Recommending Privacy Settings for Internet-of-Things

A Dissertation Proposal by
Yangyang He
Jan 2019

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

Approved By:

Dr. Bart P. Knijnenburg
Advisor/Committee Chair

Dr. Larry F. Hodges
Committee Member

Dr. Brian Malloy
Committee Member

Dr. Alexander Herzog
Committee Member

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) Recommending User Privacy Preferences for Fitness IoT. 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. To appear on 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. IUI2018, 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 live, 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 that advances rapidly recently, these internet-connected devices are able to gain knowledge of its 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 [59, 87, 48, 46, 39].

A wide range of well-respected organizations has estimated that IoT will grow rapidly and bring huge social and economic potential. For example, Gartner [23] 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 [77]. 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 [105], processing and storing the data in ways unexpected by the consumer [65], and privacy

and security breach [65, 113].

In IoT environments, all the IoT devices are intended to collect information from the users to realize their functionality. Technical solutions can be used to minimize the data collected for such functionality [53, 73, 100], 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 [19, 55, 89]. However, as the diversity of IoT devices increases, it becomes more and more difficult to keep up with the many different ways in which data about ourselves is collected and disseminated. Although generally users care about their privacy, few of them in practice find time to carefully read the privacy policies or the privacy-settings that are provided to them. 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. 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. 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 [24, 1, 49, 10, 13], and 2) privacy nudges [3, 63, 30, 63]. 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 [49]. 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 the 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 proposal, I first present the background and related work of this proposal 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 on 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). The current biggest limitation for such "data-driven" approach is that we did not test any of the presented interfaces, so we don't know what level of complexity (both in terms of the user interface and the in terms of the profiles) is most suitable. Thus for my proposed work, I will address this limitation by discussing our proposed study to evaluate the new interface of recommending privacy-settings for household IoT in Chapter 7. Finally, I conclude this proposal 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. However, such disclosed information could be accessed by other smart devices owned by themselves, other people, organizations, government, or some third-parties with good or bad purpose, which brings privacy risks to the users. Thus, we attempt to know the IoT acceptance model for following reasons: 1) The factors that affect users' adopting phase may have a high chance to also have 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; 4) These factors can potentially help us develop the scales to evaluate the interfaces that we design, and build a theory 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 [5]. 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 unique addressing scheme, are able to interact with each other and cooperate with their neighbors to reach common goals [6]. As various wireless sensor technologies (e.g. RFID, embedded sensors, and actuator nodes) and artificial intelligence advance rapidly during the last two decades, the definition of the IoT has evolved to more broad covering wide range of monitoring and control applications based on a network of sensing and actuating devices that controlled remotely through the Internet in many fields, such as tracking, transportation, household usage, healthcare and fitness [59, 87, 48, 46, 39].

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 [105, 76]. With such huge social and economic potential, IoT is estimated to grow rapidly by a wide range of well-respected organizations. For example, Gartner [23] 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. However, there exist several key security and privacy concerns associated with the rise of the IoT, including data processing and storage, privacy and security breach, etc [105, 65, 113].

Previous studies mostly focused on the technical issues of IoT technologies [27, 56, 84]. For example, Uckelmann et al. systematically explained the architecture of future IoT [94]. Chen et al. present a vision of IoT's applications in China [17]. 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 [37]. However, little attention has been devoted to, from the perspective of individual consumers, understanding how will the user of IoT will trade off the above mentioned benefits and privacy concerns of IoT technology when they consider adopting it [2, 32, 67].

Furthermore, researchers identified the security and privacy issues as the major challenges for consumer acceptance of the IoT technology's user-oriented IoT applications (Medaglia & Serbanati,

2010) [30]. Arguably, if the user find their privacy demands can not be satisfied (e.g. it's confusing to) 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 origin Technology Acceptance Model and 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

Many research has attempt to examine the technology acceptance. Among them, the Technology Acceptance Model (TAM) is arguably the most popular model that explains how users come to accept and use a technology [21]. TAM suggests that an individual's *Behavioral Intention* to Use an information technology is significantly dependent upon the individual's perception of *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 have applied to a wide range of technology adoption contexts [111], such as the adoption of PC [98], smartphones [71], mobile marketing [9], Internet banking [75], facebook [58, 79], and online shopping [33].

2.2.2 UTAUT

The unified theory of acceptance and use of technology (UTAUT) is a technology acceptance model proposed by Venkatesh et al. [99]. Compared to TAM, UTAUT model 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 de-

termine technology use. UTAUT also identifies four moderators (i.e., age, gender, experience, and voluntariness).

UTAUT model has been applied or extended in the many contexts, such as electronic learning [102], e-government [104], and cloud computing [61]. UTAUT is adapted upon previous models of technology adoption, and designed specifically to investigate users' acceptance of a new technology and it has explanatory power higher than previous models (e.g. TAM). These make the UTAUT model suitable for understanding the acceptance of IoT.

2.2.3 The Acceptance of IoT

Researchers have attempted to identify the factors that affect the acceptance of IoT by customers. Acquity Group [36] 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 [32], 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.

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 (The questionnaire is attached in Appendix). These questions need participants to input their personal preferences about 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

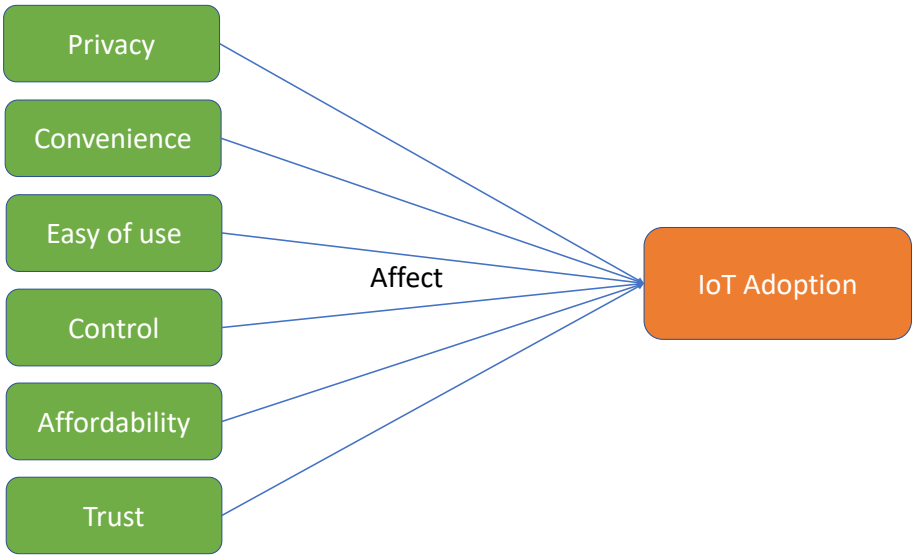


Figure 2.1: The factors that affecting users' adoptions of IoT found in our study

and affinity diagram techniques. We then use a ground approach to creating a theory, which is shown in Figure 2.1.

The results showed similar founding as fore-mentioned work [32, 2]. However, in our study, we noticed an interesting phenomenon that no literature has mentioned – once the trust to 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:

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

Figure 2.2: Trust Chain

to the manufacturers (i.e. the brand of the devices), and can arguably be categorized as an emotional behavior because users wouldn't 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. Research has shown that in IoT domain, users are more likely to perceive concrete benefits and abstract risks, resulting this emotional behavior phenomenon [Kevin's work]. Such behavior could bring harm to their privacy and security. To be more rational, users are suggested to investigate the Third-Parties that will handle their personal data. Thus, we suggest the manufacturer/designers of the IoT privacy to provide users transparency and control on what third-parties they will sharing 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 affect users' decisions when adopting IoT. 4) The acceptance of IoT is still not systematically examined.

In the next chapter, we discuss the reason that cause the privacy issues in IoT, how effectively existing privacy control schemes are, and the work that aim 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 are gaining popularity and bringing privacy issues to us at the same time, it is urgent to study the reason that cause 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 [69], but can be clustered into groups [4, 52]. In [108, 50], Facebook users are found to have 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 user's preferences change for every fitness/heath index. Weight was found the be the most important index [12].

In the other hand, 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 were not match the users' desired settings. In [66], 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 diversified. One reason for this is the increasing number of privacy rules make manual privacy configuration excessively challenging for normal users [31]. Knijnenburg et al. discover that people's information disclosure behaviours are affected by multiple dimensions [52]. 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 group and adapt its privacy practices to the disclosure style of this group to satisfy different types of information and users. However, more privacy policies in the other 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 [107]. Therefore, we used a data-driven approach (machine learning techniques) to discover the suitable smart privacy profiles for the user groups with different "disclosure styles".

3.2 Privacy in IoT

IoT systems are capable of providing a highly personalized services to their users [96, 25, 34]. Henka et al. [40] propose an approach to personalize services in household IoT using the Global Public Inclusive Infrastructure's [97] preference set to describe an individual's needs and preferences, and then adapting a smart environment accordingly. Russell et al. [81] use unobtrusive sensors and micro-controller to realize a human detection for further providing personalization in a scenario of a family making use of the IoT in their daily living.

Researchers have shown that privacy plays a limiting role in users' adoption of personalized services [90]. For example, Awad and Krishnan [7] show that privacy concerns inhibit users' use of personalized services, and Sutanto et al. [88] demonstrated that privacy concerns can prevent people from using a potentially beneficial personalized application. Kobsa et al. [54] 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 [74, 41, 43], and researchers therefore claim that both the benefits and the risks meet a certain threshold [92], or that they should

be in balance [16].

The argument that using user-generated data for personalization can result in privacy concerns has also been made in IoT environments [112, 32, 2]. One of the first examples in this regard was the work by Sheng et al. [85], 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 [72, 64]. 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 [20]. Likewise, Jayraman et al.'s privacy preserving architecture aggregates requested data to preserve user privacy [44].

Other research has considered IoT privacy from the end-user perspective [29], 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 [95]) 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 [107], and Feth et al. investigated the creation of understandable and usable controls [29]). 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 Control Schemes

Previous studies in smartphone privacy have showed that the current smartphone privacy interfaces lack the potential to provide the necessary user privacy information or control for both Android and iOS systems [62]. Several solutions have been proposed to improve mobile privacy protection and offer users more privacy control [28, 11]. These leads 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 [93, 106]. In AOI model, the smart phone 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 number of users would read or pay attention to the privacy settings when installing the app, and even fewer users can understand their meaning [28, 47]. Several third-party apps have been developed to cope with this problem, such as Turtleguard [93] and Mockdroid [11]. In the AOFU model [93], permissions are only asked during the first use of an app or a 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 user more informed and gives them more control as the previous model does not allow users to be informed effectively [30]. Moreover, it has been proven that interactive notification is more efficient in informing users request access [30].

A few privacy management were developed to simplify the task of controlling personal data for smartphone users. For instance, ipShield [14] is a context-aware privacy framework for mobile systems that provides users with great control of their data and inference risks. My Data Store [101] offers a set of tools to manage, control and exploit personal data by enhancing an individual's awareness on the value of their data. Similarly, Databox [15] 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 the 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 smartphone domain, privacy nudging is an effective scheme to increase users' awareness [3]. Privacy nudging allows users to be informed and aware on both their privacy settings and how the third party applications access their data [63, 30]. It has been showed that 78.7% [63] of the privacy recommendation were adopted by the smartphone users. However, such nudging 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 will soon start to ignore, like software EULAs [35] or privacy policies [45]. In addition, Privacy nudges lack the personalization and provide general recommendation.

Another approach which is more user-centric is the user-tailored privacy [50]. It models

users' privacy concerns and provides them with adaptive privacy decision support. This model can be seen as personalized "smart nudges" where the recommendation is aligned with the user's privacy preference. User-tailored privacy aids users in making privacy decisions by providing them the right amount of both the privacy-related information associated to them and the useful privacy control that do not overwhelm or mislead them. However, in practice it is hard to implement general privacy model as the idea is too broad and abstract especially in the diversity of privacy perception of users.

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 [83]. This approach can be further simplified by grouping recipients into relevant semantic categories, such as Google+'s *circles* [103]. Taking a step further, Raber et al. [78] 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 [107]. 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) [51]. 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. [82] 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. [70] 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. [22] 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. [60] 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. [26], 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. [80] 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 proposal, 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.

In the next chapter, we will examine our methodology in the general/public IoT context, and compare it with the existing research.

Chapter 4

Recommending Privacy Settings for General/Public IoT

In chapter **??**, we have discussed what are the key factors affecting users to adopt IoT systems/devices, the privacy risks caused by inappropriate privacy disclosure and the difficulties that people have when manually configuring their privacy-setting for their IoT systems/devices. To alleviate similar burden of doing this in OSN/mobile areas, researchers have applied machine learning techniques to predict people's location-privacy preferences, thereby automatically configuring their location-privacy settings. Therefore, we speculate that machine learning algorithm based user clustering can also be used to recommend privacy-setting for IoT users.

In this chapter, we demonstrate our work completed in exploring recommending privacy settings for general IoT, including the dataset that we use, our methodology, the inspection of users' behaviors using statistical analyses, prediction of users' behaviors using machine learning techniques, and the privacy-setting prototypes that we create based on both statistical and machine learning results.

In this chapter the following questions will be answered:

- Q1: What are the key parameters affecting the users' privacy decisions in a general IoT scenario?
- Q2: Can you cluster users of general IoT and provide them effective and accurate smart default/profiles of privacy-settings using machine learning techniques?

As we have already discussed, there is similarity in people's privacy preferences. Therefore, neighbourhood-based recommendations may be as accurate as model-based recommendations. Furthermore, neighbourhood-based recommendations are made from crowdsourcing sources, which means that their performance may be better than that of model-based recommenders when the data of individual users are insufficient.

4.1 Dataset and design

As we have discussed in Chapter 1, the development of usable privacy interfaces commonly relies on user studies with existing systems. Since the Intel control framework has yet to be implemented [18], this method is not possible. We therefore we leveraged data collected by Lee and Kobsa [57], 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', 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

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

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

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 [86]. However, since people differ extensively in their privacy preferences [69], 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 [52, 69, 109]. We perform machine learning analysis on this dataset to create a similar set of "smart profiles" for our general IoT privacy-setting interface.

4.2 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 [60].

'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-

[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 [8].

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.

Moreover, we found no significant interaction effects of parameters on decision. The only significant interaction however was 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.

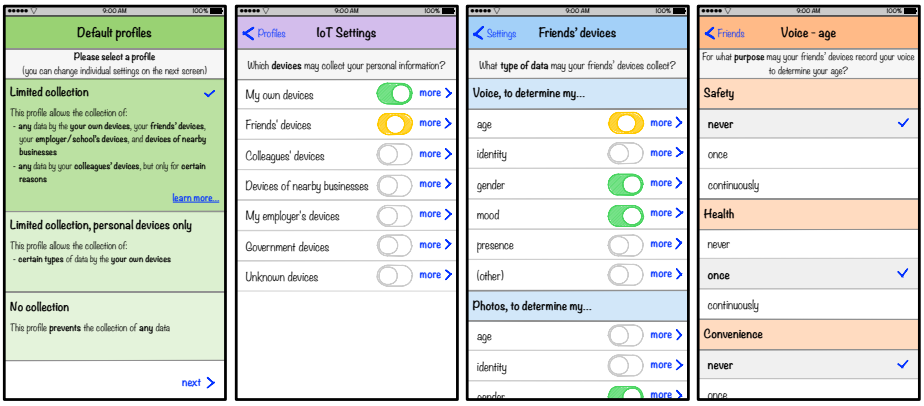


Figure 4.1: From Left, Screen 1 shows three default settings, Screen 2,3 and 4 shows layered interface

4.3 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 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.

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

Accuracies of the resulting solutions are reported in Table 4.2.

4.3.1 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.

4.3.2 Overall Prediction

We next create a "smart default" by predicting the allow/reject decision with the scenario parameters using J48 with Weka's [38] 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

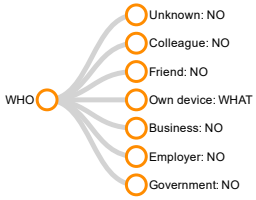


Figure 4.2: The Overall Prediction decision tree. Further drill down for 'who' = 'Own device' is provided in Table 4.4

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 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.

4.3.3 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 "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

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

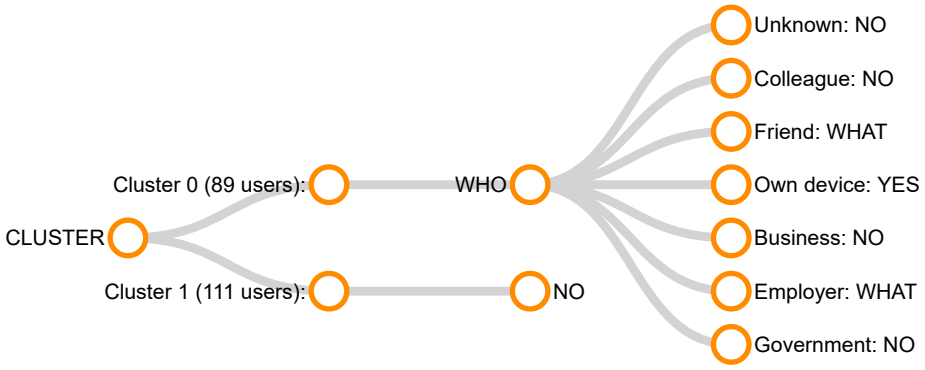


Figure 4.3: Attitude-based clustering: 2-cluster tree. Further drill down for **who** = 'Friend' or 'Employer/School' in Cluster 0 is hidden for space reasons.

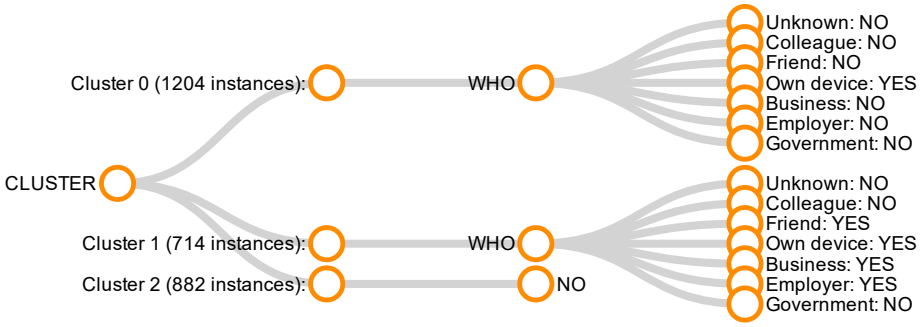


Figure 4.4: Attitude-based clustering: 3-cluster tree

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.

4.3.4 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 particpants 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**.

4.3.5 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 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

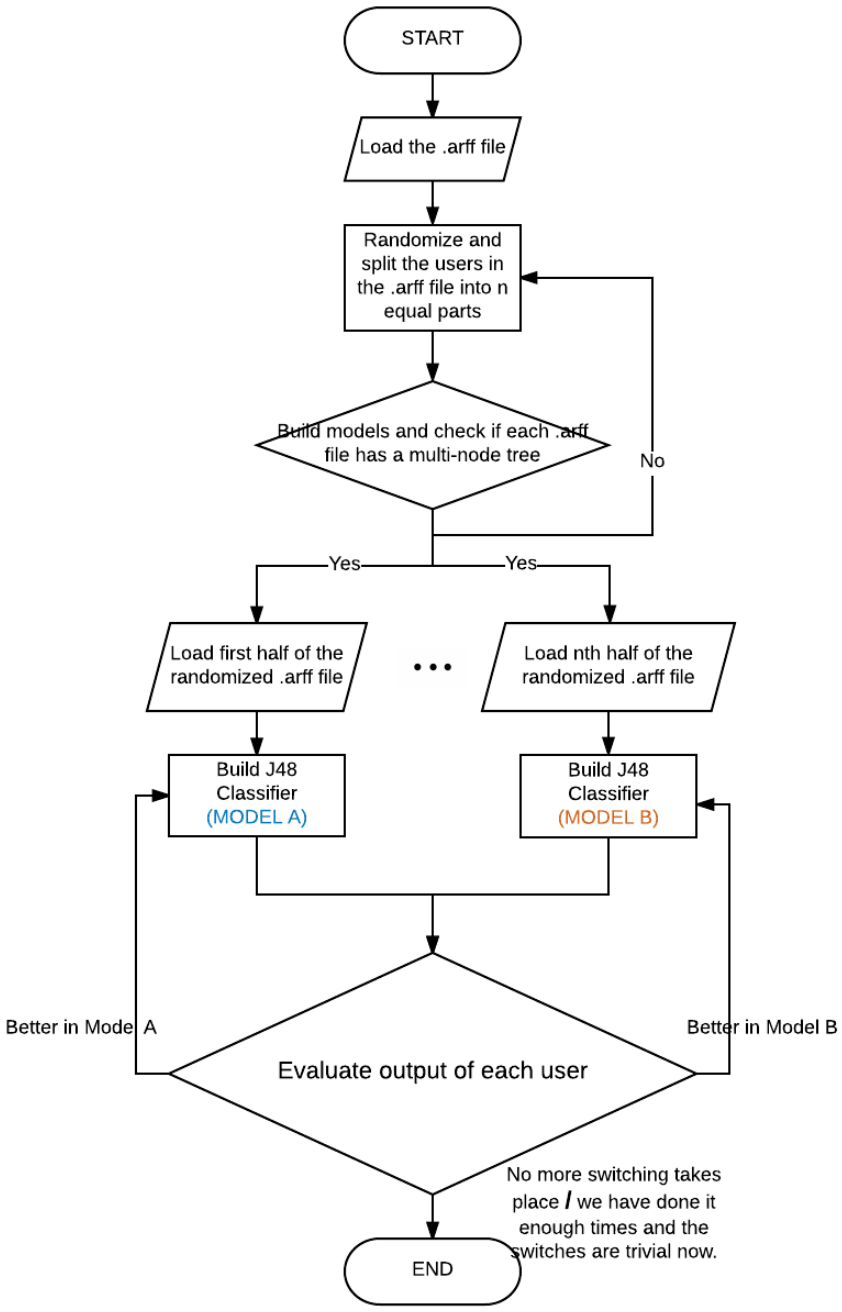


Figure 4.5: The Flow Chart for Fit-based Clustering

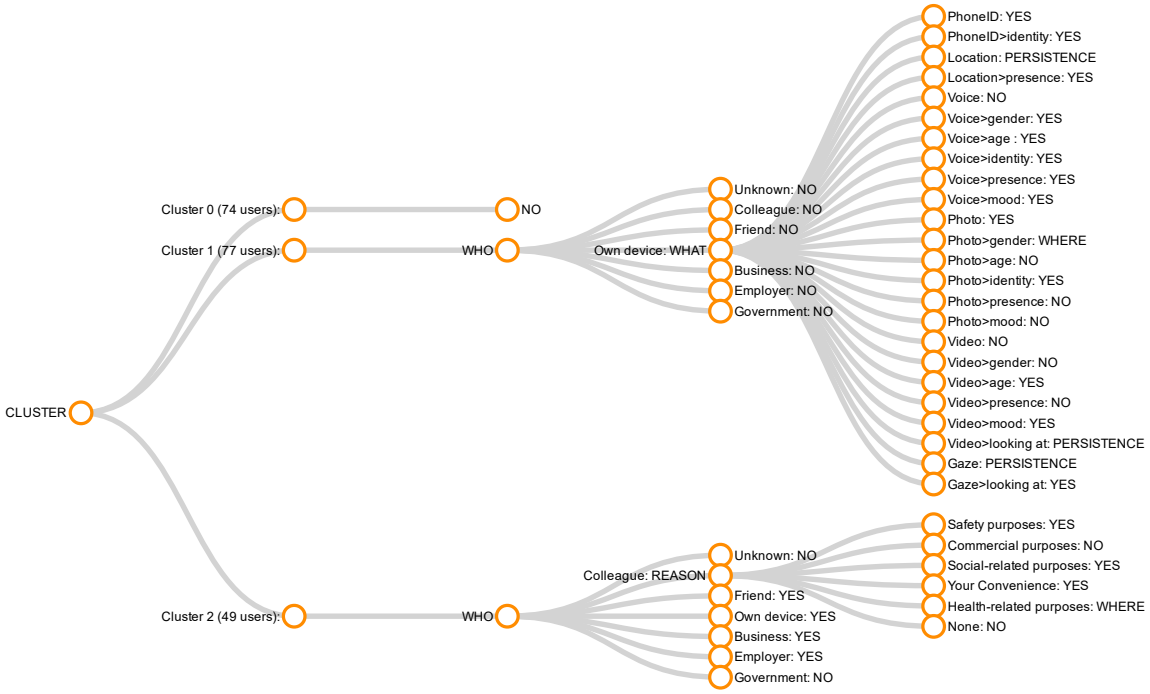


Figure 4.6: Fit-based clustering: 3-cluster tree. Further drill down is hidden for space reasons.

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.

4.3.6 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

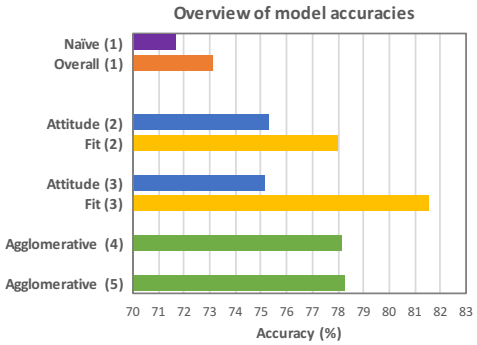


Figure 4.7: Accuracy of our clustering approaches

81.54% of the settings. This rivals the accuracy of some of the "active tracking" machine learning approaches [82].

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.

4.4 Privacy-setting Prototypes (original work)

In Section 4.2, 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 4.3) 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.

4.4.1 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 integrated to this prototype in nature. For "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 '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.

4.4.2 Smart Profiles

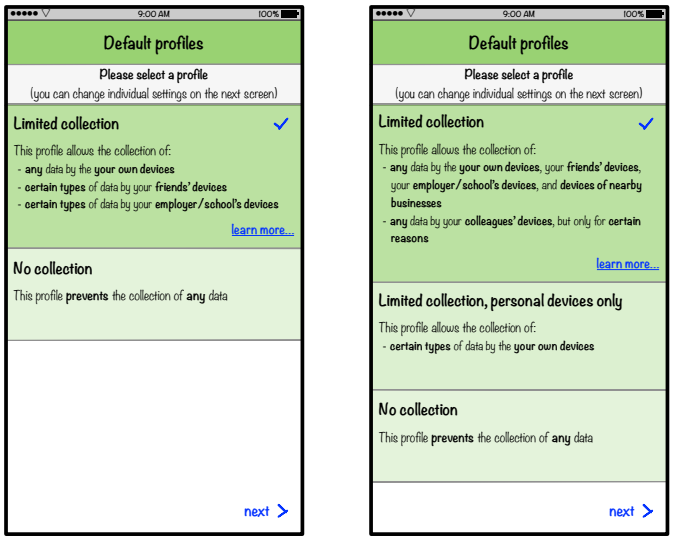
To improve the accuracy of the default setting, we can instead build two "smart profiles", and allow the user to choose among them. Using the 3-cluster solution of the fit-based approach (see Figure 4.6), we can attain an accuracy of 81.54%. Screen 1 in Figure 4.1 shows a selection screen where the user 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), where they can further change some of their settings.

4.5 Summary

In this chapter, we have presented the following:

- Using statistical analysis, uncover the relative importance of the parameters that influence users' privacy decisions. Develop a "layered interface" in which these parameters are presented in decreasing order of importance.



(a) 2-profile choice interface

(b) 3-profile choice interface

Figure 4.8: Two types of profile choice interfaces

- Using a tree-learning algorithm, create a decision tree that best predicts participants' choices based on the parameters. Use this tree to create a "smart default" setting.
- Using a combination of clustering and tree-learning algorithms, create a set of N decision trees that best predict participants' choices. Use the trees to create N "smart profiles".
- Develop a prototype for an IoT privacy-setting interface that integrates the layered interface with the smart default or the smart profiles.

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 [57] 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.

Our analysis allowed us to use *data-driven design* to bootstrap the development of a privacy-setting interface, but a future user experiment could investigate whether users are comfortable with the layered interface, and whether they prefer a single "smart default" setting or a choice among "smart profiles".

In the next chapter, we discuss the challenges and solutions when we extended work that we have done in the domain of household IoT ("smart home") domain.

Chapter 5

Recommending Privacy Settings for Household IoT

In Chapter 4, we have discussed recommending privacy preference for general IoT users. In this chapter, we present the work completed to date in the areas 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 [68].

5.1 Experimental Setup

In Chapter 4, we found that "where" does not have significant effect on disclosure decisions; also the usage environment of household IoT systems/devices are always in users' home. 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, where encounters are often ephemeral, hence persistent tracking is less common than in household IoT. "Storage" and "Action" allow us to explore secondary uses of the information; something we

learned from the qualitative feedback in our previous study was a prominent concern among users.

Because of the above reasons, we conducted 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. In this section, we first discuss the factorial procedure by which we developed 4608 highly specific IoT scenarios, as well as the questions we asked participants to evaluate these scenarios. We then describe the participant selection and experimental procedures used to collect over 13500 responses from 1133 participants.

5.1.1 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 5.1.2). An example scenarios 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 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 of 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 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. 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.

5.1.2 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.

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).

5.1.3 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. Participation was restricted to Mechanical Turk workers with a high reputation (at least 50 completed tasks 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

Table 5.1: Parameters used to construct the information-sharing scenarios. The "codes" are used as abbreviations in graphs and figures throughout the paper and the Appendix.

Parameter	**Levels**	**Code**
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

participants over 60 years old (5 participants did not disclose their age). This significant increase in participants over the Lee and Kobsa [57] dataset is commensurate with our expectation of more complex privacy decision behaviors in household IoT compared to public IoT.

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. If they got any of these questions wrong, they would be asked to read the transcript of the video and re-answer the questions.

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 13 scenarios had an additional attention check question (e.g., "Please answer this question with Completely Agree", 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. Participants rushing through the experiment and/or repeatedly failing the attention check questions were removed from the dataset.

5.2 Statistical Analysis

Our statistical analysis shows that unlike results from [8], 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, which separated 'Device/Sensor Management' and 'Data Storage & Usage', for users to manually change their privacy settings.

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

We also analyze the effects of defaults and framing. As outlined in section 5.1.2, 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.

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.

5.3 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 longer-term (*Actions*).

Based on our statistical analysis in 5.2, 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 5.1) 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.

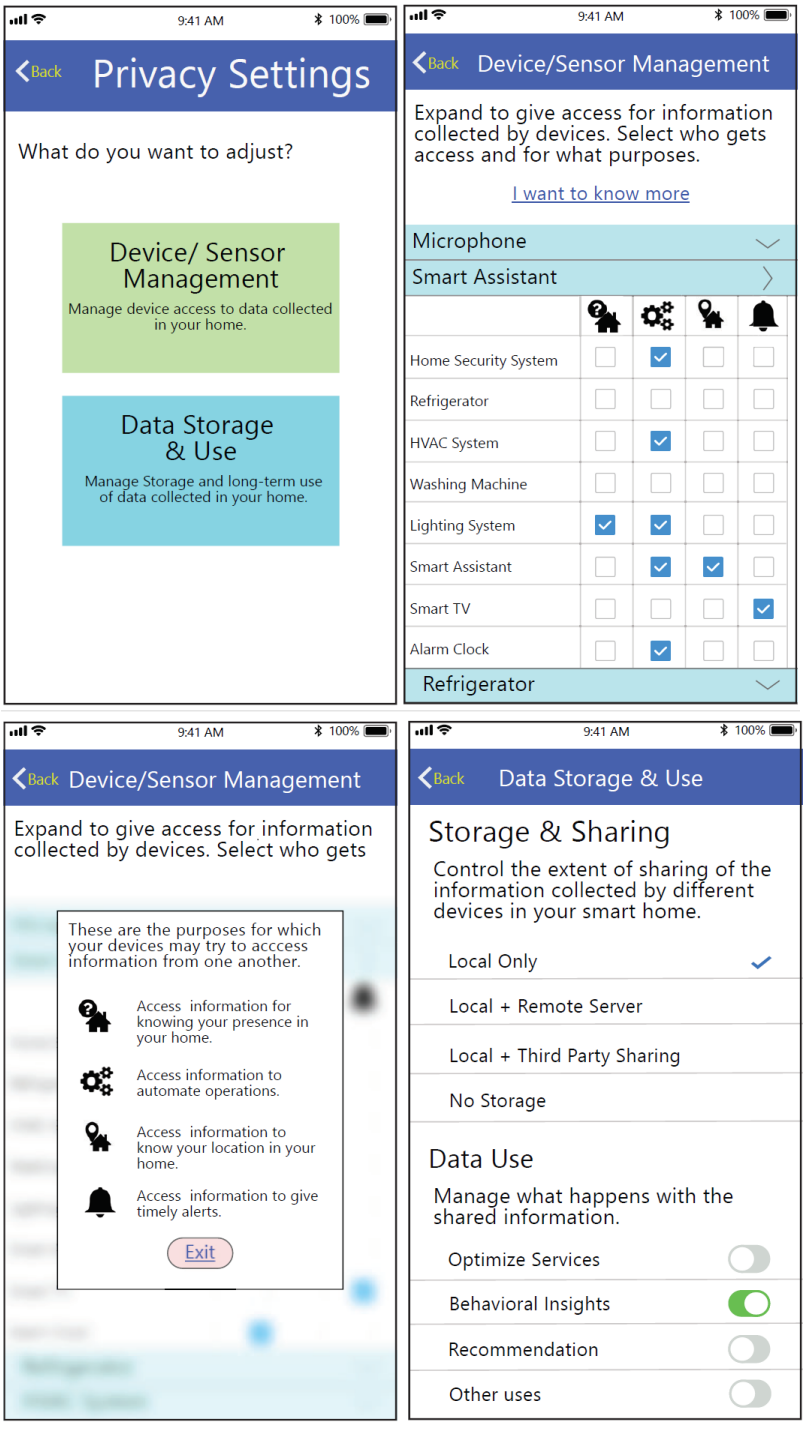


Figure 5.1: Screen 1 (top left) is the landing page of our manual settings interface, screen 2 (top right) is the Device/Sensor Management page, screen 3 (bottom left) shows the explanation when you click on "I want to learn more", and screen 4 (bottom right) is the Data Storage & Use page.

Device/Sensor Management: This screen (Figure 5.1, 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 5.1, 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'.

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 5.1, screen 3).

Data Storage & Use: This screen (Figure 5.1, 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 5.5 revisits the interface designs presented here.

5.4 Predicting users' behaviors (original work)

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

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 [110] 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 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 5.5, 5.7, 5.10 and 5.14 throughout the paper, and combined in Figure 5.18.

5.4.1 Naive Prediction Model

We start with the naive or "information-less" predictions. Compared to our previous work [8], 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 setting disallows any 'smart home' functionality by default—arguably not a solution the producers of smart appliances can get behind.

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. 5.2)	1	1	3	61.39%
Overall (Fig. 5.5)	1	1	8	63.32%
	1	1	264	63.76%
Attitude-based clustering (Fig. 5.7)	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. 5.10)	1133	4	2	79.4%
	1133	5	2.4	80.35%
	1133	6	3.17	80.60%
Fit-based clustering (Fig. 5.14)	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%

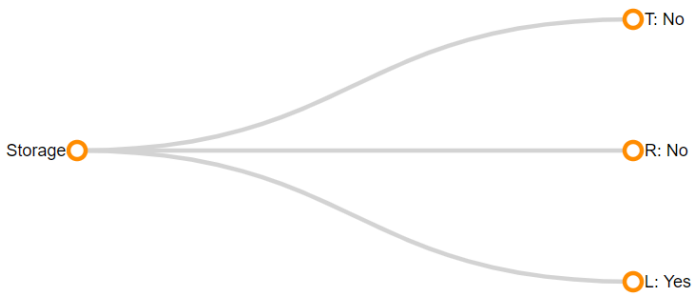


Figure 5.2: A "smart default" setting based on the "One Rule" algorithm (4 nodes, accuracy: 61.39%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

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

5.4.2 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 [42]. 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 5.2, 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[2] over the naive "disable all" default. Note, though, that this default setting is overly permissive, with 3262 false positive predictions (see Table 5.3).

5.4.3 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 5.3, this model predicts users' decision on **Storage** first. It predicts *disable* for every scenarios with collected data stored on a remote

[2] 61.39 / 53.26 = 1.153

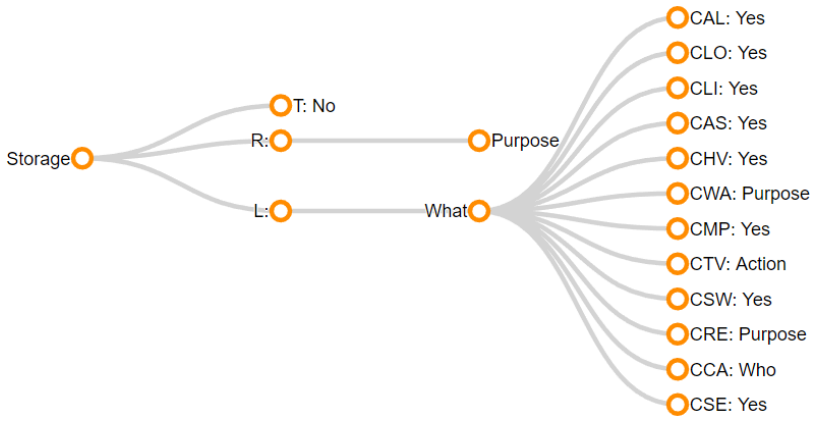


Figure 5.3: A "smart default" setting with 264 nodes (accuracy: 63.76%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

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

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 [8] 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

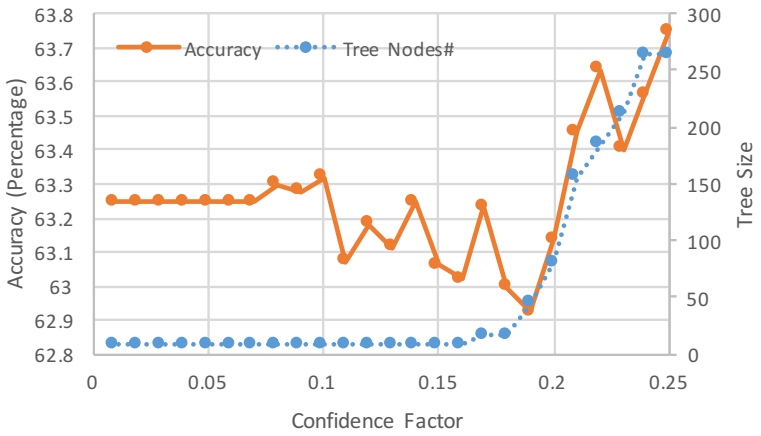


Figure 5.4: Accuracy and parsimony (tree size) of the smart default change as a function of Confidence Factor

resulting "smart default" setting. The parameter used to alter the amount of post-pruning performed 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 5.4 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 5.5 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 8 nodes incurs a negligible 0.67% reduction in accuracy. This decision tree is shown in Figure 5.6, 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:

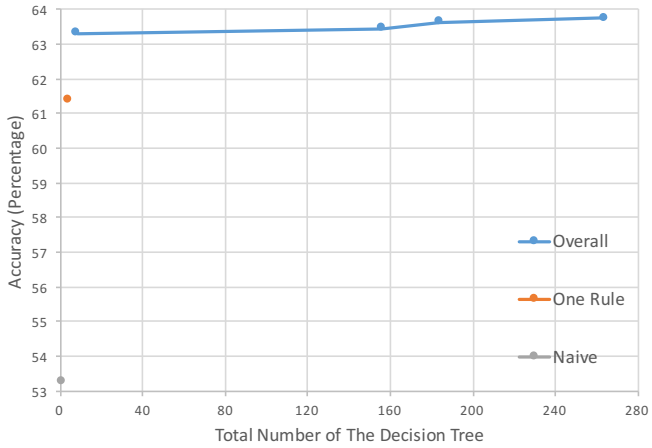


Figure 5.5: Parsimony/accuracy comparison for Naive, One Rule, and Overall Prediction

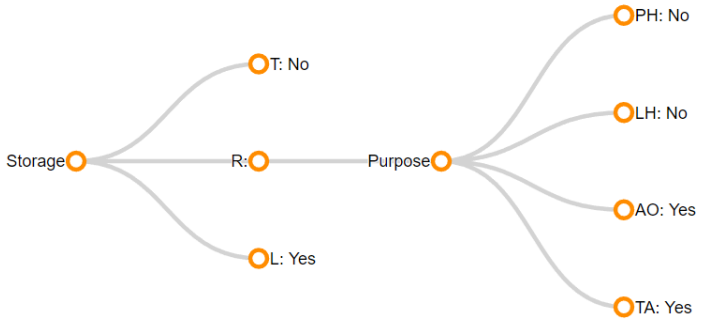


Figure 5.6: A "smart default" setting with only 8 nodes (accuracy: 63.32%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

- 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 [52]. As a result, our "one-size fits all" default setting—smart as it may be—is not very accurate. Recent work in the field of privacy suggest to *tailor* the privacy settings to the user to accommodate for these interpersonal differences [51]. Our previous work therefore moved beyond

"smart default" settings by clustering participants with similar privacy preferences and creating a set of "smart profiles" covering each of the clusters [8]. 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.

5.4.4 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). 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 5.7, which displays the most accurate solution for any given tree size and number of clusters.

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 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 5.7), 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 5.8). 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 5.7), 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

Figure 5.7: Parsimony/accuracy comparison for attitude-based clustering

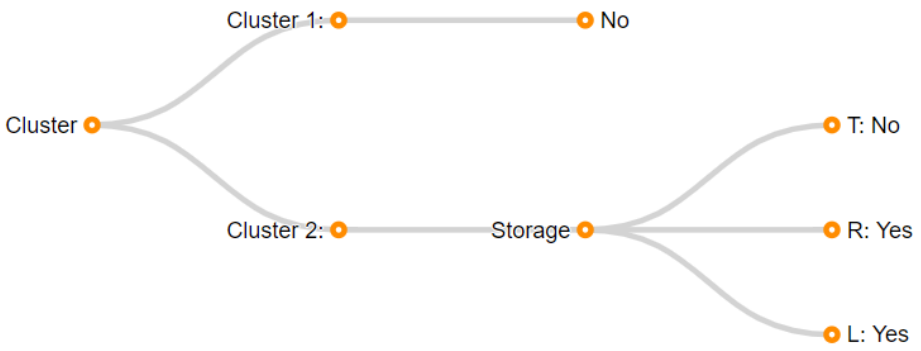


Figure 5.8: The most parsimonious 2-profile attitude-based solution (2 nodes/profile, accuracy: 69.44%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

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 5.6). This solution has an accuracy of 72.19%, which is a 4.0% increase over the most parsimonious 2-cluster solution.

The 4-cluster solutions (the grey line in Figure 5.7) 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 5.7) 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 5.7 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 5.9: 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).

5.4.5 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 agglomer-

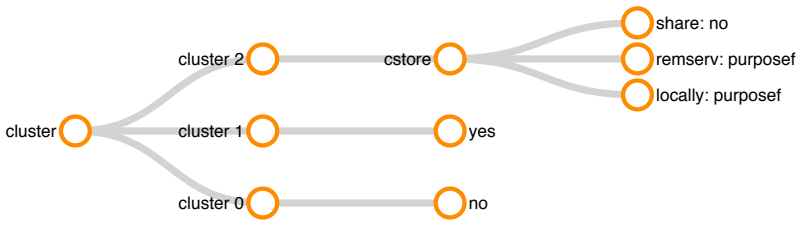


Figure 5.9: A 3-profile solution example of attitude-based clustering (18.33 nodes/profile, accuracy: 73.26%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

ative) 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 [8] 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 5.10). This suggests that without extensive trimming, our agglomerative 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 5.11:

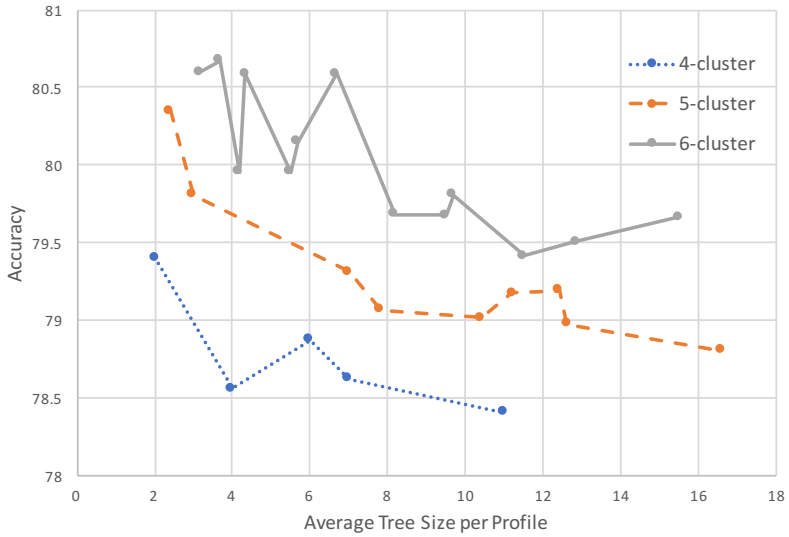


Figure 5.10: Parsimony/accuracy comparison for agglomerative clustering

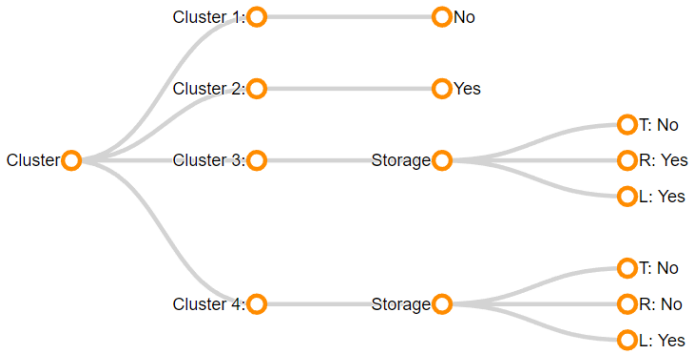


Figure 5.11: The best 4-profile agglomerative clustering solution (2 nodes/profile, accuracy: 79.40%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

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-cluster agglomerative solution. The decision trees are shown in Figure 5.12: 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[3] has an average of 3.17 nodes per profile and an accuracy

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

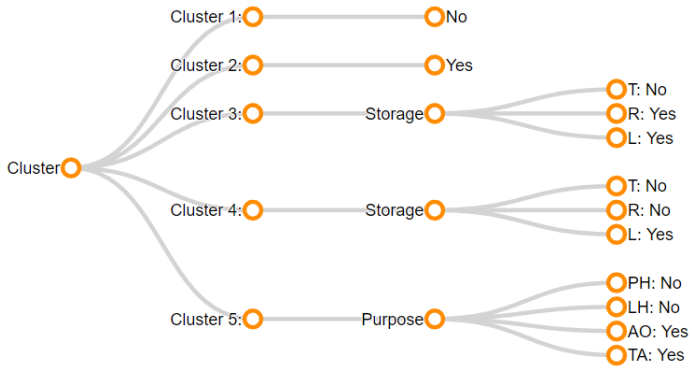


Figure 5.12: The best 5-profile agglomerative clustering solution (2.4 nodes/profile, Accuracy: 80.35%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

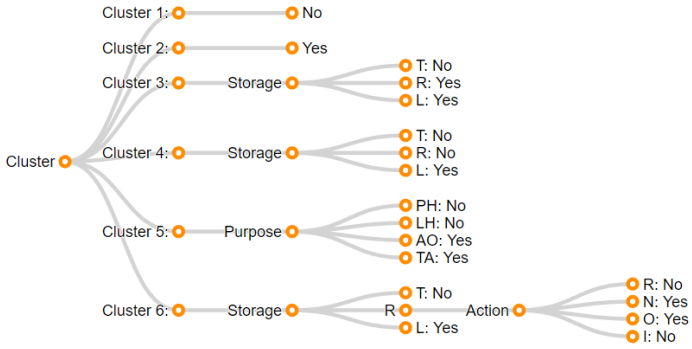


Figure 5.13: The best 6-profile agglomerative clustering solution (3.17 nodes/profile, Accuracy: 80.68%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

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 5.13: 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).

5.4.6 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 steps of our algorithm are as follows:

- **Random starts:** We randomly divide participants into k separate groups, and learn a tree for

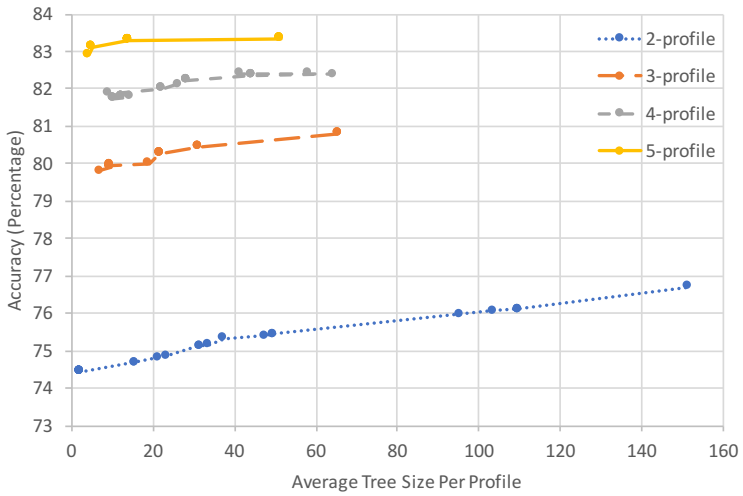


Figure 5.14: Parsimony/accuracy comparison for fit-based clustering

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 5.14.

For the 2-cluster solutions (the blue line in Figure 5.14), 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

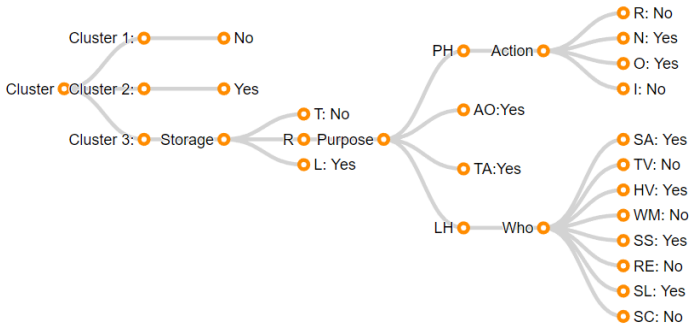


Figure 5.15: The most parsimonious 3-profile fit-based solution (7 nodes/profile, accuracy: 79.80%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

attitude-based solution (see Figure 5.8), but with a higher accuracy (74.43%).

For the 3-cluster solutions (the orange line in Figure 5.14), 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 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 5.15.

For the 4-cluster solutions (the grey line in Figure 5.14), 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 5.16.

For the 5-cluster solutions (the yellow line in Figure 5.14), 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 5.17.

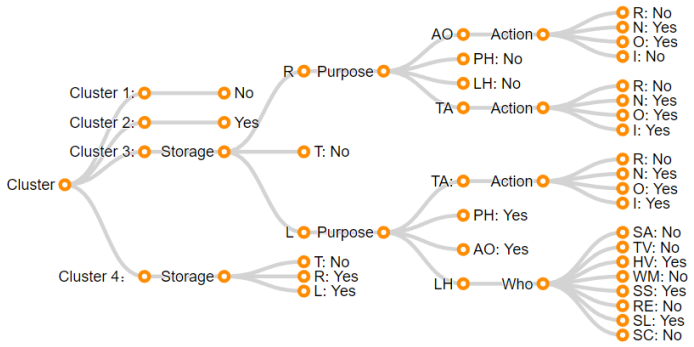


Figure 5.16: The most parsimonious 4-profile fit-based solution (9.25 nodes/profile, accuracy: 81.88%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

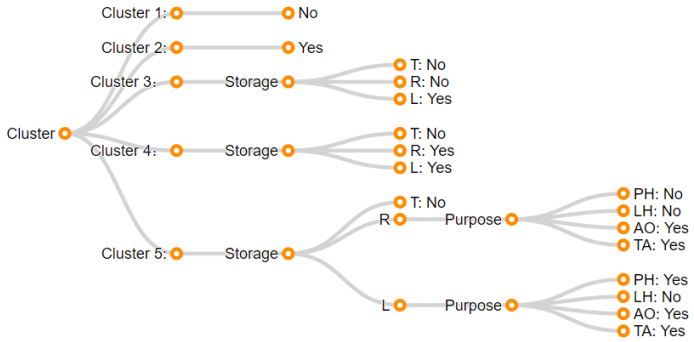


Figure 5.17: The most parsimonious 5-profile fit-based solution (4.2 nodes/profile, accuracy: 82.92%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

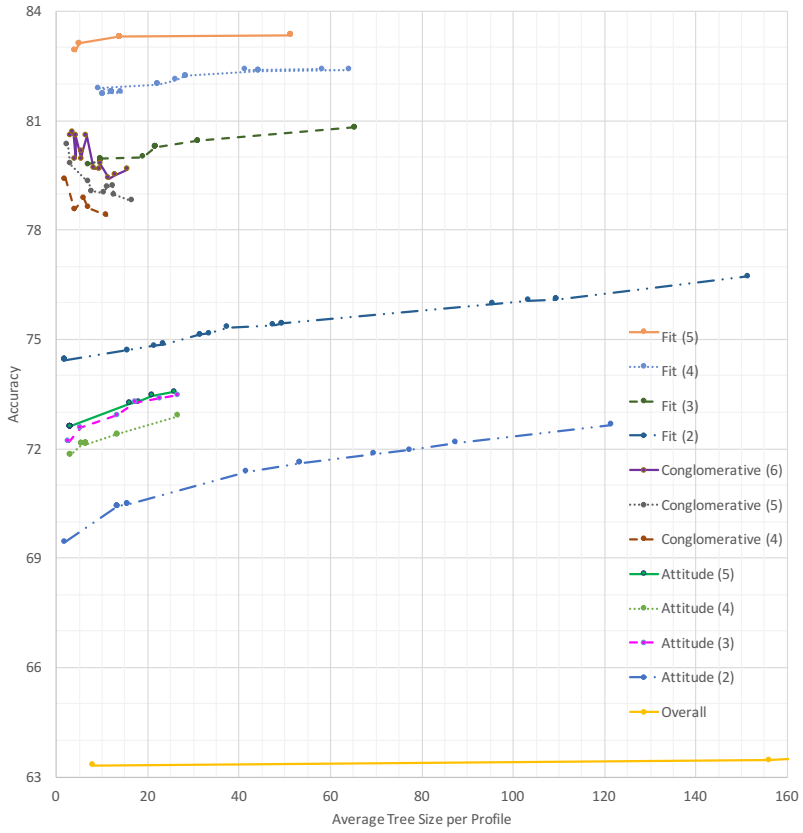


Figure 5.18: Summary of All our Approaches

5.4.7 Discussion of machine learning results

Figure 5.18 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 5.1) these defaults are incredibly easy for users to implement by themselves.

The same is true for the 4-profile agglomerative clustering solution (see Figure 5.11) and the 5-profile agglomerative clustering solution (see Figure 5.12): 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 5.17) 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 5.19. 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.

Other usable solutions are the 3-profile fit-based solution (Figure 5.15) or the 4-profile fit-based solution (Figure 5.16. 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.

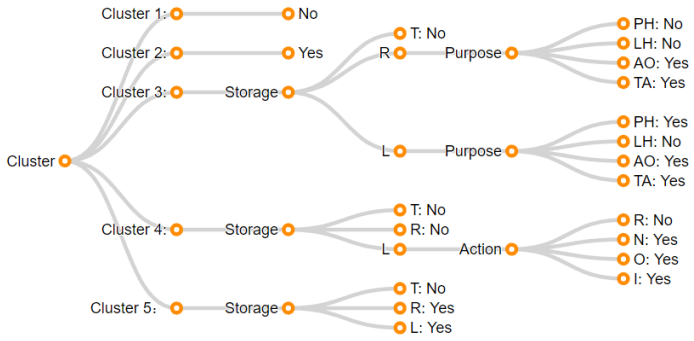


Figure 5.19: A good 5-profile fit-based clustering solution (5 nodes/profile, Accuracy: 83.11%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

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

In Section 5.3 we developed a prototype interface that household IoT users can use to manually set their privacy settings (see Figure 5.1). Our machine learning analysis (Section 5.4) 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). 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 5.17 and 5.19).

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.

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

This machine learning solution (Figure 5.17) requires an interaction between the *Storage* parameter and the *Purpose* parameter—two parameters that are controlled independently in the

prototype in Figure 5.1. Our solution is to slightly alter the interface, and add the profile selection page at the beginning of the interface (see Figure 5.20):

- **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*).

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

The alternative machine learning solution presented in Figure 5.19 requires an additional interaction between the *Storage* parameter and the *Action* parameter. This requires us to slightly alter the interface again (see Figure 5.21):

- **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'.

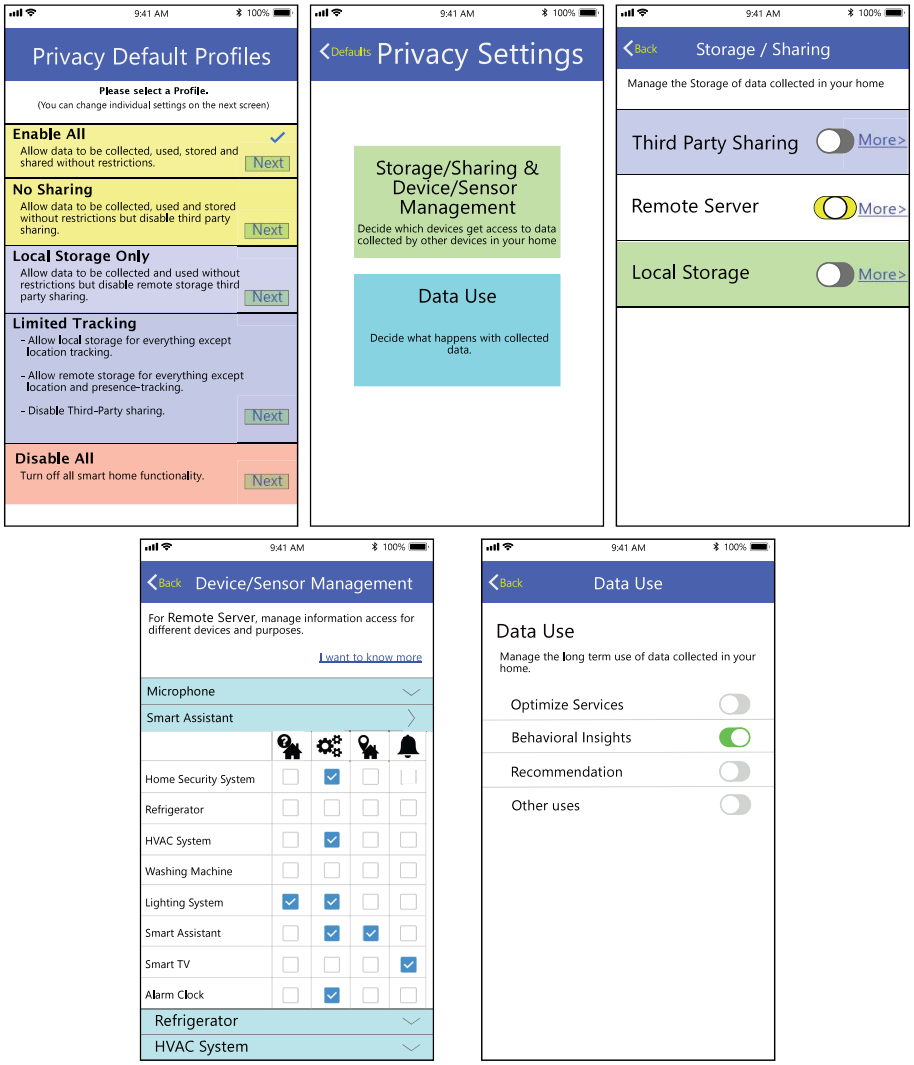


Figure 5.20: Design for 5-Profile solution presented in Section 5.5.1. From top left, screen 1 is the profile selection page, screen 2 is the slightly altered landing page of our manual settings interface, screen 3 is the slightly altered Data Storage page, screen 4 (bottom left) is the Device/Sensor Management page, and screen 5 is the Data Use page.

- **Screen 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.

5.5.3 Reflection on design complexity

The interfaces presented in this section have an additional 'layer' compared to the original interface presented in Section 5.3. 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 5.4 are not only more difficult to explain to the user, they also contain 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.

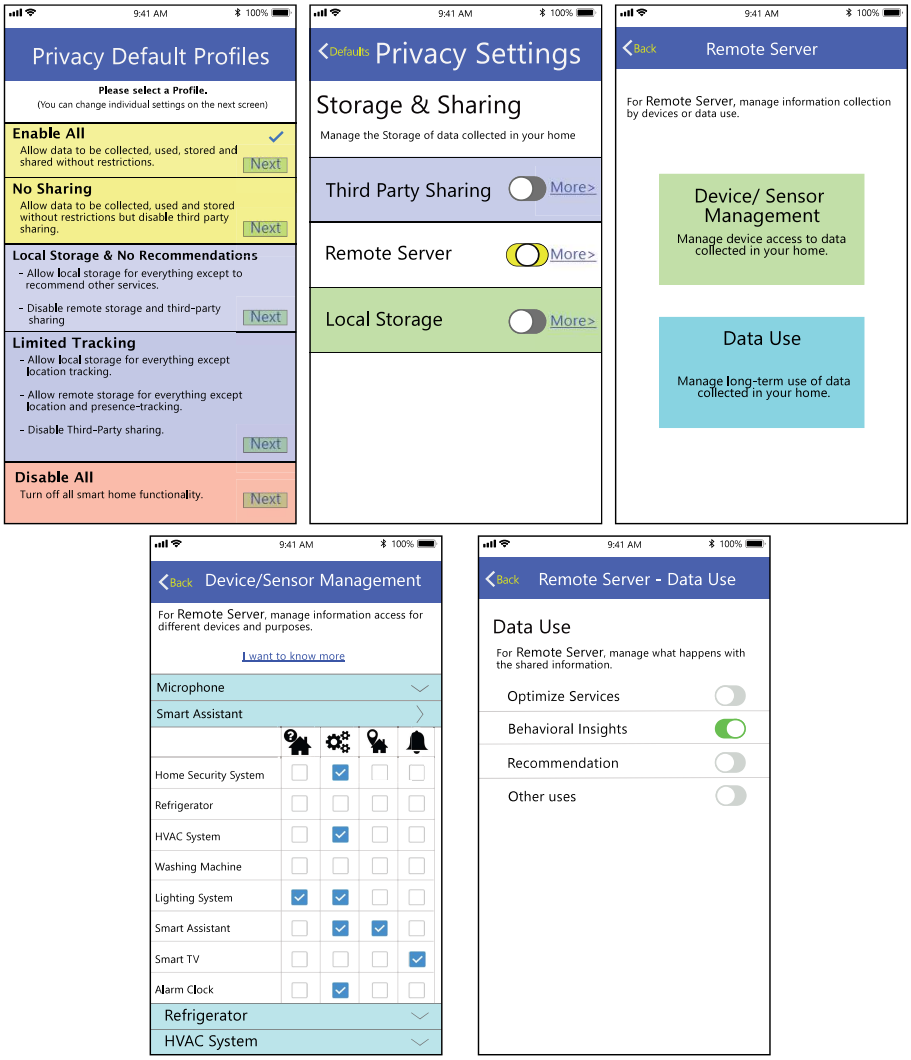


Figure 5.21: Design for 5-Profile solution presented in Section 5.5.2. From top left, screen 1 is the profile selection page, screen 2 is the slightly altered Data Storage page, screen 3 follows the 'More' button to offer access to screen 4 (bottom left, the Data Use page) and screen 5 (bottom right, the Device/Sensor Management page).

Chapter 6

Recommending Privacy Settings for Fitness IoT

In Chapter 5, we have discussed recommending privacy preference for household IoT users. In this chapter, we present the work completed to date in the areas of recommending privacy for Fitness IoT.

Wearable fitness trackers are undoubtedly gaining popularity. As fitness-related data are persistently captured, stored, processed and shared by these devices and related services, the issue of privacy management is becoming increasingly urgent both for the user and the service, which has to respect privacy law, including the new European Union's General Data Protection Regulation (GDPR). This concerns all third parties that manage user data and has of course a major impact on personalization services.

Previous studies in mobile privacy (e.g.,[28]) have proven that mobile interfaces lack the potential to provide the necessary user privacy information and control for both Android and iOS systems [62]. Several solutions from literature have been proposed from then on to improve mobile privacy protection and offer users more privacy control (e.g., [11]). These leads into rapid improvement of privacy management of current mobile systems (i.e., from Android 6.0+ and iOS 5.0+), providing more control on the user's privacy settings.

As of May 25, 2018, the European Union (EU) enforce the General Data Protection Regulation (GDPR) [91] which applies to the storage, processing and use of the subject's personal data

from the TPs 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 TPs. This results in a complex task for the users given the number of devices and applications which have to be read and processed specifically.

6.1 Data Model

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

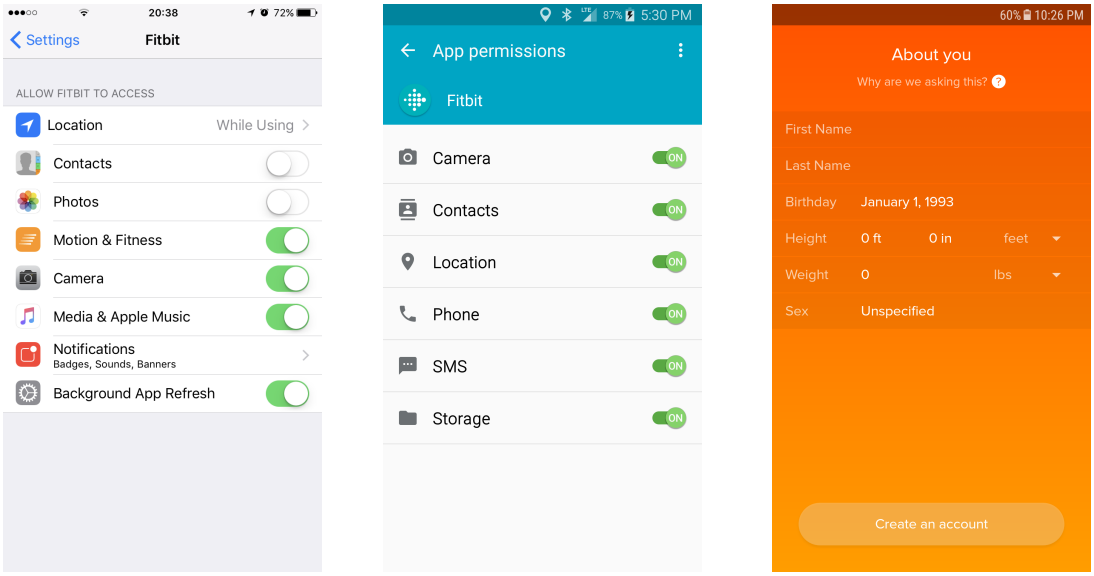
By examing the permission questions from the mainstream fitness trackers (Fitbit, Garmin, Jawbone, and Misfit), we categorize these questions into 3 groups – *Smartphone Persmission*, *In-app Requests*, and *FItness Data*, as shown in Table **??**.

6.1.1 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 **??** and **??**, 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).

6.1.2 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 **??** when signing up an account during the first-time using the mobile App. Note that these data are mandatory for all fitness trackers in Table **??**; the only optional piece of information is Misfit's request on users' occupation. Figure 6.2d shows the *A set* for the Fitbit app (other apps are similar), as reported in Table **??**.



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

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

(c) The interface of In-App permissions of Fitbit Android App

Figure 6.1: Interface examples of permission requests for Fitbit fitness trackers

6.1.3 The F set (fitness data)

The F set contains the data fitness trackers collect while the user is using the device. Some of this data is automatically collected by the tracker (e.g., steps, distance) and shared with the device's own fitness tracking app (e.g. the Fitbit device shares fitness data with the Fitbit app), while the user has to enter other data manually into the app (e.g., food and water logs, friend list).

While this data is "shared" with the native fitness tracker TP by default (since this TP serves as the collecting TP), most trackers have an API that allows users to further share this data with other TPs in exchange for additional fitness or health services the user can benefit from. This data sharing was modeled in [**?**] together with its associated risks. Table **??** shows the data that can be shared to other TPs from the four considered fitness apps. In this comparison, Fitbit gives the users more granular control over which of the fitness data can be shared with other TPs through their API, as shown in Figure **??**[1]. Additionally, these settings can be revisited in their web app[2], where users have the option to revoke the granted access. The other apps in Table **??** also give users control, but only give users the option to allow/deny the other TP access to the entire F set. We follow Fitbit's permission model for this set but give users even more fine-grained control over

[1] `https://dev.fitbit.com/build/reference/web-api/oauth2/`
[2] `https://community.fitbit.com/t5/Flex-2/How-do-I-revoke-access/td-p/2701359`

Activity and Exercise data, breaking these permissions down into steps, distance, elevation, floors, activity minutes, and calories activity. We implement this additional granularity because these data involve a particular inference risk, potentially exposing some of the other data in this set [**?**]. A total of 14 permissions are included in the F set.

Note that the F set permissions are repeated for *each additional TP* that requests access to this data. As such, these permissions are not for the native app of the fitness tracker, but for other TP apps that the user desires to use and allow access to her/his fitness tracking data. In this study, instead of taking into account individual TPs, we use the PPIoT *EntityType*, discussed in Section **??**, to investigate which group category of TP apps (namely "who") the user prefers to share with. This parameter has been shown to be important in determining users' privacy settings [**?**]. Since Entity Types are intimately related to GDPR-based requirements, these permissions are included in the G set.

6.1.4 G Set (GDPR-based permissions)

The G set includes permissions that are based on GDPR requirements. We report the exact terms used in PPIoT to unambiguously represent these permissions. 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*.

The types of TPs (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*.

We did not include the *hasMethod* property since it involves technical background, as stated in Section **??**, which may not be known to the users. For simplicity, we assume that the TPs' *hasMethod* data access are *encrypted*.

6.1.5 A Conundrum of Settings

We note that Fitbit asks for a staggering total of 24 permissions across the S, A, and F data sets. Our data model, which takes a superset of permissions asked by all four fitness trackers, more granular *Activity and Exercise* data, and the additional G set, includes 45 permissions in total. Moreover, if the user wants to share their fitness data (F set) with one or more additional health or fitness tracking apps, the permissions for this must be decided upon for each additional TP individually.

Most current fitness tracker apps do not ask these permissions in a very clear manner, and the settings are often hard to find in case the user wants to change them. That said, even with a more usable UI for making these settings the sheer number of them is arguably a significant burden to the user and cause of possible errors. This is why we advocate the use of semi-automated interactive *privacy recommendations* to partially relieve users' burden of setting each of these individual permissions and meanwhile maintain the control on privacy preferences.

6.2 Data Collection

To conduct the data collection, a mobile fitness application mock-up, named *FitPro* was developed. FitPro systematically asked for all of the permissions in the Data Model for Fitness IoT that we defined in Section **??**. Participants were asked to set up an new account by providing their information. All the questions at this stage are organized according to our data model discussed in previous section, including 1) In-app permissions, 2) Smartphone permissions, 3) Fitness data permissions, and 4) GDPR-based permissions. After providing answers to these questions, participants were asked to fill our a survey questionnaire. We aimed to measure the users' privacy-related attitudes (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. The questionnaire is shown in Appendix.

A total number of 310 participants were recruited through Amazon Mechanical Turk. After data preprocessing, 295 user samples were utilized. We asked people to only participate if they were active Fitbit users[3], and checked this requirement by asking participants to enter the initial and

[3]We restricted our study to Fitbit users rather than users of any fitness trackers to make sure that our sample had

last few digits of their Fitibit serial number. The participants consisted of 34.2% males and 65.8% females, had mean age of 35, and were generally highly educated (62% had at least a bachelor's degree). We restricted our study to fitness tracker users to detect the real preferences of target users.

6.3 Data Analysis

In this section, we present our data analysis on the data we collected. Figure **??** shows that there is considerable variability in the average rate at which each permission is allowed or denied in our study. The permissions requested by the application (A set), mainly concerning demographics (see Table 1), have a high disclosure rate, which is in line with the results of other studies (cf. [**?**]).

For the smartphone permissions (S set), participants are more likely to allow motion, location, bluetooth, and mobile data. This makes sense, because these are the minimum permissions needed to run a fitness tracker app. In this set, the permission to access photos or contacts is granted much less often.

Regarding the purpose, frequency and retention period of data collection (G set), participants seem most open to data collection for health (the main purpose of a fitness tracker) and safety (another purpose often indicated by fitness trackers for continuous location-tracking services). 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.

We do not show the fitness data (F set) in Figure **??** because the permissions for these data are requested for multiple entity types of the G set, as discussed in Section 6.1.3. Hence, we present these data in Figure **??** instead, showing each permission for each GDPR *EntityType*. Users are more likely to give permission to their friends on social networks and to other health/fitness apps, and they are less likely to give permission to share their data with government fitness programs or publicly on social media. As for various data types, steps are shared most openly, while location, friends, and weight are shared less openly.

Upon further inspection, we note that participants tend to share either (almost) all or (almost) none of fitness data with an entity. This suggests that Fitness data permissions are more likely to be influenced by the receiver ("who") rather than the specific data item ("what"). As

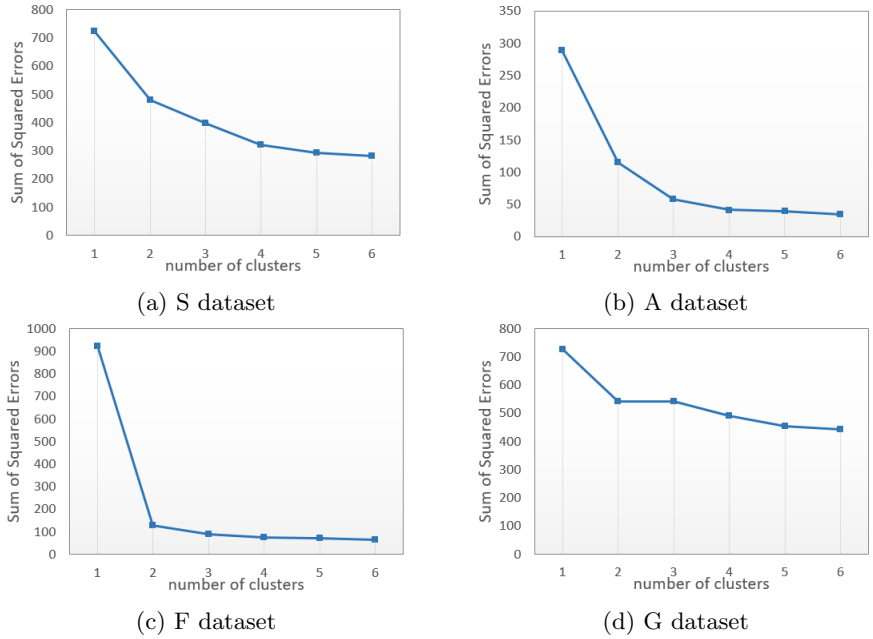
a more homogeneous existing experience with fitness permission-setting interfaces.

discussed in Section **??**, these "who" parameters are instances of the GDPR *EntityType*. Therefore, we expect that clustering F permissions should provide a unanimous deny/share for all items, while clustering G permissions should provide more nuanced clusters of different entity types receiving the data specified in the F set.

6.4 Predicting users' Preference (original work)

We predict participants' *enable/disable* decision using machine learning methods. Our dataset shows considerable variability between participants' privacy preferences—a finding that is broadly reflected in the privacy literature (cf. [52]). 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.

To this end, we cluster participants' permissions with Weka[4] 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.



(a) S dataset (b) A dataset

(c) F dataset (d) G dataset

Figure 6.2: Evaluation of different numbers of clusters for each set.

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

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 the users. A further drawback of clustering the full set of 45 permissions is that it gives large error rates (e.g., the sum of squared error for the viable 4-cluster solution is 1435), for anything but a very large number of clusters.

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 6.2. 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).

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

6.4.1 Clustering Outcomes

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 6.2. Using the elbow method [**?**], we conclude that 2 is the optimal number of clusters for each dataset[5].

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

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

6.4.1.1 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.

6.4.1.2 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.

6.4.1.3 The *F* Set

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

6.4.1.4 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 TPs. Sharing is allowed only for health and safety purposes.

6.5 Profile Prediction (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. This section aims to answer the research question: **RQ3** Are there any privacy profile items or questionnaire items that can be used as a determiner to predict which privacy profile best describes a user?

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 prediction. Since the items are the permission preferences included in the subprofiles, collected through our FitPro prototype app, we call this the "direct predicition" approach. Additionally, we also explored whether the items from our questionnaire (see Section **??**) could drive the predicition. Since these items are not part of the privacy subprofiles, we call this 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 tree learning algorithm. J48 is an efficient and widely used decision tree algorithm that can be used for classification [**?**]. Previous work shows the effectiveness of this approach to predict privacy settings within each cluster [**?**]; here we take the opposite approach and use it to predict cluster assignments instead. In our approach, the J48 algorithm extracts the permission items (for the direct prediction) or questionnaire items (for the indirect prediction) that classify a new user into the correct subprofile with the highest possible accuracy.

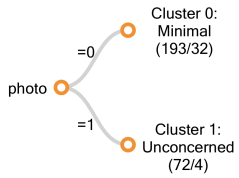
The evaluation of all developed J48 trees was performed using k-fold cross validation.

6.5.1 Direct Prediction Questions

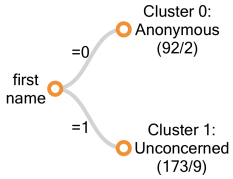
In our direct prediction approach, the aim is to ask users to answer certain permission items from each subset as a means to classify them into the correct subprofile (thereby providing a recommendation for the remaining items in that subset). For this approach, we thus classify users using the items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

Our results for this approach are reported in Figure 6.3. It shows for each subset the question that best classifies our study participants into the correct subprofile.

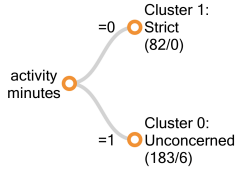
When running tree-based algorithms, a trade-off has to be made between the parsimony and the accuracy of the solution. Parsimony prevents over-fitting and promotes fairness [**?**] and can be accomplished by pruning the decision trees. In our study, while multi-item trees may provide better predictions, the increase in accuracy is not significant compared to the single-item trees presented



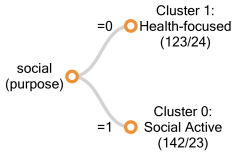
(a) S set (86.42%)



(b) A set (95.85%)



(c) F set (97.74%)



(d) G set (82.26%)

Figure 6.3: The permission drivers for the privacy subprofiles and their respective prediction accuracies.

in Figure 6.3. 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 **??**), 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.

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 **??**.

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"

subprofile. The question really fits the G set since GDPR permissions are mostly about handling the user information by the TPs. 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 **??**.

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 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 **??** 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 TPs 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 TPs, even if the risk decreases.

For the G set, users who share their fitness app Profile with other TPs 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 tree 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 [**?**], 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 6.4 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 6.3 to **??**), and take the form of (# assigned / # incorrect).

6.6 Privacy-setting Recommendations (original work)

In this section, we describe different types of guided privacy-setting approaches for IoWT users that are based on the previous clustering and tree-learning results. When implemented in the PDM, the guided interface simplifies the privacy-setting experience by providing privacy recommendations. This answers **RQ4**: How can we effectively exploit the results to provide recommendation? The PDM design prototype implementing the recommendation strategies is available online[6].

6.6.1 Manual Setting

The baseline privacy settings interface is one where users have to manually set their settings (see Figure **??**). 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

[6]The UI design can be found in `http://pdm-aids.dibris.unige.it/interface/`

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 (cf. [66]), 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 **??**). Figure **??** 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 (cf. [52]). 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 **??** shows the subprofile selection interface for the S set. Users can choose either the ''Minimal" or "Unconcerned" subprofile, which are shown in Figures **??** and **??** respectively. Similar interfaces are provided for the F, A, and G sets (not depicted here).

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 will have to 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 **??**. 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 **??**, 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 6.5 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 **??**. 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 **??** in Appendix.

6.8 Conclusion

In this chapter, we presented a data-driven approach to develop recommendation strategies for supporting users to set permissions on their personal data collected and shared by tracking devices in the fitness domain.

The motivating issue is the complex scenario of data sharing among devices and Third Party applications in the Internet-of-Wearable-Things (IoWT), which makes setting one's privacy preferences an increasingly complex task. The goal is to balance the users' control over their data and the

simplicity of setting, in the light of the GDPR (General Data Protection Regulation) requirements.

First, we defined a data model of privacy preferences for the fitness domain that can be represented using our PPIoT (Privacy Preference for Internet of Things) Ontology. The data model is based on the whole set of permissions required by the most popular fitness trackers and includes the permissions specified in the GDPR.

In our approach, we use the Semantic Web to define a semantic layer that aims to provide unambiguous and formal representation of the user's privacy preferences, regardless of the diverse representations used by the TPs themselves. The PPIoT ontology is part of our Personal Data Manager (PDM) framework which is the intended testbed for the recommendation strategies of privacy preferences that we propose in this paper.

Despite the vast variation in user privacy preferences, we managed to find a concise set of relevant privacy profiles that are able to represent these preferences. With two subprofiles for four subsets of permissions (sets S, A, F and G in the paper), a total of 16 possible privacy profiles can be recommended to the user. Additionally, we managed to determine specific subprofile items ("direct prediction") and questionnaire items ("indirect prediction") that serve as predictors for these profiles.

Our results also show interesting semantic relationships between predictors and privacy settings. In particular, users' tendency to make friends while using the fitness tracker is a significant predictor that they accept smartphone data permission requests (the S set), answer in-app requests (the A set), and share their fitness tracking data (the F set).

This study also found that in sharing fitness tracking data, users care more about "who" will receive that data rather than "what" data is shared specifically. This confirms previous studies [57, **?**] showing no significant interaction between these two parameters. Initial results also show that knowledge about users' actions when risks decrease is more useful to give good recommendations than knowledge about users' actions when benefits increase. Finally, we proposed different recommendation strategies and related user interfaces for supporting users to set their privacy permissions. They include a fully manual approach, as well as interactive prediction-based recommendations that are based on our clustering and classification results. Users can interact with the user interface by answering the "trigger questions" that are selected by our classifiers as predictors of users' subprofiles. These recommendation approaches are aligned with the PPIoT ontology: the data model vocabularies and the recommendation strategies will be used by the PDM to model the user privacy

preferences and support privacy settings.

Even though several works exist on privacy preference modeling, this paper makes a contribution in modeling privacy preferences for data sharing and processing of tracked data in the IoT and fitness domain, with specific attention to GDPR compliance. Moreover, the identification of well-defined clusters of preferences and predictors of such clusters is a relevant contribution for the design of recommendation strategies and interactive user interfaces that aim to balance users' control over their privacy permissions and the simplicity of setting these permissions.

In this light, our main contribution is a generic method to develop user profiles and a series of recommendation strategies for privacy management that can be applied to any user-tailored privacy decision-support systems that model and manage the user privacy permissions, like our PDM. Our main contribution in this light is a process that can be used for the identification of privacy profiles and predictors of these profiles. Such predictors include privacy setting preferences (direct prediction) but also, and more interestingly, some user traits (indirect prediction): users' privacy attitudes, the negotiability of their preferences, and social influence.

One of the main limitations of our work is the fact that the recommendation strategies are static: they do not update automatically based on new input. A dynamic recommender has some drawbacks, though: if the recommender is to update predictions for the *current user* based on their feedback, it has only very limited opportunities to do so, since the interaction consists of only four screens (unlike a typical recommender system, where users have continual interactions with the system). Likewise, if the recommender is to learn from each user and recalculate the recommendations for *subsequent users*, it means that the system needs some sort of centralized learning component where all users' privacy preferences are stored. This in itself requires that users agree and give their permissions for their privacy preferences to be stored and processed.

As such, our aim is to study which tracking data are viable for determining the right recommendation in a simplified manner. For future refinements, we plan to use dynamic cognitive environment techniques (e.g., Dynamic Bayesian Filtering, Kalman Filtering, PhD filtering, etc.) that provide update steps to extend our static approach. Moreover, for future refinement we plan also to combine direct recommendation and indirect recommendation, which are currently two different strategies that result from our study.

With regard to the PPIoT ontology, while its logical consistency has been evaluated using Jena Semantic Web reasoner, we are currently working on extending the use case scenarios in order

to comprehensively evaluate its feasibility to model the user and TP privacy preferences in the IoWT.

Another limitation of our 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 is another suggestion for future work. The user study should also evaluate the user control provided by the PDM.

Last, we discuss a limitation of our dataset. The permission settings that we collected could be biased by the fact that the subjects knew it was a simulation of an app privacy setting. In order to reduce this possible effect, the interaction design and the user interface of the app were made very realistic and we asked users to behave like when they usually install an app.

With the limitations discussed above, our results could be immediately integrated in personalized services in the fitness domain. In fact, our data model for the fitness domain has a wide coverage of tracking data that should likely include those used by personalized fitness service. As argued, though, this approach can also be applied to other IoT scenarios (e.g. household IoT, public IoT), or even other complex privacy situations (e.g., social networking, online shopping) as well. We encourage researchers to adopt and further extend this "User-Tailored Privacy" approach (cf. [50]) in their own work.

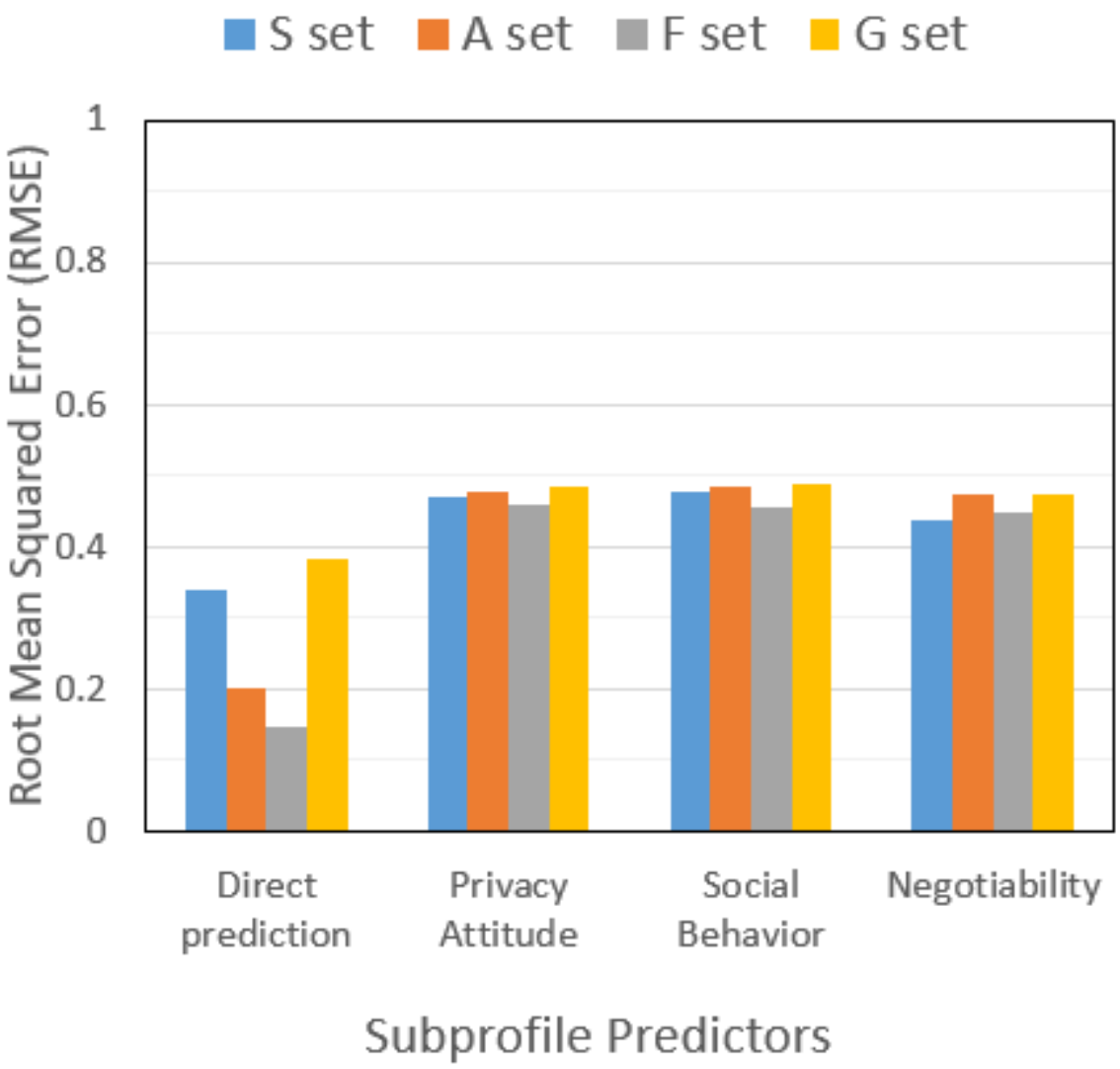


Figure 6.4: Tree evaluation. Root mean square error for each J48 tree algorithm.

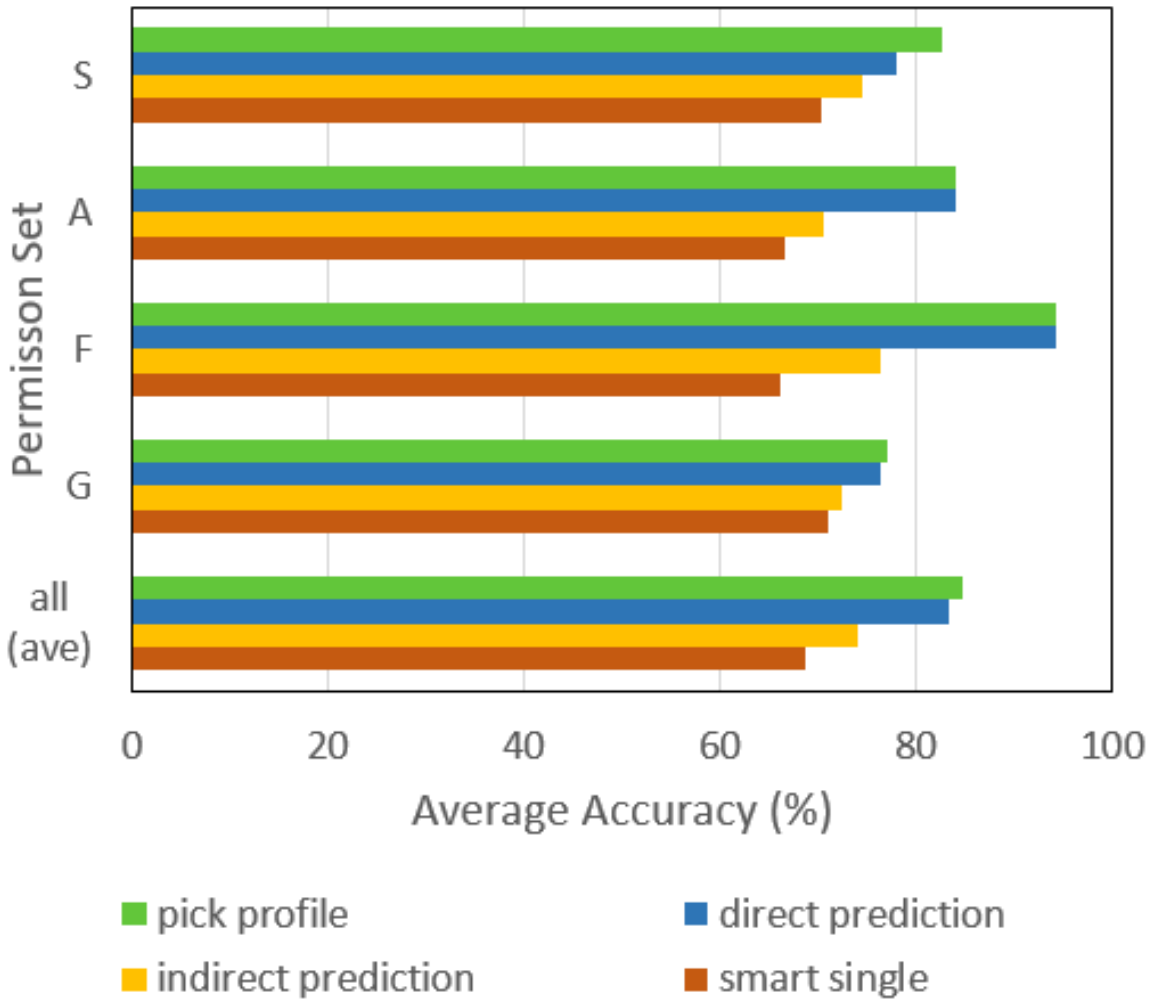


Figure 6.5: Average accuracies of the recommender strategies on the 30 users.

Chapter 7

Evaluate the Household IoT Privacy-setting Interface Prototype (Proposed original work)

To further explore this trade-off between parsimony and accuracy and to answer the second research question in Chapter 1, I propose the following user study plan focusing on evaluating the user experience of the privacy-setting interface prototypes.

7.1 Planned Experimental Setup

Proposed user study will be a between-subject study. All the participants will be recruited through Amazon Mechanical Turk. During this user study, we will manipulate two different independent variables to compare several default/profile solutions. The first one is the extend of default/profile's conservatives. We consider the default settings that with all disabled by default as the most conservative profile; and the default settings with all enabled by default as the most open profile, the 'smart default' and 'smart profiles' are considered to be in the middle. The other independent variable is the different levels of complexity for the settings interface. Hence 4x2 = 8 total experimental conditions (i.e., user interfaces) will be presented to the participants. The Dependent variable of our study will be the user experience of the system, including the satisfaction and trust

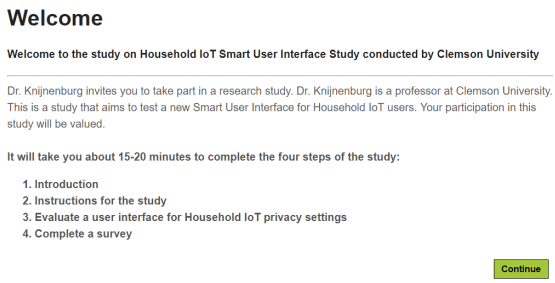


Figure 7.1: Experiment Landing Page

to the company.

During the user study [1], the users will be first be welcome with brief introduction of the experimental instructions (See Figure 7.1), followed by a participant consent form (See Figure 7.2).

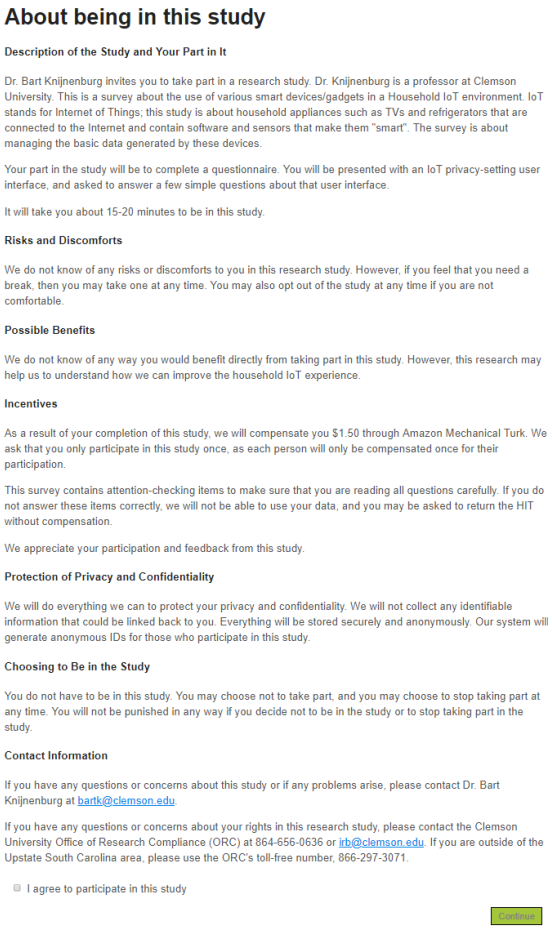
Then the participants will be introduced with the concept of the household IoT devices that appearing in this study, corresponding to the 'Who' and 'What' parameters of an IoT scenario. As shown in Figure 7.3, the introduction contains both figures, text, and audio information. After the introduction, the participant will be given an example scenario to further understand the context of our study. Attention checks will also be given here to make sure the participants have paid attention to the explanations.

After above procedures, one out of the 8 user interfaces will be randomly chosen for each participants. Participants need to go through the whole interface to see if the preset privacy settings is suitable for them, and make necessary changes to accommodate their actual privacy demands. All these changes will be recorded to compared with the preset settings for further analysis purpose. A simple user interface condition with all settings turned off is shown in Figure 7.4.

Next, the participants will be give a survey containing questions about three different aspects: *Subjective System Aspects* (Orange color), *Personal Characteristics* (Blue color), and *Situational Characteristics* (Green color), as shown in Figure 7.5. All the items of the questionnaire are shown in Appendix.

As shown Figure 7.5, we expect 'General Privacy Concerns', 'Data Collection Concerns', and 'Knowledge' all have a positive effect on the 'Perceived Privacy Threats', which consequently has a negative effect on the 'Trust' and 'Satisfaction'. The mediation effect of 'Trust' on 'Satisfaction' will also be investigated. The effect of user's decision style is also interesting to us since different style of

[1] The user study url can be found here: http://yyhe.people.clemson.edu/uistudy/



About being in this study

Description of the Study and Your Part in It

Dr. Bart Knijnenburg invites you to take part in a research study. Dr. Knijnenburg is a professor at Clemson University. This is a survey about the use of various smart devices/gadgets in a Household IoT environment. IoT stands for Internet of Things; this study is about household appliances such as TVs and refrigerators that are connected to the Internet and contain software and sensors that make them "smart". The survey is about managing the basic data generated by these devices.

Your part in the study will be to complete a questionnaire. You will be presented with an IoT privacy-setting user interface, and asked to answer a few simple questions about that user interface.

It will take you about 15-20 minutes to be in this study.

Risks and Discomforts

We do not know of any risks or discomforts to you in this research study. However, if you feel that you need a break, then you may take one at any time. You may also opt out of the study at any time if you are not comfortable.

Possible Benefits

We do not know of any way you would benefit directly from taking part in this study. However, this research may help us to understand how we can improve the household IoT experience.

Incentives

As a result of your completion of this study, we will compensate you $1.50 through Amazon Mechanical Turk. We ask that you only participate in this study once, as each person will only be compensated once for their participation.

This survey contains attention-checking items to make sure that you are reading all questions carefully. If you do not answer these items correctly, we will not be able to use your data, and you may be asked to return the HIT without compensation.

We appreciate your participation and feedback from this study.

Protection of Privacy and Confidentiality

We will do everything we can to protect your privacy and confidentiality. We will not collect any identifiable information that could be linked back to you. Everything will be stored securely and anonymously. Our system will generate anonymous IDs for those who participate in this study.

Choosing to Be in the Study

You do not have to be in this study. You may choose not to take part, and you may choose to stop taking part at any time. You will not be punished in any way if you decide not to be in the study or to stop taking part in the study.

Contact Information

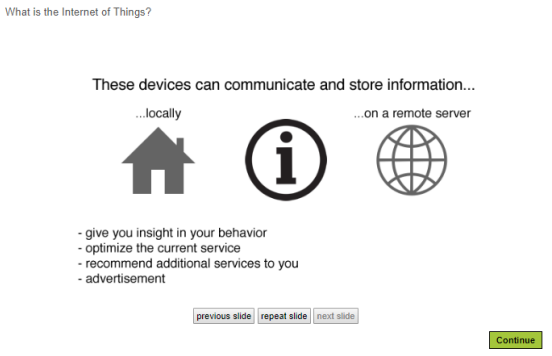
If you have any questions or concerns about this study or if any problems arise, please contact Dr. Bart Knijnenburg at bartk@clemson.edu.

If you have any questions or concerns about your rights in this research study, please contact the Clemson University Office of Research Compliance (ORC) at 864-656-0636 or irb@clemson.edu. If you are outside of the Upstate South Carolina area, please use the ORC's toll-free number, 866-297-3071.

I agree to participate in this study

Continue

Figure 7.2: User Consent Form



What is the Internet of Things?

These devices can communicate and store information...

...locally ...on a remote server

- give you insight in your behavior
- optimize the current service
- recommend additional services to you
- advertisement

previous slide repeat slide next slide

Continue

Figure 7.3: Introduction to Household IoT

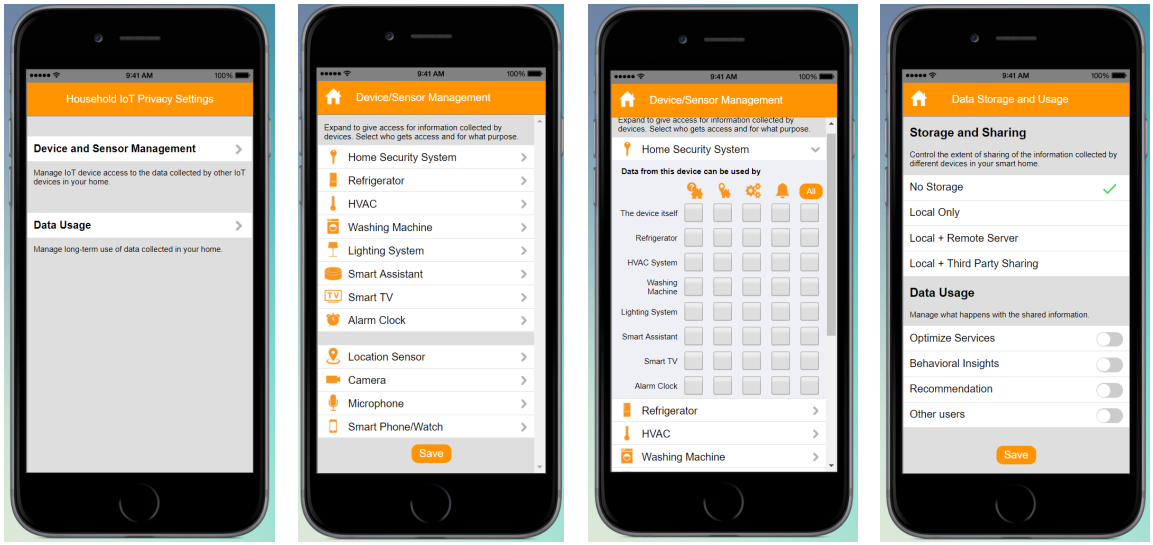


Figure 7.4: Simple User-Interface condition with all settings turned off

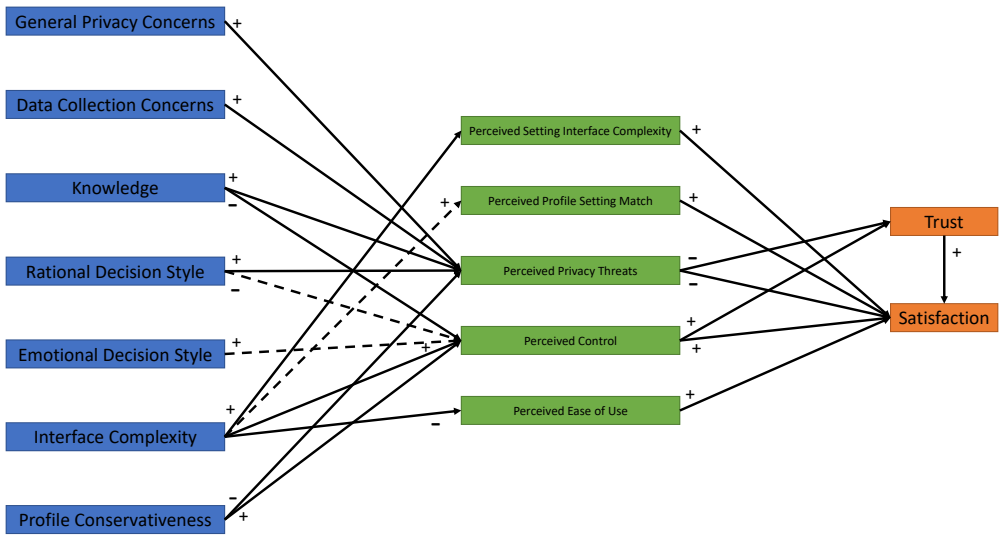


Figure 7.5: Expected Structural Model for Proposed User Study

decision making may have effect on 'Perceived Control' or 'Perceived Privacy Threats', which will then affect user's 'Trust' and 'Satisfaction'. 'Interface Complexity' is expected to have a positive effect on'Perceived Interface Complexity', 'Perceived Profile Setting Match', 'Perceived Control', and 'Perceived Ease of Use', which will have a positive effect on 'Trust' and 'Satisfaction'. 'Profile Consevativeness' is expected to have a negative effect on 'Perceived Privacy Threats' and a positive effect on 'Perceived Control', which will then have a positive effect on both 'Trust' and 'Satisfaction'.

After the user study is finished, We will use statistics to analysis the effect of the independent variables on the subjective system aspects, and further mediation effect on the user experience. We also wonder how the personal characteristics ans situational characteristics affect the user experience. Finally, we will apply machine learning techniques to uncover deep insights of the results.

Chapter 8

Conclusion

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] 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.

[3] 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.

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

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

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

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

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

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

[32] 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.

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

[34] 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.

[35] 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.

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

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

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

[43] 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.

[44] 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.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

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

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

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

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

[53] 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.

[54] 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.

[55] 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.

[56] 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.

[57] 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.

[58] 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.

[59] 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.

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

[61] 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.

[62] 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.

[63] 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.

[64] 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.

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

[66] 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.

[67] 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.

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

[69] 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.

[70] 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.

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

[72] 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.

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

[74] 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.

[75] 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.

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

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

[78] 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.

[79] 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.

[80] 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.

[81] 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.

[82] 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.

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

[84] 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.

[85] 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.

[86] 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.

[87] 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.

[88] 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.

[89] 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.

[90] 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.

[91] 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.

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

[93] 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.

[94] 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.

[95] 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.

[96] 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.

[97] 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.

[98] 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.

[99] 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.

[100] 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.

[101] 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.

[102] 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.

[103] 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.

[104] 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.

[105] 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.

[106] 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.

[107] 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.

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

[109] 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.

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

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

[112] 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.

[113] 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