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

---

A Dissertation Proposal
by
Yangyang He
Aug 2018

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

Approved By:

Dr. Bart P. Knijnenburg
Advisor/Committee Chair

Dr. Larry F. Hodges
Committee Member

Dr. Alexander Herzog
Committee Member

Author's Publications

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

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

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

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

Outline

List of Tables . . . . . **iii**

List of Figures . . . . . **iv**

1 Motivation **1**

2 The Acceptability of IoT (original work) **4**
2.1 Experimental Setup 4
2.2 Results Analysis 5
2.3 Summary 12

3 Recommending Privacy Preference for General Public IoT **14**
3.1 Dataset and design 15
3.2 Statistical Analysis 17
3.3 Predicting users' behaviors (original work) 18
3.4 Privacy-setting Prototypes (original work) 25
3.5 Summary 28

4 Recommending Privacy Perference for Household IoT **30**
4.1 Experimental Setup 30
4.2 Statistical Analysis 34
4.3 Privacy-Setting Prototype Design 35
4.4 Predicting users' behaviors (original work) 37
4.5 Privacy-Setting Prototype Design Using Machine Learning Results (original work) . 54

5 Proposed Work **59**
5.1 Planned Experimental Setup 59

6 Related Work **63**
6.1 Personalization in Iot Systems 63
6.2 Privacy in Personalized systems 63
6.3 Privacy in IoT 64
6.4 Existing privacy control schemes 65
6.5 Privacy-Setting Interfaces 65
6.6 Privacy Prediction 66
6.7 Data-driven design 67

7 Conclusion **69**

Bibliography **69**

Appendices **74**

List of Tables

2.1 Participants Demographics 5

3.1 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."* 16
3.2 Comparison of clustering approaches 20
3.3 Confusion matrix for the overall prediction 20
3.4 Drill down of the Overall Prediction tree for 'who' = 'Own device' 21

4.1 Parameters used to construct the information-sharing scenarios. The "codes" are used as abbreviations in graphs and figures throughout the paper and the Appendix. . . . 33
4.2 Comparison of clustering approaches (highest parsimony and highest accuracy) . . . 38
4.3 Confusion matrix for the One Rule prediction 39
4.4 Confusion matrix for the overall prediction 40

List of Figures

2.1 Process of accepting IoT as observed 5
2.2 Trust Chain 9
2.3 An interface for providing the user with "control" 11

3.1 From Left, Screen 1 shows three default settings, Screen 2,3 and 4 shows layered interface 18
3.2 The Overall Prediction decision tree. Further drill down for 'who' = 'Own device' is provided in Table 3.4 20
3.3 Attitude-based clustering: 2-cluster tree. Further drill down for **who** = 'Friend' or 'Employer/School' in Cluster 0 is hidden for space reasons. 22
3.4 Fit-based clustering: 3-cluster tree. Further drill down is hidden for space reasons. . 24
3.5 Accuracy of our clustering approaches 25
3.6 Two types of profile choice interfaces 27

4.1 From left, screen 1 is the landing page of our manual settings interface, screen 2 is the Device/Sensor Management page, screen 3 shows the explanation when you click on "I want to learn more", and screen 4 is the Data Storage & Use page. 36
4.2 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 4.1. 39
4.3 A "smart default" setting with 264 nodes (accuracy: 63.76%). Parameter value abbreviations correspond to the "code" column in Table 4.1. 40
4.4 Accuracy and parsimony (tree size) of the smart default change as a function of Confidence Factor 41
4.5 Parsimony/accuracy comparison for Naive, One Rule, and Overall Prediction 42
4.6 A "smart default" setting with only 8 nodes (accuracy: 63.32%). Parameter value abbreviations correspond to the "code" column in Table 4.1. 42
4.7 Parsimony/accuracy comparison for attitude-based clustering 44
4.8 The most parsimonious 2-profile attitude-based solution (2 nodes/profile, accuracy: 69.44%). Parameter value abbreviations correspond to the "code" column in Table 4.1. 44
4.9 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 4.1. 46
4.10 Parsimony/accuracy comparison for agglomerative clustering 47
4.11 The best 4-profile agglomerative clustering solution (2 nodes/profile, accuracy: 79.40%). Parameter value abbreviations correspond to the "code" column in Table 4.1. 47
4.12 The best 5-profile agglomerative clustering solution (2.4 nodes/profile, Accuracy: 80.35%). Parameter value abbreviations correspond to the "code" column in Table 4.1. 48
4.13 The best 6-profile agglomerative clustering solution (3.17 nodes/profile, Accuracy: 80.68%). Parameter value abbreviations correspond to the "code" column in Table 4.1. 48
4.14 Parsimony/accuracy comparison for fit-based clustering 50

4.15 The most parsimonious 3-profile fit-based solution (7 nodes/profile, accuracy: 79.80%). Parameter value abbreviations correspond to the "code" column in Table 4.1. 50
4.16 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 4.1. . . 51
4.17 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 4.1. . . 51
4.18 Summary of All our Approaches 52
4.19 A good 5-profile fit-based clustering solution (5 nodes/profile, Accuracy: 83.11%). Parameter value abbreviations correspond to the "code" column in Table 4.1. 53
4.20 Design for 5-Profile solution presented in Section 4.5.1. 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. . . 56
4.21 Design for 5-Profile solution presented in Section 4.5.2. 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). 58

5.1 Experiment Landing Page 60
5.2 User Consent Form 60
5.3 Introduction to Household IoT 61
5.4 Simple User-Interface condition with all settings turned off 61

Chapter 1

Motivation

During the last two decades, computers have evolved into intricate personal tracking devices such as smart phones, smart watches, and fitness trackers. At the same time, computers and communication technologies are being embedded in appliances such as TVs, refrigerators, light fixtures and thermostats to create 'smart home' environments. Finally, public sensing devices track us as we move about the built environment. By using all kinds of sensors, such as cameras, microphones, GPS, accelerometers, even the simplest of appliances are able to gain knowledge of its surrounding and their users. These connected devices, exchange data with each other, and further interact with our day-to-day activities. It is no longer surprising that our smart refrigerator knows what food is stored inside it and notify us that we need to buy groceries when we start our cars as we go back home from work. These smart connected devices are arguably revolutionizing our everyday life.

As forecast by Gartner [**?**], the total number of 21 billion IoT devices will be in use by 2020. Cisco also predicts the global IoT market will be $14.4 trillion by 2022. This rapidly accelerating growth of these Internet of Things (IoT) technologies brings a wealth of opportunities as well as risks.

When users are considering adopting new IoT devices, they want to take the benefit of using those smart connected electronic 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 will result in unknown privacy risks to the users. A few research has shown that privacy issues are the underlying obstacles to the adoption of social and mobile

technologies []. Privacy concerns have been identified as an important barrier to the growth of IoT.

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

However, as the 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 read the privacy policies or the privacy-settings carefully 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. This privacy-setting choice overload makes it difficult for IoT users to correctly and precisely make their decision to express their true demands.

In addition, the 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:

How can we help users simplify the task of controlling privacy setting for IoT devices in a user-friendly manner, so that they can make good privacy decisions? This question can be further divided into two sub-questions: 1). Can we recommend them the appropriate IoT privacy-setting according to their decision making characteristics?)2. How do they feel about the new privacy-setting recommendation interface that we made?

In this proposal, we try to solve the main research question:

1. In Chapter 2, we present a preliminary survey study that we conducted by interviewing with potential IoT users. By doing this, we try to gain deeper insight on the acceptability of IoT systems, which will be helpful and supportive to our following investigation to the decision-making process of IoT users when they share their personal data with differernt general public IoT devices. This will further affect how we design the privacy-setting interface and recommend privacy-settings for the users.

2. In Chapter 3, we demonstrate our existing work on recomming privacy preferences for general IoT. For this study, we leveraged data collected by Lee and Kobsa [22], which asked 200 participants about their intention to allow or reject the IoT features presented in 14 randomized generated general public IoT usage scenarios. The scenarios have 5 manipulable parameters: 'Who', 'What', 'Where', 'Reason', and 'Persistence'. We first apply statistical analysis on the dataset to determine the effect of each scenario parameter on users' decisions to allow the general IoT scenarios. Based on this statistical analysis, we design an "layered" intelligent user interface to reduce the complexity of manually setting privacy preferences for IoT. To further simplify the task of manully setting privacy preferences, we next use machine learning techniques to predict users' decisions based on the scenario parameters. By using Weka Java library, I develop 5 differernt machine learnign algorithms to cluster the participants and create a number of "smart profiles" accordingly. Each "smart profile" is a group of pre-set privacy setting preferences that users can apply by a single click. We present the detailed explanation of all the "smart profiles" to the users so that they can easily choose the one that are most suitable for them.

3. In Chapter 4, we expand

4. In Chapter 5 I discuss my proposed study to evaluate the new interface of recommending privacy-settings for household IoT.

Chapter 2

The Acceptability of IoT (original work)

In this chapter, we present a preliminary survey study based on interviews with potential IoT users to gain deeper insight on the acceptability of IoT systems. I first discuss the experimental setup of our preliminary user study. Secondly, I demonstrate the analysis on the results of the study.

2.1 Experimental Setup

For this experiment, we interviewed 10 users with the demographics shown in Table 2.1. The interview is approximately 30-50 minutes in length and covered a wide range of open questions related to IoT. These questions need participants to input their personal preferences about technology and self-perceived tech savviness. We first recorded the entire conversation with the participants on the understanding that their anonymity was kept. The entire recorded conversation was then transcribed manually. We also tried to take note of other interpersonal cues, such as body language Keywords. During the analysis, we extracted participants' key statements from our interviews and used card sorting and affinity diagram techniques to group the specific statements. We emphasize any related key word, such as "privacy" or "ease of use".

Table 2.1: Participants Demographics

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

2.2 Results Analysis

Based on the results from our interviews, the factors that affect the acceptability of IoT devices can be summarized into following three aspects: Privacy, Usability, and Affordability. As shown in Figure 2.1, while making the decision of whether to adopt the IoT technology, the users usually consider the trade-off between privacy and usability as against affordability. If the user's find that they are going to get better usability and privacy at a price that they can afford, they are more likely to go ahead and choose an IoT system/device. Within the above three aspects, only the usability and privacy are relevant to our research questions. Since we can not do anything to affordability in our study , however, the results still provide a good insight for manufacturers about the trade-off between usability, privacy , and affordability. Next, we present our analysis to the effect of usability and privacy to the acceptability of IoT systems/devices.

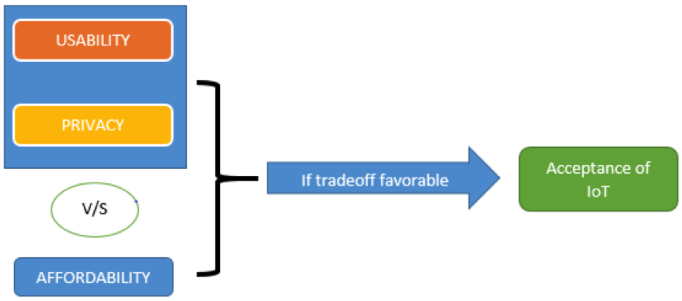


Figure 2.1: Process of accepting IoT as observed

2.2.1 IoT Privacy and Acceptability

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

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

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

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

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

I: "About voice?"

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

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

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

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

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

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

Another aspect related to the IoT privacy we observed in our interviews is the **Trust**, the object of which is to whom users’ informations are shared with. The object of trust from users can be varied in different contexts of IoT environments. For example, in general IoT environment, the objects can be an individual (e.g. your colleagues), an organization (e.g. your employer), the government and so on. While the user is in a Household IoT environment, his/her information

may be first shared within all the connected IoT devices deployed in his/her home for various functionalities. Moreover, those smart IoT devices may further transfer users' information to their manufactures to store on a remote server (cloud) or even share them with the third-party for other purpose, such as advertisements and better recommendations.

From our interview, we observed that the trust to the second-party or even the third-party also varies from user to user. One of the participants pointed out that, *P: "For example, Apple in the news recently for refuting the FBI. FBI wanted in, Apple said we can't access these phone that actually turned me on to apple I previously used android. And the fact that they say they made their devices so secured that they can't even access them that really interests me. So yeah I am very concerned about it but I think now that I evolved into the Apple eco-system. I pretty much give apple everything because I trust them."*

Another example is:

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

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

I: "Any company or any organization?"

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

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

P: "Yes, I trust them."

It is evident from the conversation above that once established, trust can propagate from the second-party to the third-party via a "trust chain". As shown in Figure 2.2, a "trust chain" is established when the organization we trust, deals with a third party organization which we are not

Figure 2.2: Trust Chain

aware about in the first place but still choose to trust. This kind of trust can be established only when there is a clear sight at the benefits that the user might get out of such a connection.

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

2.2.2 IoT Usability and Acceptability

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

2.2.2.1 Convenience and Usability

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

by enabling the users with a common platform from where they can easily connect with their devices goes a long way in improving the overall usability of the systems and thereby impacts the acceptability of IoT in its totality. Usability for a few users also encompasses the aesthetics of any system which is evident from the statements made by participants.

2.2.2.2 Being in Control and Usability

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

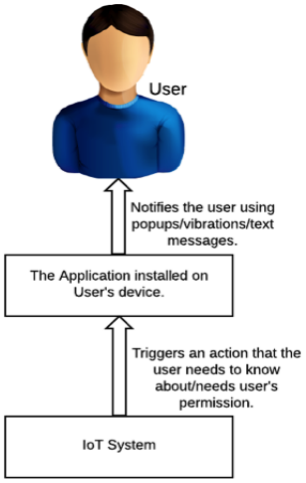


Figure 2.3: An interface for providing the user with "control"

2.2.2.3 Being Notified and Being in Control

"Control" can be the complete manual control of the system or it can be a situation where the user is notified regarding something which can be changed or altered subject to manual intervention. This is basically the system saying that it has an affordance which the user can utilize to better suit his/her convenience. In such a situation, the notification system (perhaps an application for IoT installed on the user's tablet) forms an interface between the machine and the user which serves as a medium to control the degree of automation. The entire idea behind having such an interface is to provide the user with control without compromising convenience. This phenomenon is depicted in the figure 2.3.

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

2.3 Summary

Based on the above analysis to our results, we see that when making the decision of whether to adopt the IoT technology, the users usually consider the trade-off between privacy and usability as against affordability (See Figure 2.1). If the user's find that they are going to get better usability and privacy at a price that they can afford, they are more likely to go ahead and try out an IoT device/system.

In a deeper level of usability, if the users find that the IoT systems/devices will enhance their convenience, they will be more inclined to accept it. However, this is based on their perception of the actual utility of the automation provided by IoT. For example, if someone stays near a grocery store, he/she would tend to believe that there is not enough purpose for an IoT systems/devices when it comes to automatic ordering of the same grocery list online.

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

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

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. However, since people differ extensively in their privacy settings [26]. At the same time, the vast number of different IoT devices makes choosing adequate privacy settings a very challenging task that is likely to result in information and choice overload [45]. Under these circumstances, a data-driven design approach seems promising since we could cluster similar users and summarize their privacy preference to generate a set of "smart profiles" for new users to choose from in our IoT privacy-setting interface.

We discuss this data-driven approach in the following chapters.

Chapter 3

Recommending Privacy Preference for General Public IoT

In chapter **??**, we have discussed what are the key factors that affecting users to adopt or accept 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 have been applied to predicting people's location-privacy preferences, thereby automatically configuring their location-privacy settings. But none similar research has been done in IoT domain yet. 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 preference for general IoT, including the data-driven design, the dataset that we use, the inspection of users' behaviors using statistical analyses, prediction of users' behaviors using machine learning techniques, and the privacy-setting prototypes that we create based on both statistical and machine learning results.

This chapter is to answer the following questions:

- 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.

3.1 Dataset and design

As we have discussed in Chapter **??**, the development of usable privacy interfaces commonly relies on user studies with existing systems. Since the Intel control framework has yet to be implemented [4], this method is not possible. We therefore we leveraged data collected by Lee and Kobsa [22], 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 3.1). 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

Table 3.1: 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

control. This reduces the complexity of the decisions users have to make, without reducing the amount of control available to them. We use statistical analysis of the Lee and Kobsa dataset to decide which aspect should be presented at the highest layer of our IoT privacy-setting interface, and which aspects are relegated to subsequently lower layers.

In our second phase, we develop a "smart" default setting, which preempts the need for many users to manually change their settings [37]. However, since people differ extensively in their privacy preferences [26], 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 [20, 26, 46]. We perform machine learning analysis on this dataset to create a similar set of "smart profiles" for our general IoT privacy-setting interface.

3.2 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.

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 [23].

'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-

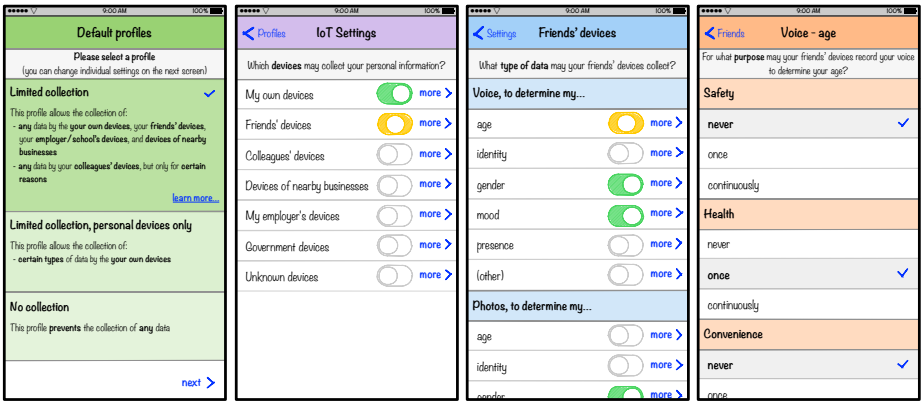


Figure 3.1: From Left, Screen 1 shows three default settings, Screen 2,3 and 4 shows layered interface

time collection is more acceptable than continuous collection. 'Where' the data is being collected does not influence intention at all. This could be an artifact of the dataset: location is arguably less prominent when reading a scenario than it is in real life.

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

Moreover, we found no significant interaction effects between parameters, other than the interaction between 'Who' and 'What'. 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 3.1). Users can utilize this interface for making manual privacy settings. The explanation to this user interface will be in section 3.4.

3.3 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 best possible 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. Accuracies of the resulting solutions are reported in Table 4.2.

3.3.1 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.

3.3.2 Overall Prediction

We next create a "smart default" by predicting the allow/reject decision with the scenario parameters using J48 with Weka's [12] default settings. The resulting tree (Figure 3.2) has an accuracy of 63.53%. The confusion matrix (Table 4.4) shows that this model results in overly conservative settings; only 208 'yes'es are predicted.

Figure 3.2 shows that this model predicts 'no' for every recipient ('who') except 'Own device'.

Table 3.2: 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 3.3: 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

For this value, the default setting depends on 'what' is being collected (see Table 3.4). For some levels of 'what', there is a further drill down based on 'where', 'persistence' and 'reason'.

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

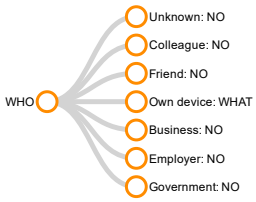


Figure 3.2: The Overall Prediction decision tree. Further drill down for 'who' = 'Own device' is provided in Table 3.4

Table 3.4: 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

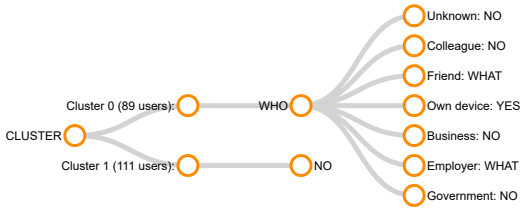


Figure 3.3: Attitude-based clustering: 2-cluster tree. Further drill down for **who** = 'Friend' or 'Employer/School' in Cluster 0 is hidden for space reasons.

3.3.3 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 3.3) 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 **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.

3.3.4 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.

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 3.4) 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**.

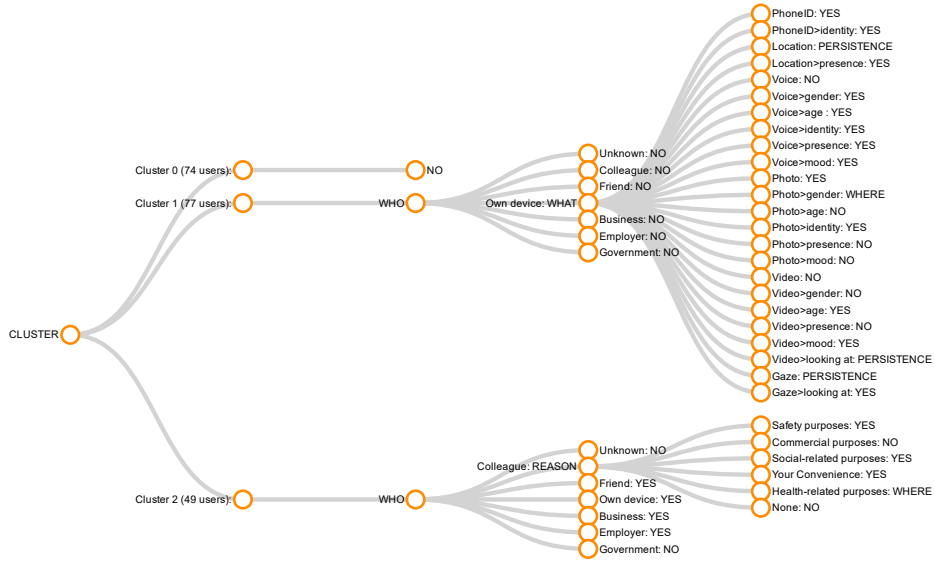


Figure 3.4: Fit-based clustering: 3-cluster tree. Further drill down is hidden for space reasons.

3.3.5 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 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.

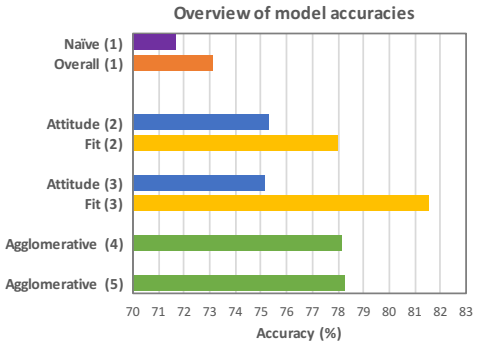


Figure 3.5: Accuracy of our clustering approaches

3.3.6 Discussion of Machine Learning Results

Figure 3.5 shows a comparison of the presented approaches. Compared to a naive default setting (all 'no'), a "smart default" makes a 2.0% improvement. The fit-based 2-cluster solution results in two "smart profiles" that make another 6.7% improvement over the "smart default", while the three "smart profiles" of the fit-based 3-cluster solution make an 11.5% improvement. If we let users choose the best option among these three profiles, they will on average be content with 81.54% of the settings. This rivals the accuracy of some of the "active tracking" machine learning approaches (cf. [34]).

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.

3.4 Privacy-setting Prototypes (original work)

In this section we employ our data-driven design methodology to develop a prototype for an IoT privacy-setting interface based on the results of our statistical and machine learning analyses.

3.4.1 Manual Settings

The first challenge is to design an interface that users can navigate manually. Using the results of our statistical analyses, we design a "layered" settings interface: 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 3.1. 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 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 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.

3.4.2 Smart Default Setting

The next challenge is to decide on a default setting, so that users only have to make minimal adjustments to their settings. We can use a simple "yes to everything" or "no to everything" default, but these are on average only accurate 28.33% and 71.67% of the time, respectively.

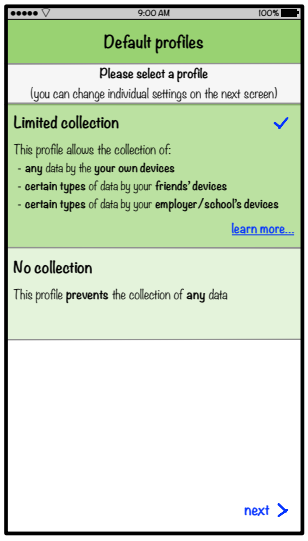
Using the results from our Overall Prediction (see Figure 3.2), we can create a "smart default" setting that is 73.10% accurate on average. In this version, the IoT settings for all devices are set to 'off', except for 'My own device', which will be set to the middle option. Table 3.4 shows

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.

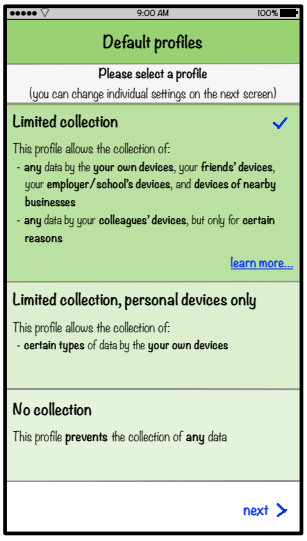
3.4.3 Smart Profiles

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 3.4), we can attain an accuracy of 81.54%. Screen 1 in Figure 3.1 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.



(a) 2-profile choice interface



(b) 3-profile choice interface

Figure 3.6: Two types of profile choice interfaces

3.5 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.
- 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.

The 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%.

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".

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 [22] 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.

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 4

Recommending Privacy Perference for Household IoT

In Chapter 3, 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 [25].

4.1 Experimental Setup

In Chapter 3, 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.

4.1.1 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 4.1.2). 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 4.1. 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.

4.1.2 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).

4.1.3 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 4.1: 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 [22] 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.

4.2 Statistical Analysis

Our statistical analysis shows that unlike results from [2], 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 4.1.2, 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.

4.3 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 4.2, 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 4.1) 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.

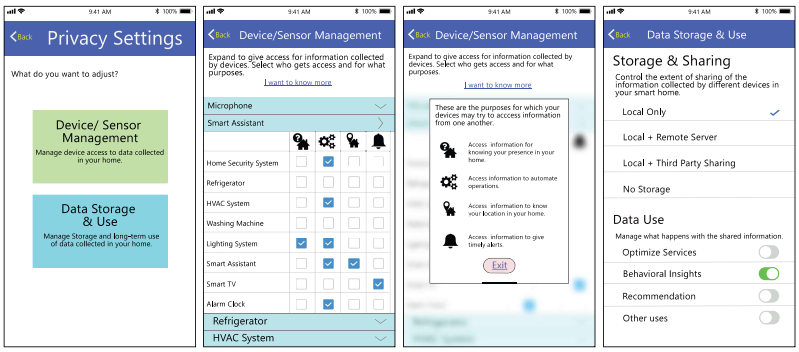


Figure 4.1: From left, screen 1 is the landing page of our manual settings interface, screen 2 is the Device/Sensor Management page, screen 3 shows the explanation when you click on "I want to learn more", and screen 4 is the Data Storage & Use page.

Device/Sensor Management: This screen (Figure 4.1, 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 4.1, 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 4.1, screen 3).

Data Storage & Use: This screen (Figure 4.1, 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 4.5 revisits the interface designs presented here.

4.4 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 [47] 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

Table 4.2: 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. 4.2)	1	1	3	61.39%
Overall (Fig. 4.5)	1	1	8	63.32%
	1	1	264	63.76%
Attitude-based clustering (Fig. 4.7)	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. 4.10)	1133	4	2	79.4%
	1133	5	2.4	80.35%
	1133	6	3.17	80.60%
Fit-based clustering (Fig. 4.14)	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%

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 4.2; more detailed results of the parsimony/accuracy trade-off are presented in Figures 4.5, 4.7, 4.10 and 4.14 throughout the paper, and combined in Figure 4.18.

4.4.1 Naive Prediction Model

We start with the naive or "information-less" predictions. Compared to our previous work [2], 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

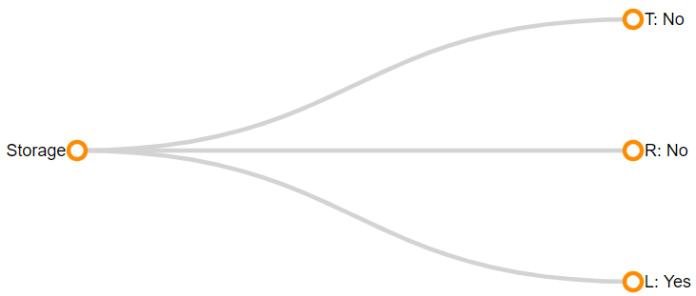


Figure 4.2: A "smart default" setting based on the "One Rule" algorithm (4 nodes, accuracy: 61.39%). Parameter value abbreviations correspond to the "code" column in Table 4.1.

Table 4.3: 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

of smart appliances can get behind.

4.4.2 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 [15]. 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 4.2, 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 4.3).

4.4.3 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 4.3, this model predicts users' decision

[2] 61.39 / 53.26 = 1.153

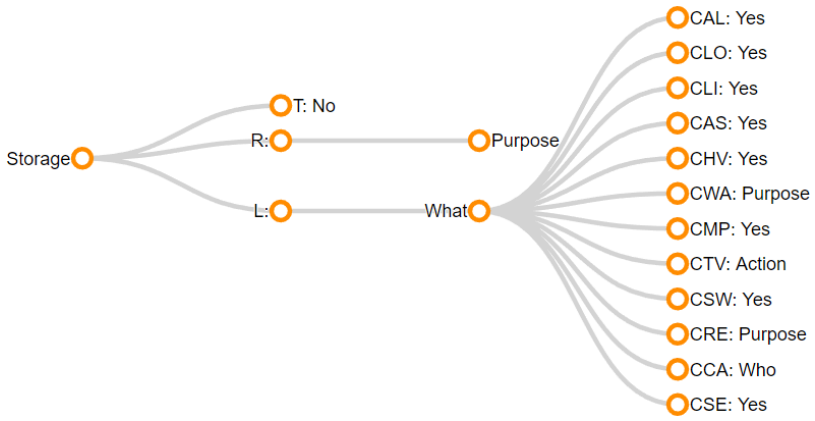


Figure 4.3: A "smart default" setting with 264 nodes (accuracy: 63.76%). Parameter value abbreviations correspond to the "code" column in Table 4.1.

Table 4.4: 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

on **Storage** first. It predicts *disable* for every scenarios with collected data stored on a remote server and shared with third party. For scenarios that store collected data on remote server without sharing, the default settings will depend on the 'purpose' of information sharing. There is a further drill down based on 'who' and 'what'. For scenarios that store collected data locally, the default settings will depend on the 'what'. There is a further drill down based on 'who', 'what', and 'action'. With this default setting, users would on average be satisfied with 63.76% of these settings—a 19.7% improvement over the naive "disable all" default.

On the downside, this "smart default" setting is quite complex—the "smart default" in our previous work [2] 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 4.4).

To better understand the parsimony/accuracy trade-off, we vary the degree of model pruning

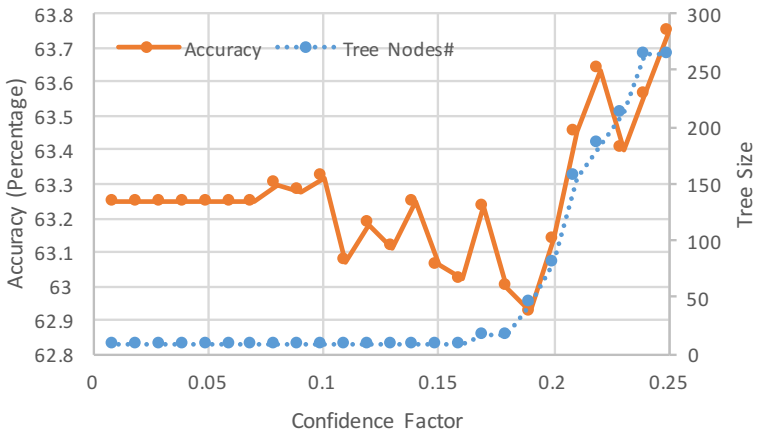


Figure 4.4: Accuracy and parsimony (tree size) of the smart default change as a function of Confidence Factor

to investigate the effect of increasing the parsimony (i.e., more trimming) on the accuracy of the resulting "smart default" setting. The parameter used to alter the amount of post-pruning performed 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 4.4 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 4.5 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 4.6, 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

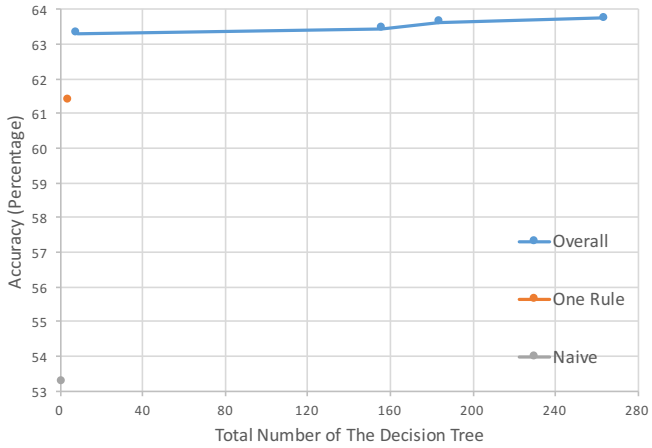


Figure 4.5: Parsimony/accuracy comparison for Naive, One Rule, and Overall Prediction

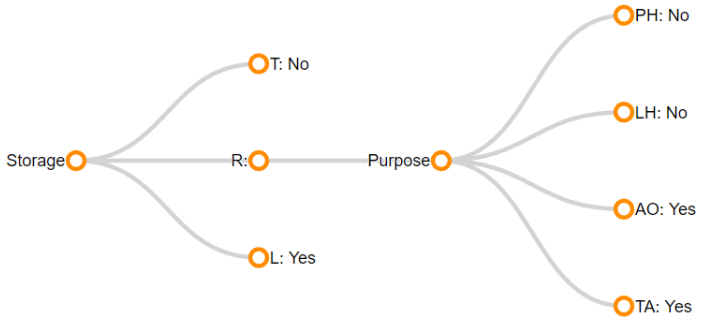


Figure 4.6: A "smart default" setting with only 8 nodes (accuracy: 63.32%). Parameter value abbreviations correspond to the "code" column in Table 4.1.

follows:

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

While the "smart default" setting makes a considerable improvement over a naive default, there is still a lot of room for improvement—even our best prediction model only correctly models on average 63.76% of the user's desired settings. This should come at no surprise, as one of the most consistent findings in the field of privacy is that people differ substantially in their privacy preferences [20]. 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 [19]. 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 [2]. 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.

4.4.4 Attitude-Based Clustering

As shown in Figure **??**, 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 4.7, 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 4.7), 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 4.8). This solution still has an accuracy of 69.44%, which is still an 8.9% increase over the best single "smart default" setting.

Figure 4.7: Parsimony/accuracy comparison for attitude-based clustering

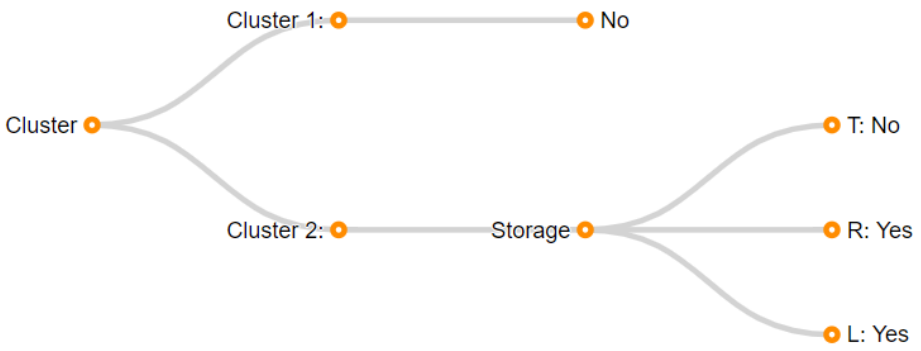


Figure 4.8: The most parsimonious 2-profile attitude-based solution (2 nodes/profile, accuracy: 69.44%). Parameter value abbreviations correspond to the "code" column in Table 4.1.

For the 3-cluster solutions (the orange line in Figure 4.7), 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 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 4.6). 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 4.7) 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 4.7) 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 4.7 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 4.9: 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).

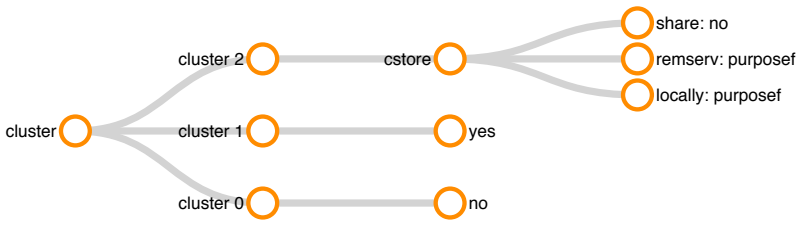


Figure 4.9: A 3-profile solution example of attitude-based clustering (18.33 nodes/profile, accuracy: 73.26%). Parameter value abbreviations correspond to the "code" column in Table 4.1.

4.4.5 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 agglomerative) approach, using users' decisions only. This method first fits a separate decision tree for each participant, and then iteratively merges these trees based on similarity. In our previous work [2] 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

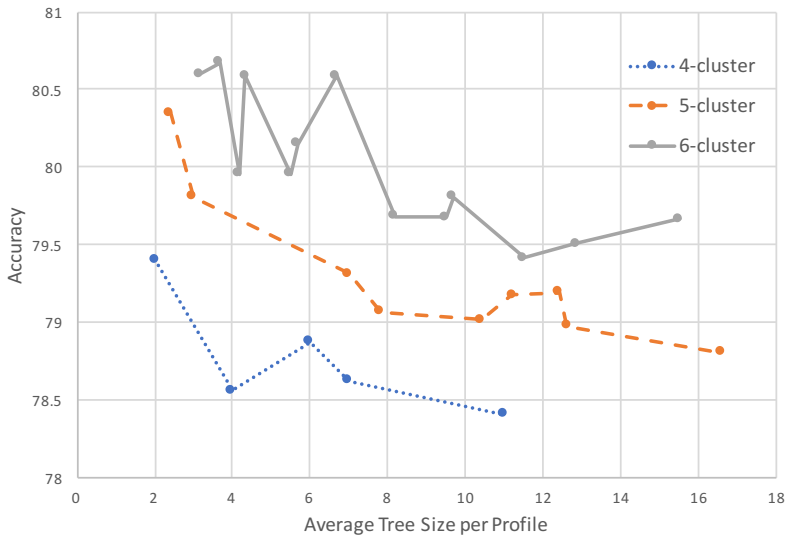


Figure 4.10: Parsimony/accuracy comparison for agglomerative clustering

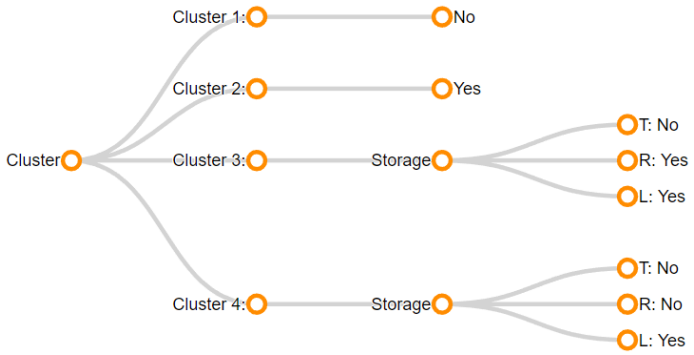


Figure 4.11: The best 4-profile agglomerative clustering solution (2 nodes/profile, accuracy: 79.40%). Parameter value abbreviations correspond to the "code" column in Table 4.1.

clustering (see Figure 4.10). 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 4.11: 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

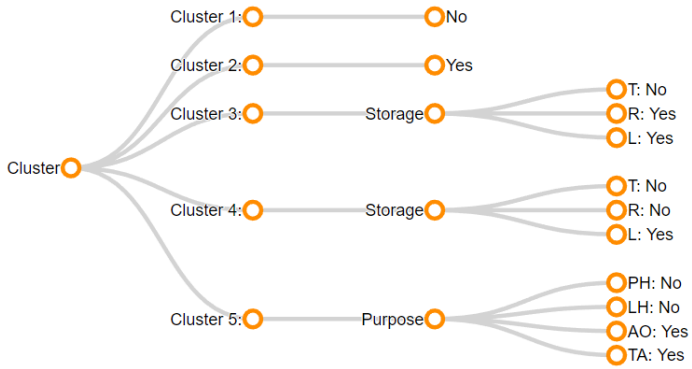


Figure 4.12: The best 5-profile agglomerative clustering solution (2.4 nodes/profile, Accuracy: 80.35%). Parameter value abbreviations correspond to the "code" column in Table 4.1.

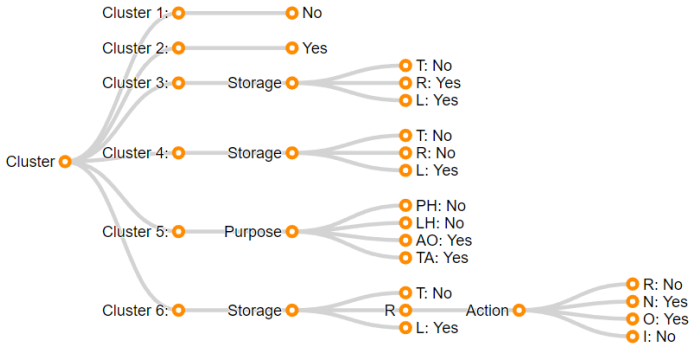


Figure 4.13: The best 6-profile agglomerative clustering solution (3.17 nodes/profile, Accuracy: 80.68%). Parameter value abbreviations correspond to the "code" column in Table 4.1.

4-cluster agglomerative solution. The decision trees are shown in Figure 4.12: 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 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 4.13: 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).

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

4.4.6 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 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 4.14.

For the 2-cluster solutions (the blue line in Figure 4.14), 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 attitude-based solution (see Figure 4.8), but with a higher accuracy (74.43%).

For the 3-cluster solutions (the orange line in Figure 4.14), 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.

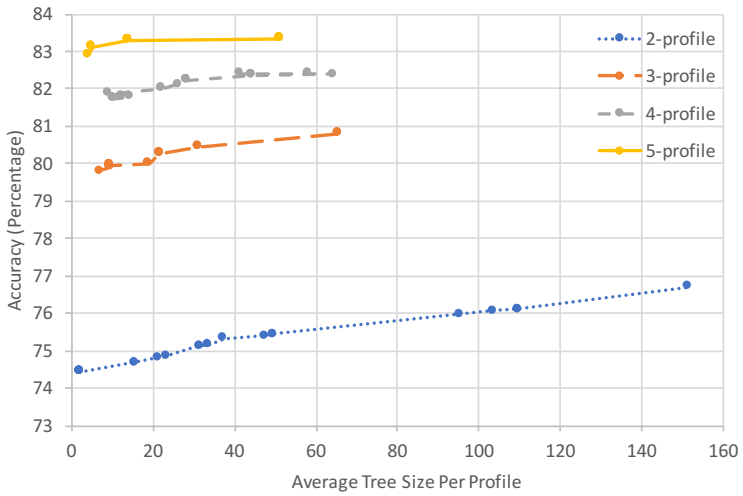


Figure 4.14: Parsimony/accuracy comparison for fit-based clustering

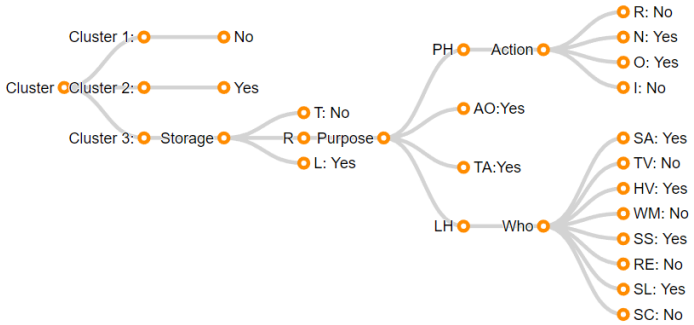


Figure 4.15: The most parsimonious 3-profile fit-based solution (7 nodes/profile, accuracy: 79.80%). Parameter value abbreviations correspond to the "code" column in Table 4.1.

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 4.15.

For the 4-cluster solutions (the grey line in Figure 4.14), 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 4.16.

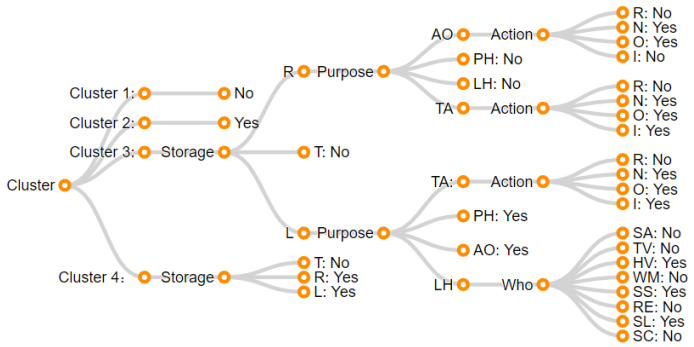


Figure 4.16: The most parsimonious 4-profile fit-based solution (9.25 nodes/profile, accuracy: 81.88%). Parameter value abbreviations correspond to the "code" column in Table 4.1.

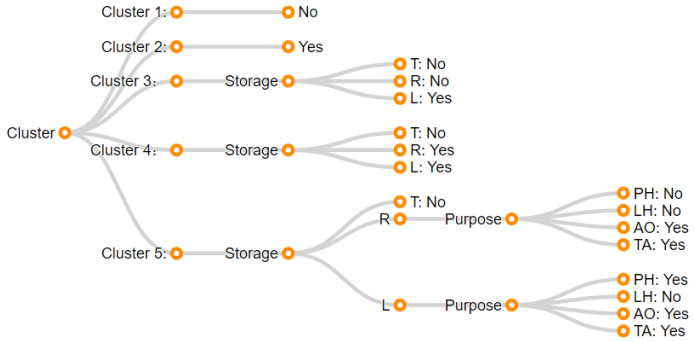


Figure 4.17: The most parsimonious 5-profile fit-based solution (4.2 nodes/profile, accuracy: 82.92%). Parameter value abbreviations correspond to the "code" column in Table 4.1.

For the 5-cluster solutions (the yellow line in Figure 4.14), 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 4.17.

4.4.7 Discussion of machine learning results

Figure 4.18 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.

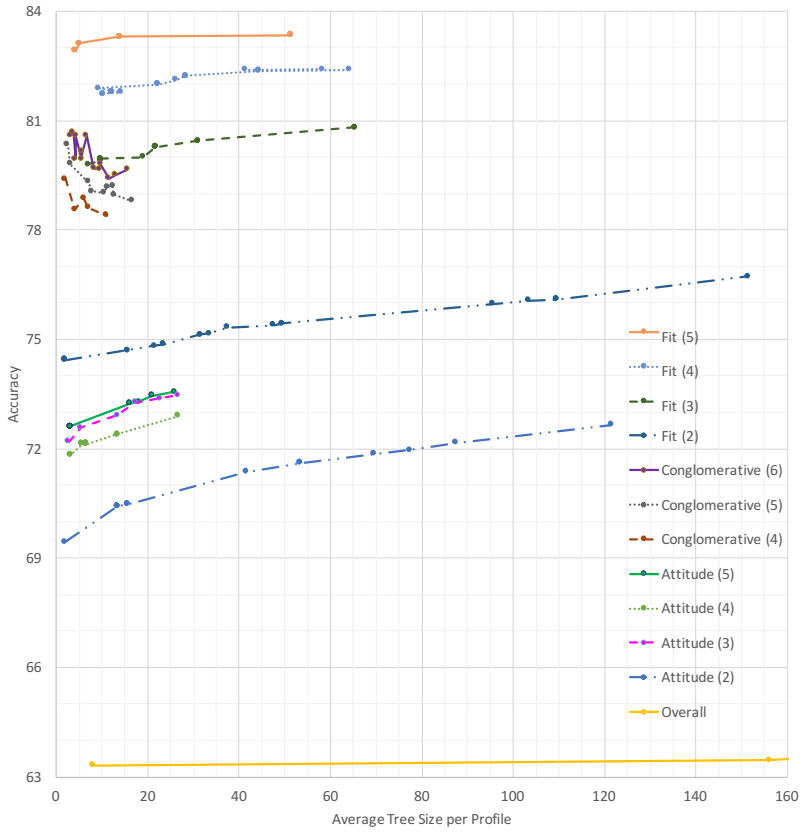


Figure 4.18: Summary of All our Approaches

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 4.1) these defaults are incredibly easy for users to implement by themselves.

The same is true for the 4-profile agglomerative clustering solution (see Figure 4.11) and the 5-profile agglomerative clustering solution (see Figure 4.12): these profiles involve little more than a single high-level setting, which users can likely easily make by themselves.

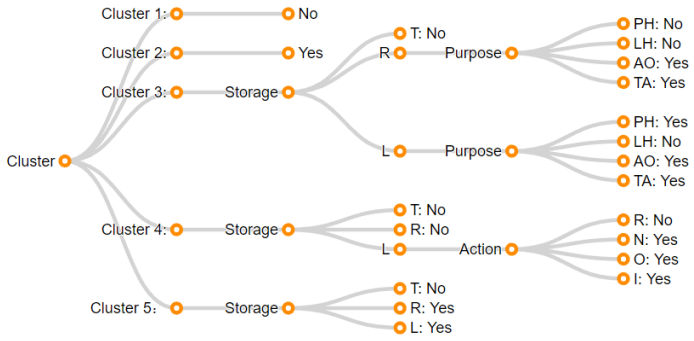


Figure 4.19: A good 5-profile fit-based clustering solution (5 nodes/profile, Accuracy: 83.11%). Parameter value abbreviations correspond to the "code" column in Table 4.1.

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 4.17) 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 4.19. 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 4.15) or the 4-profile fit-based solution (Figure 4.16. 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.

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

In Section 4.3 we developed a prototype interface that household IoT users can use to manually set their privacy settings (see Figure 4.1). Our machine learning analysis (Section 4.4) resulted in a number of interesting solutions for "smart profiles" that would allow users of this interface to set their privacy settings with a single click (i.e., a choice of profile). 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 4.17 and 4.19).

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.

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

This machine learning solution (Figure 4.17) requires an interaction between the *Storage* parameter and the *Purpose* parameter—two parameters that are controlled independently in the prototype in Figure 4.1. Our solution is to slightly alter the interface, and add the profile selection page at the beginning of the interface (see Figure 4.20):

- **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*).

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

The alternative machine learning solution presented in Figure 4.19 requires an additional interaction between the *Storage* parameter and the *Action* parameter. This requires us to slightly alter the interface again (see Figure 4.21):

- **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'.
- **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.

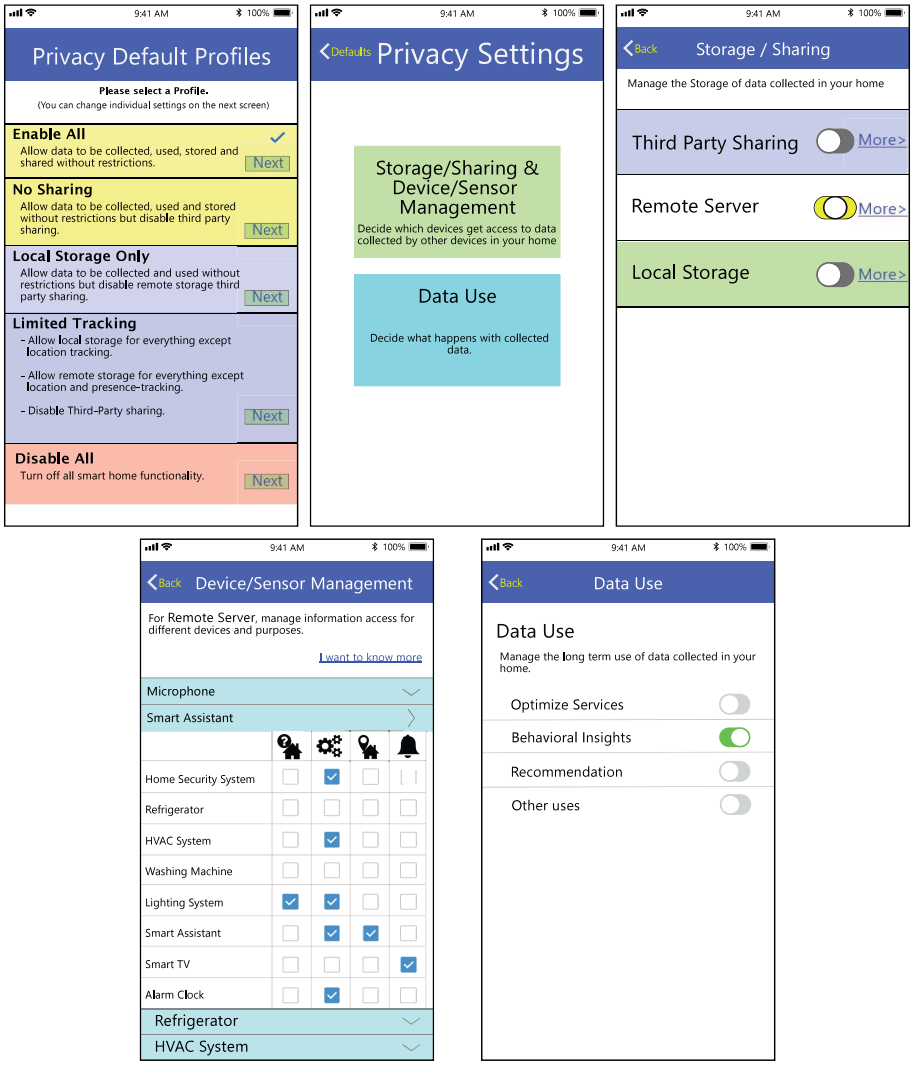


Figure 4.20: Design for 5-Profile solution presented in Section 4.5.1. From top left, screen 1 is the profile selection page, screen 2 is the slightly altered landing page of our manual settings interface, screen 3 is the slightly altered Data Storage page, screen 4 (bottom left) is the Device/Sensor Management page, and screen 5 is the Data Use page.

- **Screen 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.

4.5.3 Reflection on design complexity

The interfaces presented in this section have an additional 'layer' compared to the original interface presented in Section 4.3. 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 4.4 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.

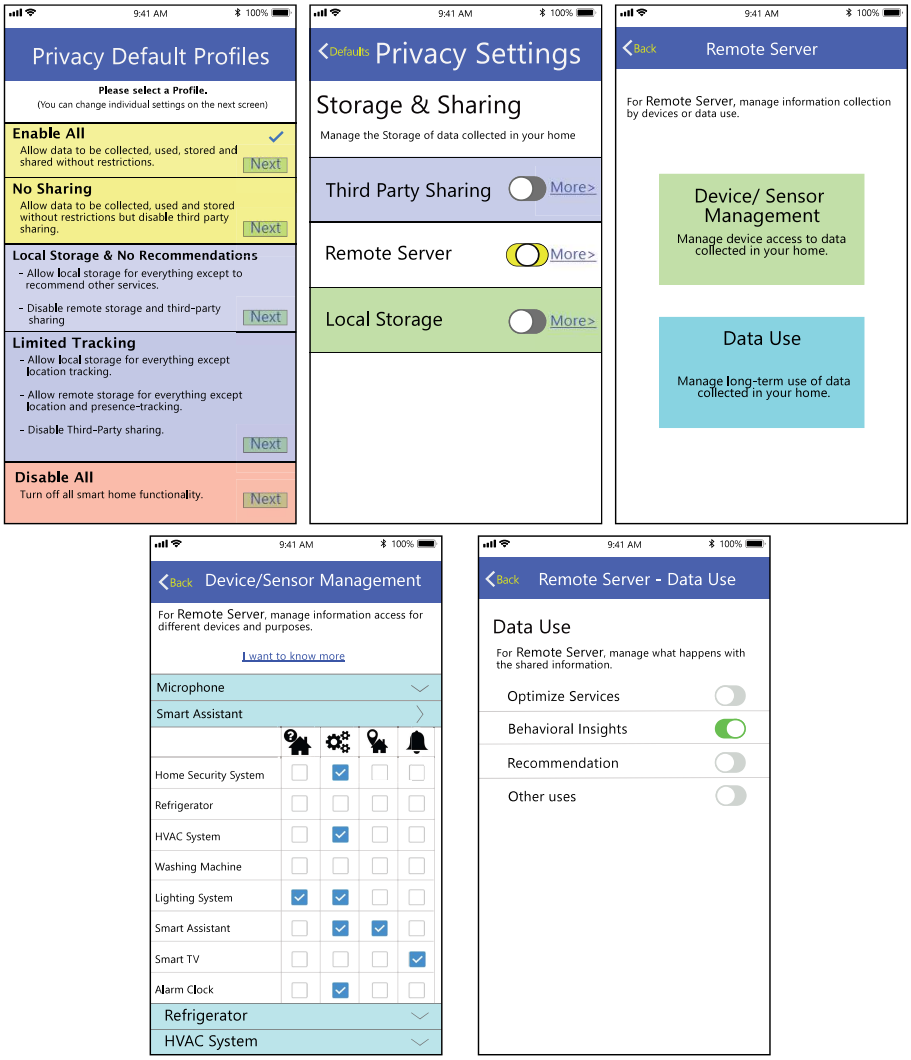


Figure 4.21: Design for 5-Profile solution presented in Section 4.5.2. From top left, screen 1 is the profile selection page, screen 2 is the slightly altered Data Storage page, screen 3 follows the 'More' button to offer access to screen 4 (bottom left, the Data Use page) and screen 5 (bottom right, the Device/Sensor Management page).

Chapter 5

Proposed 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.

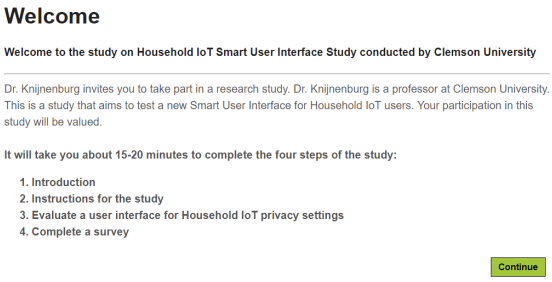
5.1 Planned Experimental Setup

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 to the company.

During the user study [1], the users will be first be welcome with brief introduction of the experimental instructions (See Figure 5.1), followed by a participant consent form (See Figure 5.2).

Then the participants will be introduced with the concept of the household IoT devices that

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



Welcome

Welcome to the study on Household IoT Smart User Interface Study conducted by Clemson University

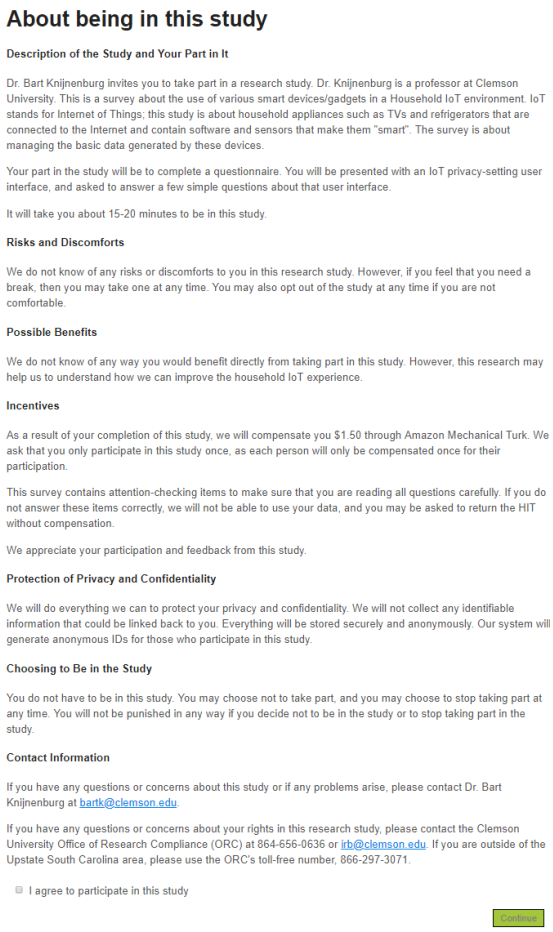
Dr. Knijnenburg invites you to take part in a research study. Dr. Knijnenburg is a professor at Clemson University. This is a study that aims to test a new Smart User Interface for Household IoT users. Your participation in this study will be valued.

It will take you about 15-20 minutes to complete the four steps of the study:

1. **Introduction**
2. **Instructions for the study**
3. **Evaluate a user interface for Household IoT privacy settings**
4. **Complete a survey**

Continue

Figure 5.1: Experiment Landing Page



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 5.2: User Consent Form

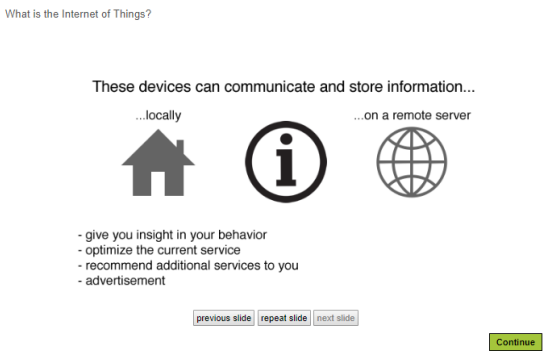


Figure 5.3: Introduction to Household IoT

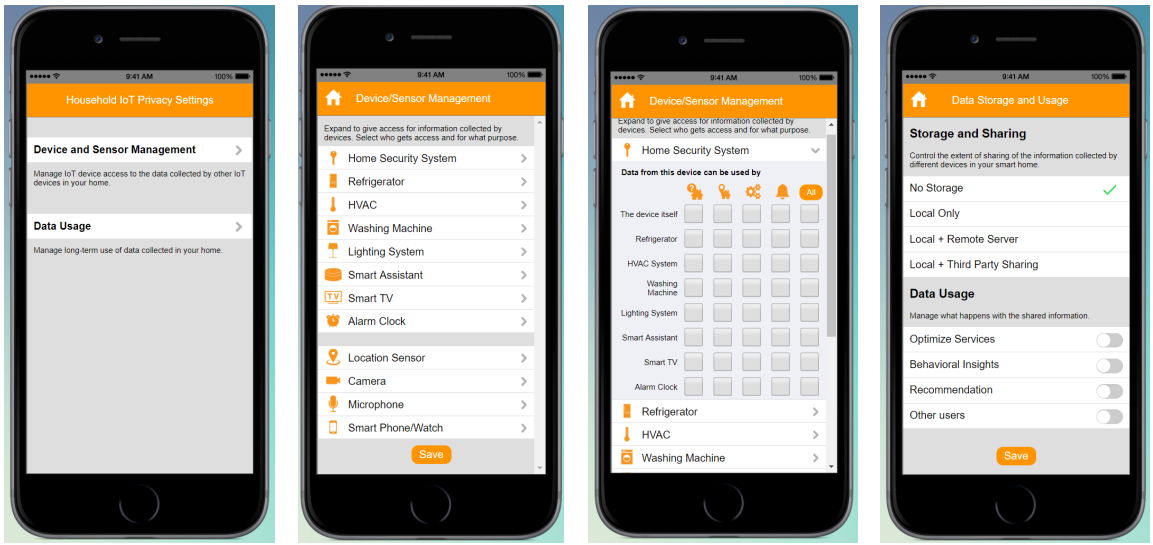


Figure 5.4: Simple User-Interface condition with all settings turned off

appearing in this study, corresponding to the 'Who' and 'What' parameters of an IoT scenario. As shown in Figure 5.3, 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 5.4.

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 **??**. All the items of the questionnaire are shown in Appendix.

As shown Figure **??**, 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 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 6

Related Work

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

6.1 Personalization in Iot Systems

One of the key features of IoT environments is that they have a high potential for providing personalized services to their users [42, 7, 10]. For example, Russell et al. [33] use unobtrusive sensors and micro-controller to realize a human detection for further providing personalization in a scenario of a family making use of the IoT in their daily living. Henka et al. [13] propose an approach to personalize services in (household) IoT using the Global Public Inclusive Infrastructure's [43] preference set to describe an individual's needs and preferences, and then adapting a smart environment accordingly.

6.2 Privacy in Personalized systems

Researchers have shown that privacy can play a limiting role in users' adoption of personalized services [39]. For example, Awad and Krishnan [1] show that privacy concerns inhibit users' use of personalized services, and Sutanto et al. [38] demonstrated that privacy concerns can prevent people from using a potentially beneficial personalized application. Kobsa et al. [21] 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 [30, 14, 16], and researchers therefore claim that both the benefits and the risks meet a certain threshold [40], or that they should be in balance [3].

6.3 Privacy in IoT

The argument that using user-generated data for personalization can result in privacy concerns has also been made in IoT environments [48]. One of the first examples in this regard was the work by, Sheng et al. [36], 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 [29, 24]. 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 [5]. Likewise, Jayraman et al.'s privacy preserving architecture aggregates requested data to preserve user privacy [17].

Other research has considered IoT privacy from the end-user perspective [9], 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 [41]) 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 [45], and Feth et al. investigated the creation of understandable and usable controls [9]). The current paper follows this approach, by outlining a novel methodology for the development of usable and efficient privacy-setting interfaces and applying it to household IoT privacy management.

6.4 Existing privacy control schemes

Smartphones give users control over their privacy settings in the form of prompts that ask whether the user allows or denies a certain app access to a certain type of information. Such prompts are problematic for IoT, because IoT devices are supposed to operate in the background. Moreover, as the penetration of IoT devices in our homes continues to increase, prompts would become a constant noise which users will soon start to ignore, like software EULAs [11] or privacy policies [18].

Pejovic and Musolesi [28] presented the design and implementation of an efficient online learner that can serve as a basis for recognizing opportune moments for interruption. The design of the library is based on an in-depth study of human interruptibility. Comparatively, our work tries to find the most suitable privacy-setting profile for each user based on their privacy preference on different household IoT scenarios.

6.5 Privacy-Setting Interfaces

Beyond prompts, one can regulate privacy with global settings. The most basic privacy-setting interface is the traditional "access control matrix", which allows users to indicate which entity gets to access what type of information [35]. This approach can be further simplified by grouping recipients into relevant semantic categories, such as Google+'s *circles* [44]. Taking a step further, Raber et al. [31] 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 [45]. A wedge-based interface will arguably not be able to succinctly represent such complexity, and therefore either be impossible, or still lead to a significant amount of information and choice overload.

We propose a data-driven approach to solve this problem: statistical analysis informs the

construction of a layered settings interface, while machine learning-based privacy prediction helps us find smart privacy profiles.

6.6 Privacy Prediction

Several researchers have proposed privacy prediction as a solution to the privacy settings complexity problem—an approach known as "user-tailored privacy" (UTP) [19]. 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. [34] 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. [27] present a system which can determine the required privacy level in new situations based on the history of interaction between users. Their system can efficiently deal with the rise of privacy concerns and help users in a pervasive system full of dynamic interactions.

Dong et al. [6] use a binary classification algorithms to give users personalized advice regarding their privacy decision-making practices on online social networks. They found that J48 decision trees provided the best results. Li and et al. [23] 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. [8], 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. [32] employ an approach similar to ours, using k-means clustering on users' contextualized location sharing decisions to come up with several default policies. They showed that a small number of policies could accurately reflect a large part of the location sharing preferences. We extend their approach to find the best profiles based on various novel clustering approaches, and take the additional step of designing user interfaces that incorporate the best solutions.

6.7 Data-driven design

In our previous work [2], we leveraged data collected by Lee and Kobsa [22], which asked 200 participants about their intention to allow or reject the IoT features presented in 14 randomized scenarios. They varied the scenarios in a mixed fractional factorial design along the following dimensions: 'Who', 'What', 'Where', 'Reason', 'Persistence'.

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

We also conducted a machine learning analysis to predict participants' reactions to the scenarios. We used the outcomes of this analysis to develop a "smart" default setting, which preempts the need for many users to manually change their settings [37]. However, since people differ extensively in their privacy preferences [26], it is not possible to achieve an optimal default that is the same for everyone. Instead, different people may require vastly different settings [20, 26, 46]. By partitioning the participants in a number of clusters, we were able to construct a number of 'privacy profiles', which represented a selection of default settings for the user to choose from. These profiles

automate (part of) the privacy-setting task.

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

Chapter 7

Conclusion

Bibliography

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

[16] 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.

[17] 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.

[18] 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.

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

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

[21] 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.

[22] 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.

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

[24] 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.

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

[26] 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.

[27] 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.

[28] Veljko Pejovic and Mirco Musolesi. Interruptme: Designing intelligent prompting mechanisms for pervasive applications. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '14, pages 897–908, New York, NY, USA, 2014. ACM.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

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

[36] 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.

[37] 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.

[38] 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.

[39] 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.

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

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] 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.

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

[48] 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.

Appendices