–30, 2014.

[99] 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.

[100] Luke Russell, Rafik Goubran, and Felix Kwamena. Personalization using sensors for preliminary human detection in an iot environment. In *Distributed Computing in Sensor Systems (DCOSS), 2015 International Conference on*, pages 236–241. IEEE, 2015.

[101] 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 Ubiquitous Comput.*, 13(6):401–412, August 2009.

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

[103] Barry Schwartz. *The paradox of choice: Why more is less*, volume 6. HarperCollins New York, 2004.

[104] Xiaopu Shang, Runtong Zhang, and Ying Chen. Internet of things (iot) service architecture and its application in e-commerce. *Journal of Electronic Commerce in Organizations (JECO)*, 10(3):44–55, 2012.

[105] Hong Sheng, Fiona Fui-Hoon Nah, and Keng Siau. An Experimental Study on Ubiquitous commerce Adoption: Impact of Personalization and Privacy Concerns. *Journal of the Association for Information Systems*, 9(6):344–376, June 2008.

[106] 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.

[107] Ludovico Solima, Maria Rosaria Della Peruta, and Manlio Del Giudice. Object-generated content and knowledge sharing: the forthcoming impact of the internet of things. *Journal of the Knowledge Economy*, 7(3):738–752, 2016.

[108] Juliana Sutanto, Elia Palme, Chuan-Hoo Tan, and Chee Wei Phang. Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS Quarterly*, 37(4):1141–1164, 2013.

[109] Karen Tang, Jason Hong, and Dan Siewiorek. The implications of offering more disclosure choices for social location sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 391–394. ACM, 2012.

[110] David G Taylor, Donna F Davis, and Ravi Jillapalli. Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic commerce research*, 9(3):203–223, 2009.

[111] Max Teltzrow and Alfred Kobsa. Impacts of User Privacy Preferences on Personalized Systems: a Comparative Study. In Clare-Marie Karat, Jan Blom, and John Karat, editors, *Designing Personalized User Experiences for eCommerce*, pages 315–332. Kluwer Academic Publishers, Dordrecht, Netherlands, 2004. DOI 10.1007/1-4020-2148-8_17.

[112] The European Parliament and the Council of the European Union. Regulation (eu) 2016/679 of the european parliament and of the council. *Official Journal of the European Union*, page 1:88, 2016.

[113] Horst Treiblmaier and Irene Pollach. Users' Perceptions of Benefits and Costs of Personalization. In *ICIS 2007 Proceedings*, 2007.

[114] Lynn Tsai, Primal Wijesekera, Joel Reardon, Irwin Reyes, Serge Egelman, David Wagner, Nathan Good, and Jung-Wei Chen. Turtle guard: Helping android users apply contextual privacy preferences. In *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[115] Virpi Kristiina Tuunainen, Olli Pitkänen, and Marjaana Hovi. Users' awareness of privacy on online social networking sites-case facebook. *Bled 2009 Proceedings*, page 42, 2009.

[116] Dieter Uckelmann, Mark Harrison, and Florian Michahelles. An architectural approach towards the future internet of things. In *Architecting the internet of things*, pages 1–24. Springer, 2011.

[117] Blase Ur, Jaeyeon Jung, and Stuart Schechter. Intruders Versus Intrusiveness: Teens' and Parents' Perspectives on Home-entryway Surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '14, pages 129–139, New York, NY, USA, 2014. ACM.

[118] Thibaut Vallée, Karima Sedki, Sylvie Despres, M-Christine Jaulant, Karim Tabia, and Adrien Ugon. On personalization in iot. In *Computational Science and Computational Intelligence (CSCI), 2016 International Conference on*, pages 186–191. IEEE, 2016.

[119] Gregg Vanderheiden and Jutta Treviranus. Creating a global public inclusive infrastructure. In *International Conference on Universal Access in Human-Computer Interaction*, pages 517–526. Springer, 2011.

[120] Viswanath Venkatesh and Susan A Brown. A longitudinal investigation of personal computers in homes: adoption determinants and emerging challenges. *MIS quarterly*, pages 71–102, 2001.

[121] Viswanath Venkatesh, Michael G Morris, Gordon B Davis, and Fred D Davis. User acceptance of information technology: Toward a unified view. *MIS quarterly*, pages 425–478, 2003.

[122] Vassilios S Verykios, Elisa Bertino, Igor Nai Fovino, Loredana Parasiliti Provenza, Yucel Saygin, and Yannis Theodoridis. State-of-the-art in privacy preserving data mining. *ACM Sigmod Record*, 33(1):50–57, 2004.

[123] Michele Vescovi, Corrado Moiso, Mattia Pasolli, Lorenzo Cordin, and Fabrizio Antonelli. Building an eco-system of trusted services via user control and transparency on personal data. In *IFIP International Conference on Trust Management*, pages 240–250. Springer, 2015.

[124] Weiquan Wang and Izak Benbasat. Recommendation agents for electronic commerce: Effects of explanation facilities on trusting beliefs. *Journal of Management Information Systems*, 23(4):217–246, 2007.

[125] Weiquan Wang and Izak Benbasat. Interactive decision aids for consumer decision making in e-commerce: The influence of perceived strategy restrictiveness. *MIS quarterly*, pages 293–320, 2009.

[126] 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.

[127] Vishanth Weerakkody, Ramzi El-Haddadeh, Faris Al-Sobhi, Mahmud Akhter Shareef, and Yogesh K Dwivedi. Examining the influence of intermediaries in facilitating e-government adoption: An empirical investigation. *International Journal of Information Management*, 33(5):716–725, 2013.

[128] Bruce D Weinberg, George R Milne, Yana G Andonova, and Fatima M Hajjat. Internet of things: Convenience vs. privacy and secrecy. *Business Horizons*, 58(6):615–624, 2015.

[129] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences. In *Security and Privacy (SP), 2017 IEEE Symposium on*, pages 1077–1093. IEEE, 2017.

[130] 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.

[131] Pamela Wisniewski, Bart P Knijnenburg, and H Richter Lipford. Profiling facebook users privacy behaviors. In *SOUPS2014 Workshop on Privacy Personas and Segmentation*, 2014.

[132] 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.

[133] Ian H Witten, Eibe Frank, Mark A Hall, and Christopher J Pal. *Data Mining: Practical machine learning tools and techniques*. Morgan Kaufmann, 2016.

[134] Barbara H Wixom and Peter A Todd. A theoretical integration of user satisfaction and technology acceptance. *Information systems research*, 16(1):85–102, 2005.

[135] Peter Worthy, Ben Matthews, and Stephen Viller. Trust Me: Doubts and Concerns Living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*, DIS '16, pages 427–434, New York, NY, USA, 2016. ACM.

[136] Heng Xu, Xin Robert Luo, John M Carroll, and Mary Beth Rosson. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision support systems*, 51(1):42–52, 2011.

[137] Heng Xu, Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal. The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of management information systems*, 26(3):135–174, 2009.

[138] Heng Xu, Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal. Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research*, 23(4):1342–1363, 2012.

[139] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*, page 5. ACM, 2015.

Appendices

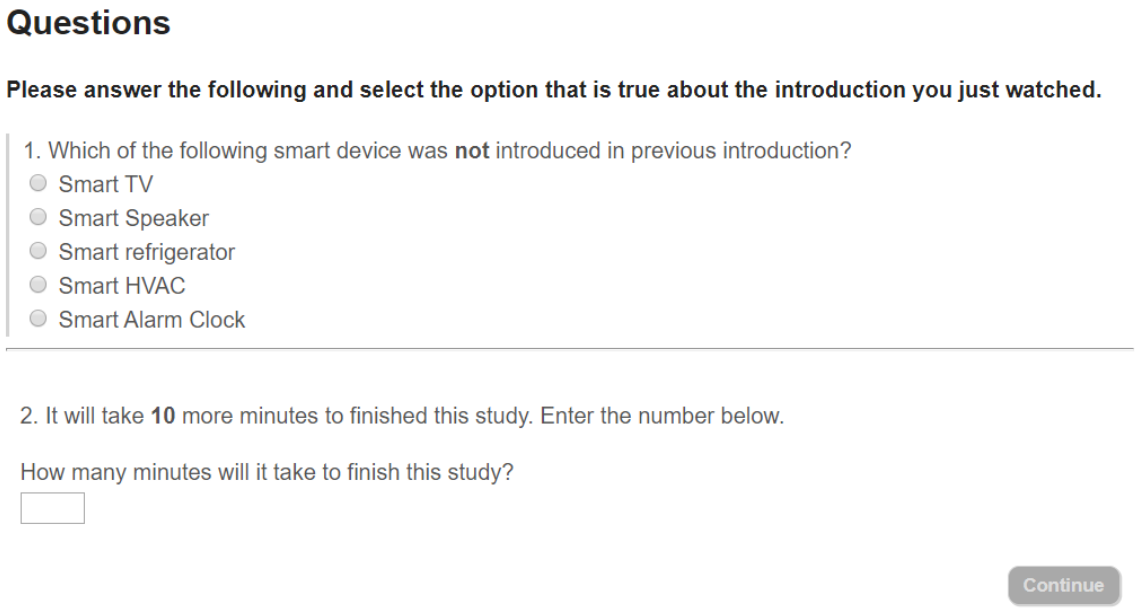


Figure A1: Attention Check Question of Evaluating privacy-setting UI for Household IoT

Table A1: Table of Accuracies.

	Pick Profile	Single Smart Default	Direct prediction	Privacy Attitude	Social Behaviour	Negotiability
S Set						
Identity	66.67 %	66.67 %	66.67 %	66.67 %	66.67 %	66.67 %
Contacts	83.33 %	70.00 %	70.00 %	56.67 %	73.33 %	80.00 %
Location	83.33 %	83.33 %	83.33 %	83.33 %	83.33 %	83.33 %
SMS	90.00 %	50.00 %	70.00 %	50.00 %	53.33 %	73.33 %
Storage	83.33 %	56.67 %	70.00 %	43.33 %	46.67 %	60.00 %
Camera	80.00 %	60.00 %	86.67 %	60.00 %	70.00 %	63.33 %
Bluetooth	83.33 %	83.33 %	83.33 %	83.33 %	83.33 %	83.33 %
Photos	80.00 %	66.67 %	100.00 %	60.00 %	76.66 %	70.00 %
Phone	96.67 %	56.67 %	76.67 %	50.00 %	60.00 %	80.00 %
Motion	96.67 %	96.67 %	96.67 %	96.67 %	96.67 %	96.67 %
Media	70.00 %	76.67 %	56.67 %	43.33 %	33.33 %	60.00 %
Mobile Data	76.67 %	76.67 %	76.67 %	76.67 %	76.67 %	76.67 %
Average	82.50 %	70.28 %	78.06 %	64.17 %	68.33 %	74.44 %
A set						
First Name	100.00 %	63.33 %	100.00 %	63.33 %	73.33 %	56.67 %
Last Name	96.67 %	60.00 %	96.67 %	60.00 %	70.00 %	60.00 %
Gender	76.67 %	76.67 %	76.67 %	76.67 %	76.67 %	76.67 %
Birthday	90.00 %	60.00 %	90.00 %	60.00 %	63.33 %	53.33 %
Height	70.00 %	70.00 %	70.00 %	70.00 %	70.00 %	70.00 %
Weight	70.00 %	70.00 %	70.00 %	70.00 %	70.00 %	70.00 %
Average	83.89 %	66.67 %	83.89 %	66.67%	70.55%	64.44 %
F set						
Steps	96.67 %	73.33 %	96.67 %	76.67 %	70.00 %	76.67 %
Distance	96.67 %	73.33 %	96.67 %	76.67 %	70.00 %	76.67 %
Elevation	100.00 %	70.00 %	100.00 %	73.33 %	73.33 %	80.00 %
Floors	96.67 %	73.33 %	96.67 %	76.67 %	70.00 %	76.67 %
Activity minutes	100.00 %	70.00 %	100.00 %	73.33 %	73.33 %	80.00 %
Calories activity	96.67 %	73.33 %	96.67 %	76.67 %	70.00 %	76.67 %
Weight	90.00 %	60.00 %	90.00 %	63.33 %	70.00 %	76.67 %
Sleep	93.33 %	63.33 %	93.33 %	66.67 %	66.67 %	80.00 %
Heartrate	100.00 %	70.00 %	100.00 %	73.33 %	73.33 %	80.00 %
Food logs	90.00 %	60.00 %	90.00 %	63.33 %	70.00 %	76.67 %
Friends	83.33 %	53.33 %	83.33 %	56.67 %	63.33 %	70.00 %
Profile	96.67 %	66.67 %	96.67 %	70.00 %	76.67 %	76.67 %
Location	86.67 %	56.67 %	86.67 %	60.00 %	66.67 %	66.67 %
Device & settings	93.33 %	63.33 %	93.33 %	66.67 %	73.33 %	73.33 %
Average	94.29 %	66.19 %	94.29 %	69.52 %	70.48 %	76.19 %
G set						
SN Public	90.00 %	90.00 %	90.00 %	90.00 %	90.00 %	90.00 %
SN Friends Only	73.33 %	53.33 %	73.33 %	63.33%	60.00 %	56.67 %
Health	66.67 %	60.00 %	60.00 %	43.33 %	40.00 %	70.00 %
Other Apps	76.67 %	76.67 %	76.67 %	76.67 %	76.67 %	76.67 %
Corporate	80.00 %	80.00 %	80.00 %	80.00 %	80.00 %	80.00 %
Government	86.67 %	86.67 %	86.67 %	86.67 %	86.67 %	86.67 %
Health	86.67 %	86.67 %	86.67 %	86.67 %	86.67 %	86.67 %
Safety	90.00 %	90.00 %	90.00 %	90.00 %	90.00 %	90.00 %
Social	93.33 %	60.00 %	100.00 %	70.00 %	60.00 %	63.33 %
Commercial	73.33 %	73.33 %	73.33 %	73.33 %	73.33 %	73.33 %
Convenience	80.00 %	73.33 %	73.33 %	76.67 %	66.67 %	70.00 %
Frequency	53.33 %	53.33 %	53.33 %	53.00 %	53.33 %	53.33 %
Retention	50.00 %	40.00 %	50.00 %	50.00 %	43.33 %	46.67 %
Average	76.92 %	71.02 %	76.41 %	72.31 %	69.74 %	72.56 %
Over-all Average	84.74 %	68.74 %	83.41 %	68.52 %	69.70 %	73.11 %

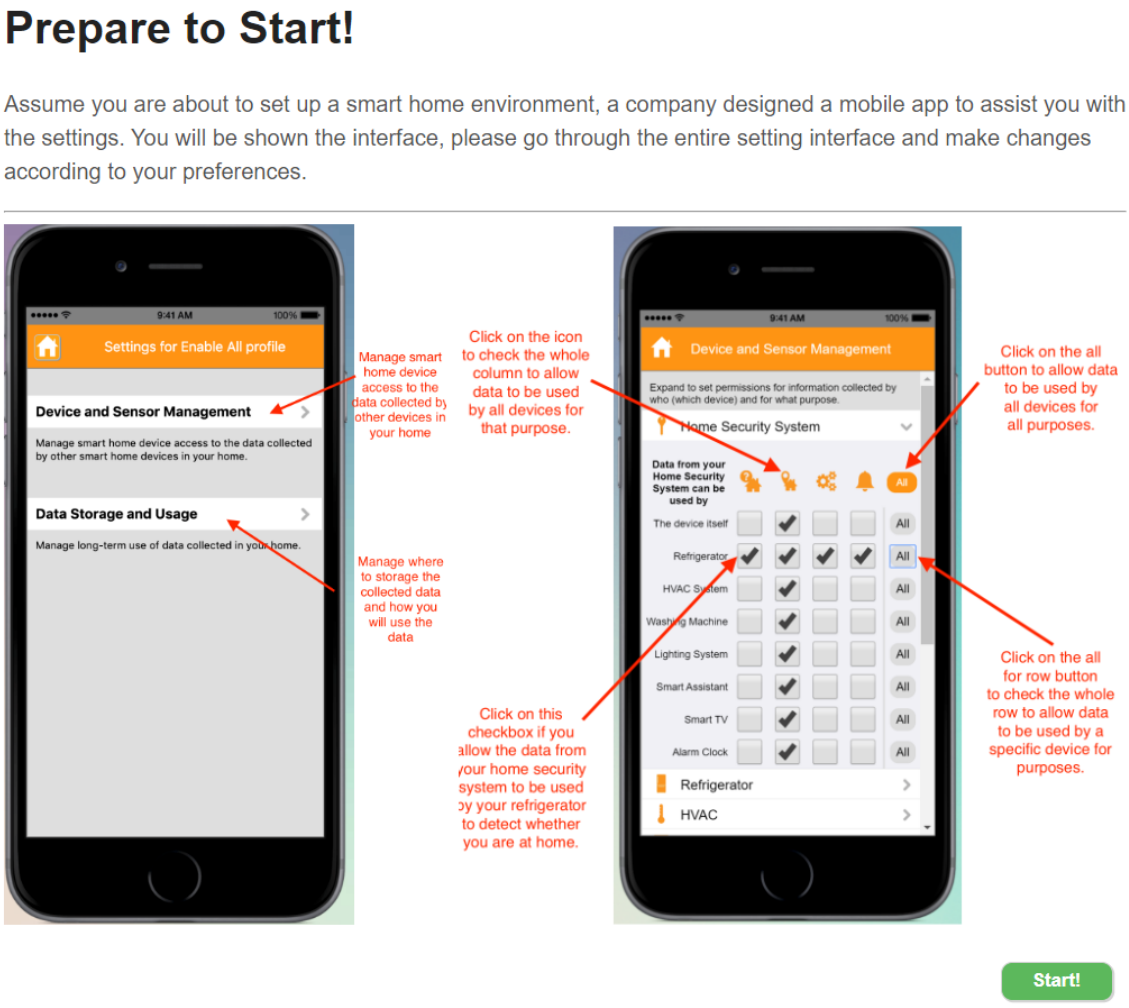


Figure A2: Instructions on how to use the UIs

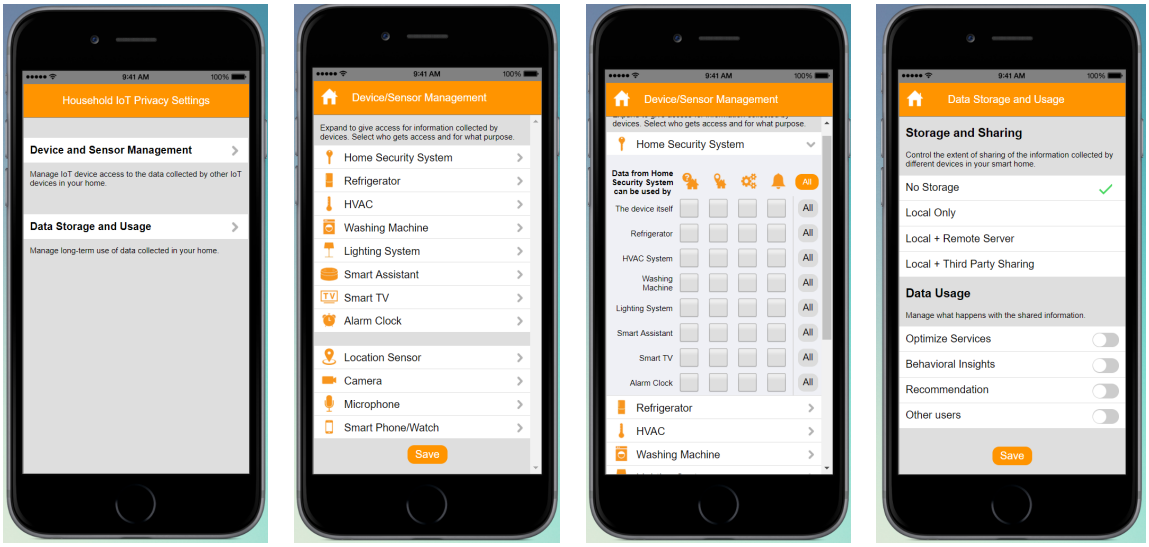


Figure A3: User Interface 1 with all settings turned off

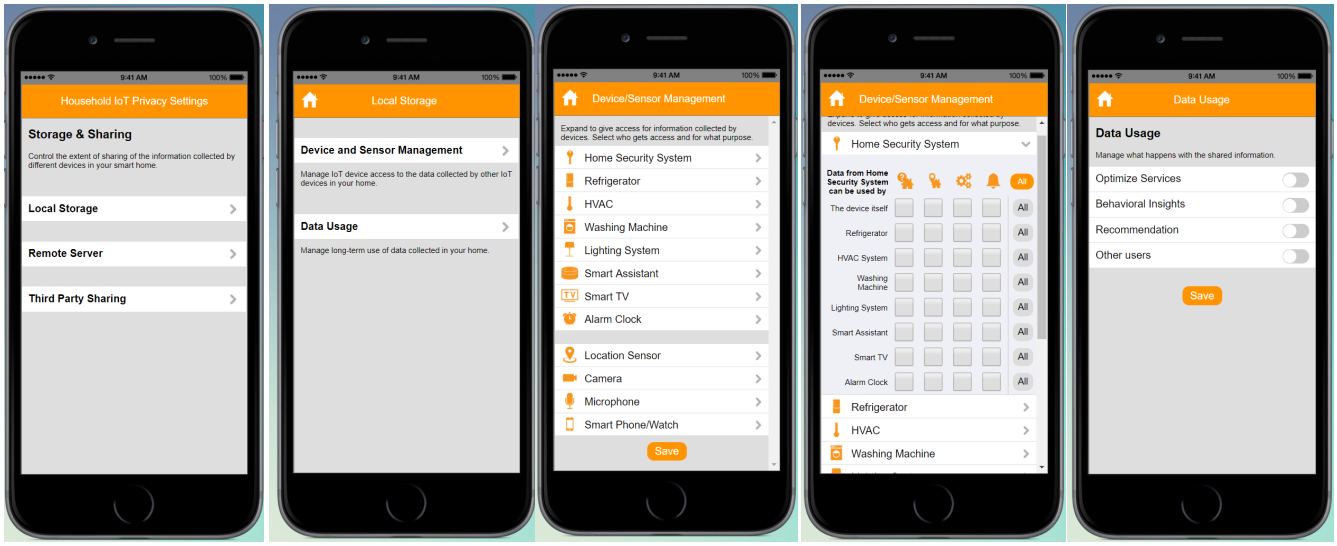


Figure A4: User Interface 2 with all settings turned off

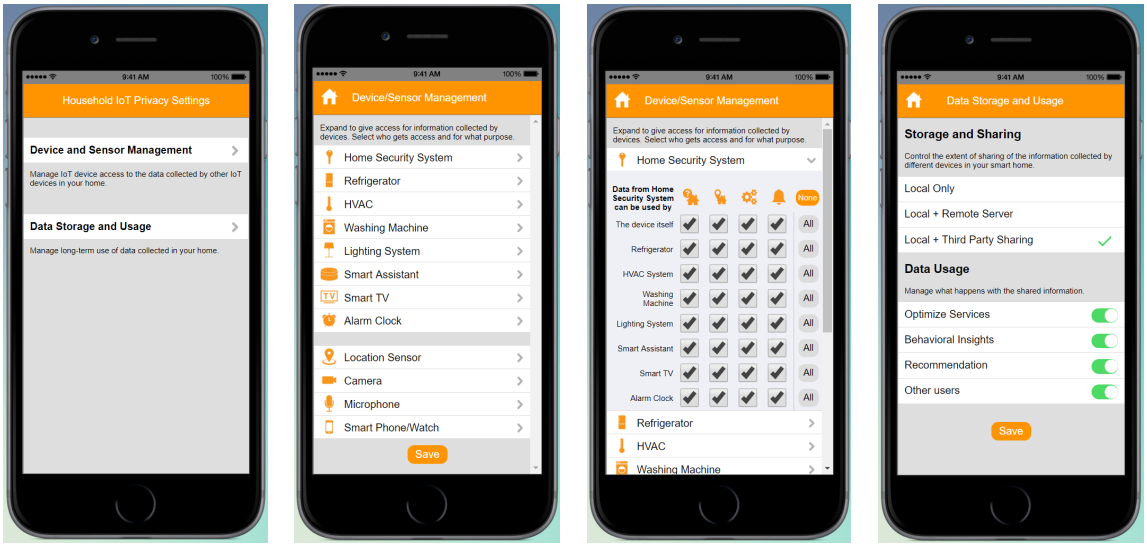


Figure A5: User Interface 1 with all settings turned on

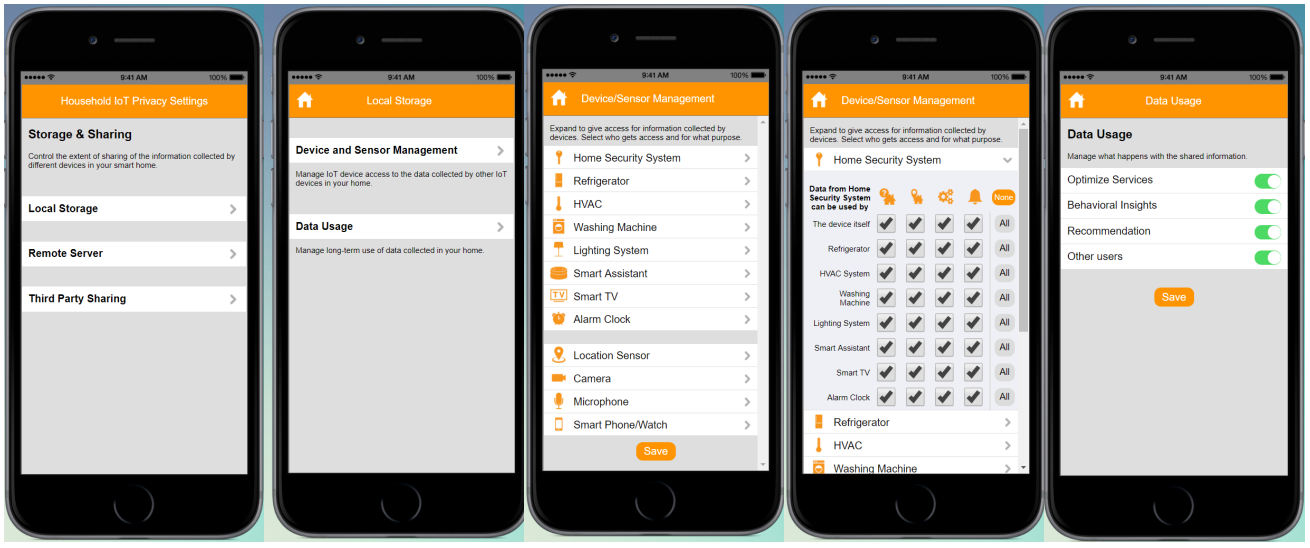


Figure A6: User Interface 2 with all settings turned on

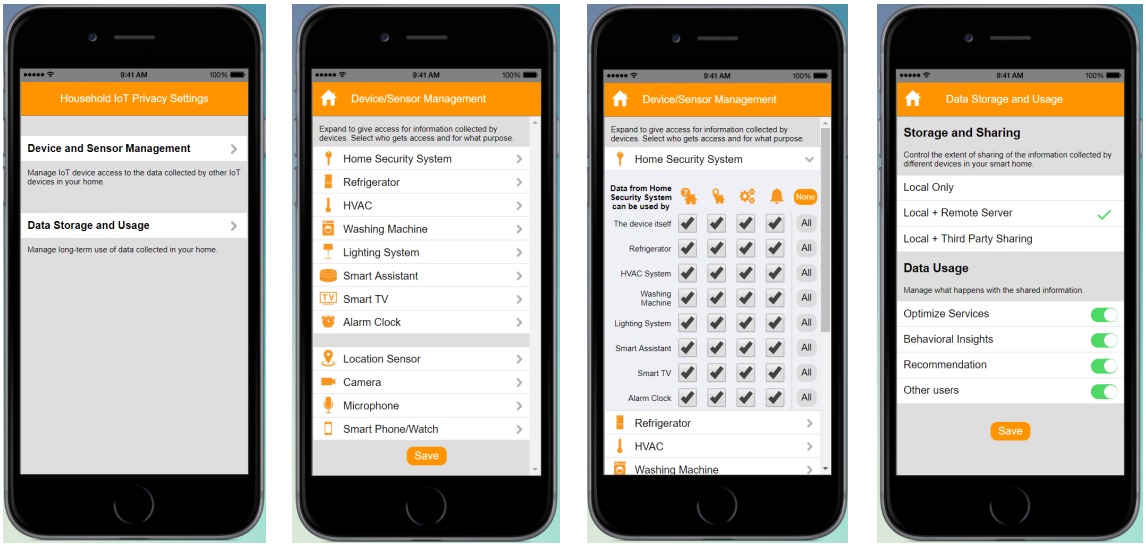


Figure A7: User Interface 1 with Smart Default

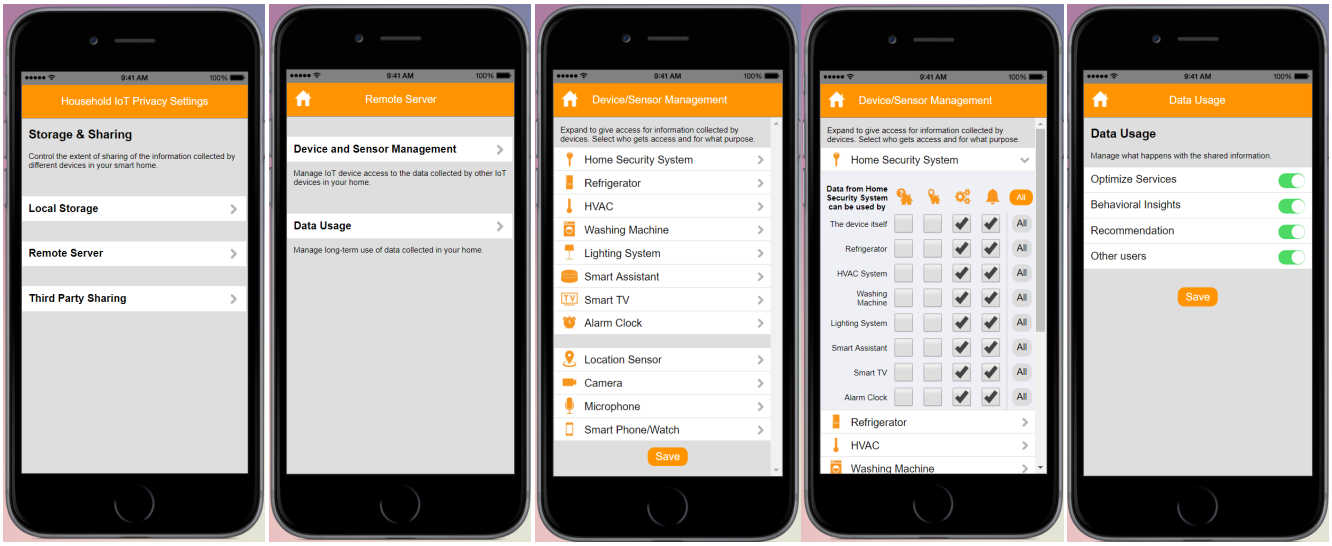


Figure A8: User Interface 2 with Smart Default

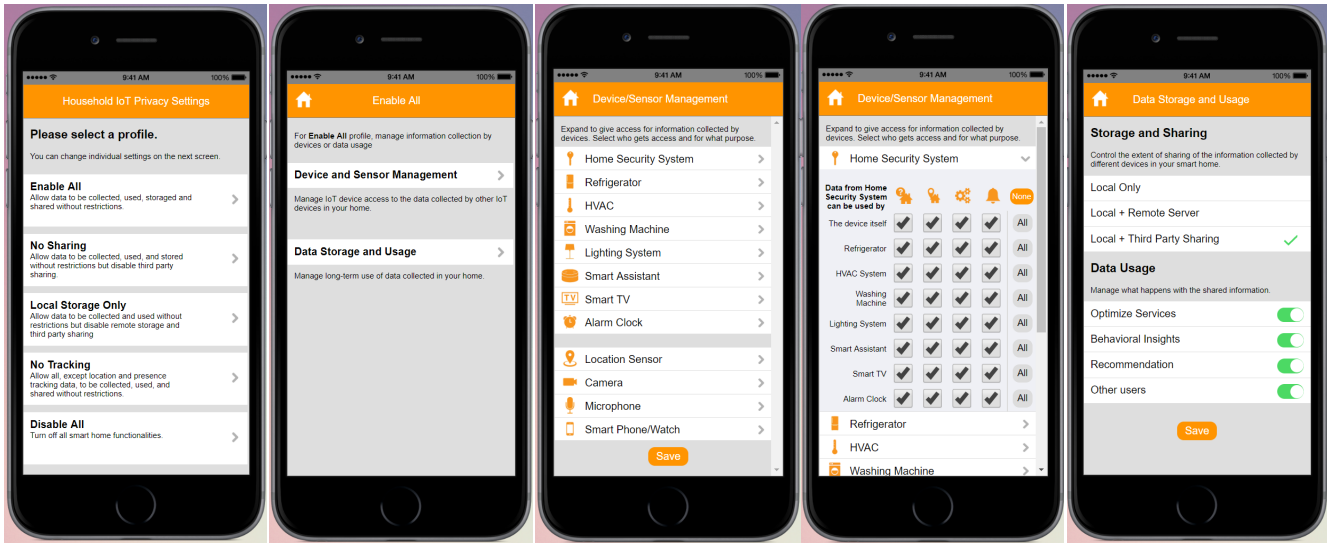


Figure A9: User Interface 1 with Smart Profiles

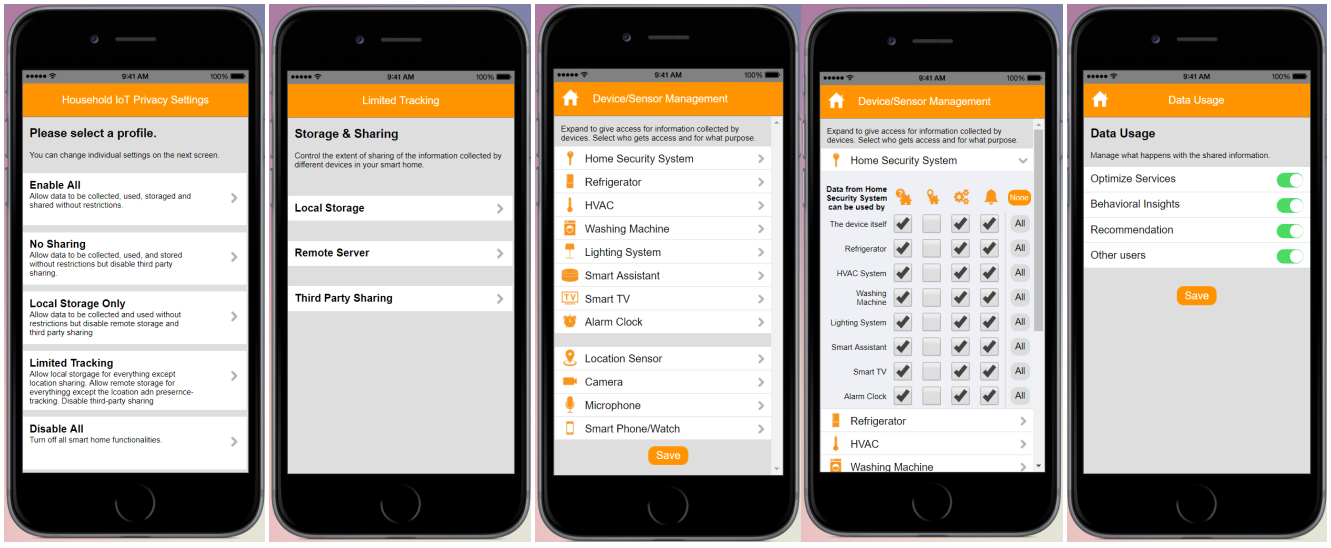


Figure A10: User Interface 2 with Smart Profiles