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

A Dissertation Proposal

by

Yangyang He

Aug 2018

Submitted to the graduate faculty of the

School of Computing

In Partial Fulfillment of the Requirements

for the Dissertation Proposal

and subsequent Ph.D. in Computer Science

Approved By:

Dr. Bart P. Knijnenburg
Advisor/Committee Chair

Dr. Larry F. Hodges
Committee Member

Dr. Alexander Herzog
Committee Member

# Author's Publications

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

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

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

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

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

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

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

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

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

# Outline

# Abstract

# Chapter 1

# Motivation

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

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

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

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

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

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

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

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

# Chapter 2

# The Acceptability of IoT

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

Based on the results from our interviews, the factors that affect the acceptability of IoT devices can be summarized into following three aspects: Privacy, Usability, and Affordability. As

Table 2.1: Participants Demographics

<table>
<tr><td>Age Range</td><td colspan="2">21-35</td></tr>
<tr><td rowspan="2">Gender</td><td>Male</td><td>8</td></tr>
<tr><td>Female</td><td>2</td></tr>
<tr><td rowspan="4">Races</td><td>Chinese</td><td>2</td></tr>
<tr><td>Indians</td><td>4</td></tr>
<tr><td>Americans</td><td>3</td></tr>
<tr><td>Latin American</td><td>1</td></tr>
</table>

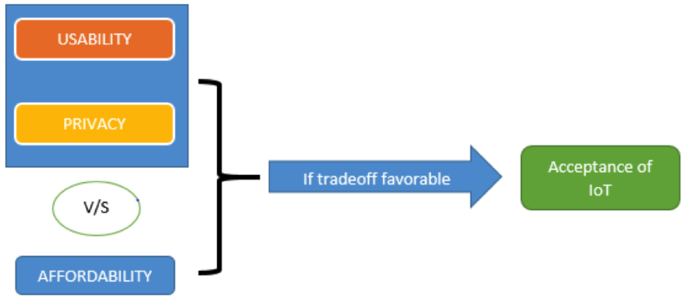



Figure 2.1: Process of accepting IoT as observed

shown in Figure 2.1, while making the decision of whether to adopt the IoT technology, the users usually consider the trade-off between privacy and usability as against affordability. If the user's find that they are going to get better usability and privacy at a price that they can afford, they are more likely to go ahead and choose an IoT system.

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

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

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

## 2.1 IoT Privacy and Acceptability

In this section, we present the 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.

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

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

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

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

*I: "About voice?"*

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

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

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

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

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

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

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

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

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

### 2.2.1 Convenience and Usability

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

### 2.2.2 Being in Control and Usability

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

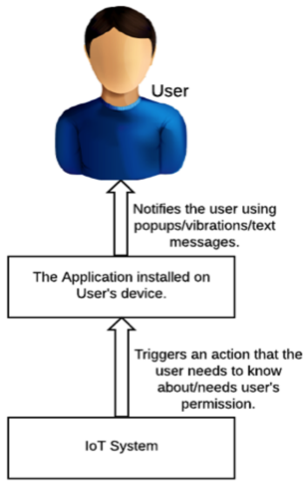



Figure 2.3: An interface for providing the user with "control"

### 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.

# Chapter 3

# Related Work

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

### 3.0.1 Personalization in Iot Systems

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

### 3.0.2 Privacy in Personalized systems

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

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

### 3.0.3 Privacy in IoT

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

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

Other research has considered IoT privacy from the end-user perspective [?], both when it comes to research (e.g., Ur et al. investigated how privacy perceptions differ among teens and their parents in smart security systems installed in homes [?]) and design (e.g., Williams et al. highlight the importance of designing interfaces to manage privacy such that they are usable to the end users of IoT devices [22], and Feth et al. investigated the creation of understandable and usable controls [?]). The current paper follows this approach, by outlining a novel methodology for the development of usable and efficient privacy-setting interfaces and applying it to household IoT privacy management.

### 3.0.4 Existing privacy control schemes

Smartphones give users control over their privacy settings in the form of prompts that ask whether the user allows or denies a certain app access to a certain type of information. Such prompts are problematic for IoT, because IoT devices are supposed to operate in the background. Moreover, as the penetration of IoT devices in our homes continues to increase, prompts would become a constant noise which users will soon start to ignore, like software EULAs [8] or privacy policies [10].

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

### 3.0.5 Privacy-Setting Interfaces

Beyond prompts, one can regulate privacy with global settings. The most basic privacy-setting interface is the traditional "access control matrix", which allows users to indicate which entity gets to access what type of information [19]. This approach can be further simplified by grouping recipients into relevant semantic categories, such as Google+'s *circles* [21]. Taking a step further, Raber et al. [16] 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 [22]. A wedge-based interface will arguably not be able to succinctly represent such complexity, and therefore either be impossible, or still lead to a significant amount of information and choice overload.

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

### 3.0.6 Privacy Prediction

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

Most existing work in line with this approach has focused on providing automatic default settings. For example, Sadeh et al. [18] 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. [15] 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. [13] similarly use J48 to demonstrate that taking the user's cultural background into account when making privacy predictions improves the prediction accuracy. Our data stems from a culturally homogeneous population (U.S. Mechanical Turk workers), so cultural variables are outside the scope of our study. We do however follow these previous works in using J48 decision trees in our prediction approach.

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

Ravichandran et al. [17] employ an approach similar to ours, using $k$-means clustering on users' contextualized location sharing decisions to come up with several default policies. They showed that a small number of policies could accurately reflect a large part of the location sharing preferences. We extend their approach to find the best profiles based on various novel clustering approaches, and take the additional step of designing user interfaces that incorporate the best solutions.

### 3.0.7 Data-driven design

In our previous work [**?**], we leveraged data collected by Lee and Kobsa [12], 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 [20]. However, since people differ extensively in their privacy preferences [14], it is not possible to achieve an optimal default that is the same for everyone. Instead, different people may require vastly different settings [11, 14, 23]. By partitioning the participants in a number of clusters, we were able to construct a number of 'privacy profiles', which represented a selection of default settings for the user to choose from. These profiles automate (part of) the privacy-setting task.

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

# Chapter 4

# Recommending Privacy Preference for General IoT

## 4.1 Introduction

In chapter 1 and 3, we have discussed what are the key factors that affecting users to 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.

### 4.1.1 Dataset and design

As we have discussed in Chapter 1, the development of usable privacy interfaces commonly relies on user studies with existing systems. Since the Intel control framework has yet to be implemented [5], this method is not possible. We therefore leverage an existing dataset collected by Lee and Kobsa [12], who asked users whether they would allow or deny IoT devices in their environment to collect information about them. A total of 2800 scenarios were presented to 200 participants (100 male, 99 female, 1 undisclosed) through Amazon Mechanical Turk. Four participants were aged between 18 and 20, 75 aged 20–30, 68 aged 30–40, 31 aged 40–50, 20 aged 50–60, and 2 aged $> 60$.

Each participant was presented with 14 scenarios describing a situation where an IoT device would collect information about the participant. Each scenario was a combination of five contextual parameters (Table 5.1), manipulated at several levels using a mixed fractional factorial design that allowed us to test main effects and two-way interactions between all parameters.

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

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

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

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

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

In our second phase, we develop a "smart" default setting, which preempts the need for many users to manually change their settings [20]. However, since people differ extensively in their privacy preferences [14], 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 [11, 14, 23]. We perform machine learning analysis on this dataset to create a similar set of "smart profiles" for our general IoT privacy-setting interface.

## 4.2 Statistical Analysis

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

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

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

### 4.2.1 Scenario Parameters and Attitude

#### 4.2.1.1 ANOVA Test of Main Effects

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

#### 4.2.1.2 Post-hoc Comparisons

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

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

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

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

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

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

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

video) regardless of what is being inferred:

- Participants were significantly more *comfortable* with 'voice' than 'video' ($d = 0.260$, $p = .005$), and found 'voice' less *risky* ($d = -0.239$, $p = .005$) and more *appropriate* ($d = 0.217$, $p = .015$) than 'video'.

- Participants were significantly more *comfortable* with 'voice' than 'photo' ($d = 0.201$, $p = .007$) and found 'voice' more *appropriate* than 'photo' ($d = 0.157$, $p = .028$). There was no significant difference in terms of *risk* ($p = .118$).

- No differences were found between 'photo' and 'video' in terms of *risk* ($p = .24$), *comfort* ($p = .35$) and *appropriateness* ($p = .26$).

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

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

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

#### 4.2.1.3 Interaction effects

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

### 4.2.2 Attitude and Behavioral intention

To test the effects of participants' attitudes on their allow/reject decision, we ran a *generalized linear mixed effects regression* (*glmer*) with a random intercept and a logit link function to account for the binary dependent variable. We found significant effects of all the three attitudes on participants' allow/reject decision (see Table 4.3). Each 1-point increase in **risk** results in a 4.04-fold decrease in the odds that the scenario will be allowed ($p < .0001$). Each 1-point increase in **comfort**

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

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

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

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

results in a 5.04-fold increase ($p < .0001$), and each 1-point increase in **appropriateness** results in a 3.47-fold increase ($p < .0001$).

### 4.2.3 Mediation Analysis

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

### 4.2.4 Discussion of Statistical Results

Our statistical results show several patterns that can inform the development of an IoT privacy-setting interface. We find that **who** is the most important scenario parameter, and should thus end up at the top layer of our interface. People are generally concerned about IoT scenarios involving unknown and government devices, but less concerned about about data collected by their

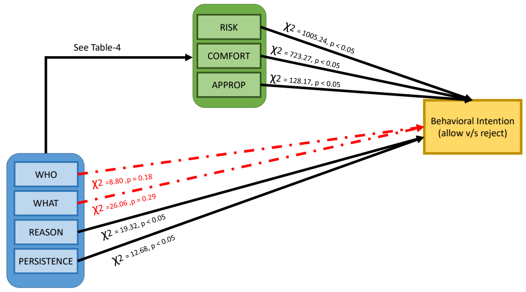



Figure 4.1: Mediation model of the effect of scenario parameters on participants' intention to allow/reject the scenario, mediated by attitudinal factors

own devices. Mistrust of government data collection is in line with Li et al.'s finding regarding US audiences [13].

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

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

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

## 4.3 Predicting users' behaviors

In this section we predict participants' allow/reject decision using machine learning methods. 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 5.9.

### 4.3.1 Naive Prediction Methods

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

### 4.3.2 Overall Prediction

We next create a "smart default" by predicting the allow/reject decision with the scenario parameters using J48 with Weka's [9] default settings. The resulting tree (Figure 4.2) has an accuracy of 63.53%. The confusion matrix (Table 5.11) shows that this model results in overly conservative

Table 4.5: Comparison of clustering approaches

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

Table 4.6: 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 |

settings; only 208 ‘yes’es are predicted.

Figure 4.2 shows that this model predicts ‘no’ for every recipient (**who**) except ‘Own device’. For this value, the default setting depends on **what** is being collected (see Table 4.7). 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.

### 4.3.3 Attitude-Based Clustering

Our first “smart profile” solution uses the attitudes (comfort, risk, appropriateness) participants expressed for each scenario on a 7-point scale. We averaged the values per attitude across each

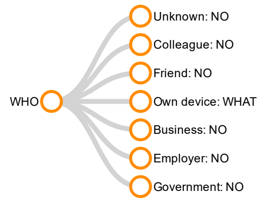



Figure 4.2: The Overall Prediction decision tree. Further drill down for **who** = ‘Own device’ is provided in Table 4.7

Table 4.7: Drill down of the Overall Prediction tree for **who** = ‘Own device’

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

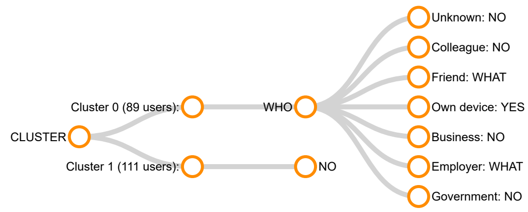



Figure 4.3: Attitude-based clustering: 2-cluster tree. Further drill down for **who** = 'Friend' or 'Employer/School' in Cluster 0 is hidden for space reasons.

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 5.9 under "attitude-based clustering".

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

The 2-cluster solution (Figure 4.3) has a 75.28% accuracy — a 3.0% improvement over the "smart default". This solution results in one profile with 'no' for everything, while for the other profile the decision depends on the recipient (**who**). This profile allows any collection involving the user's 'Own device', and may allow collection by a 'Friend' or an 'Employer/School', depending on **what** is being collected.

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

### 4.3.4 Fit-based clustering

Our fit-based clustering approach clusters participants without using any additional information. It instead uses the fit of the tree models to bootstrap the process of sorting participants into clusters. Like many bootstrapping methods, ours uses *random starts* and *iterative improvements* to find the optimal solution.

**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 5.9 under "fit-based clustering". We were not able to converge on a higher number of clusters.

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

The 3-cluster solution (Figure 4.4) 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**.

### 4.3.5 Agglomerative clustering

Our final method for finding "smart profiles" follows a hierarchical bottom-up (or agglomerative) approach. It first fits a separate tree for each participant, and then iteratively merges them based on similarity. 156 of the initial 200 trees predict "no for everything" and 34 of them predict "yes for everything"—these are merged first. For every possible pair of the remaining 10 trees, the accuracy of the pair is compared with the mean accuracy the individual trees, and the pair with the smallest reduction in accuracy is merged. This process is repeated until we reach the predefined number of clusters.

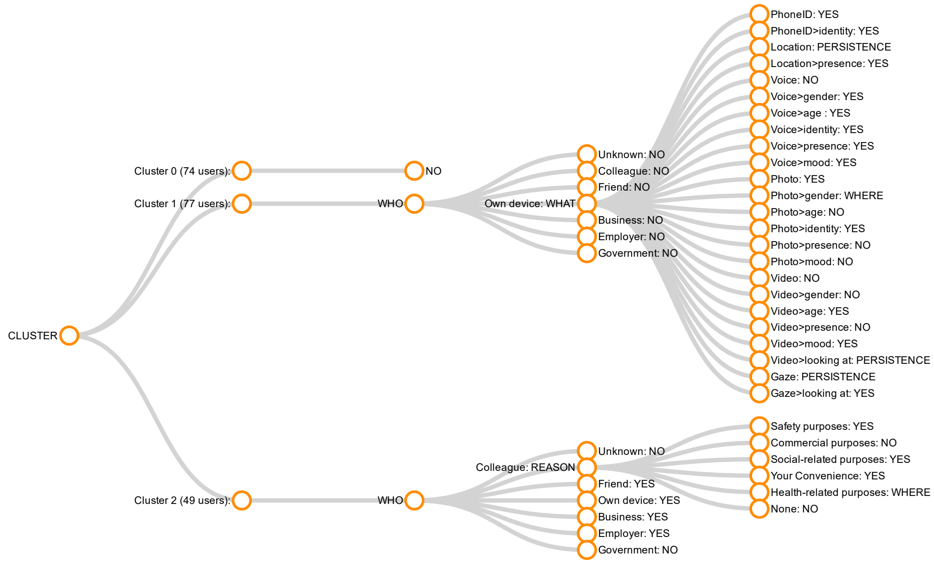



Figure 4.4: Fit-based clustering: 3-cluster tree. Further drill down is hidden for space reasons.

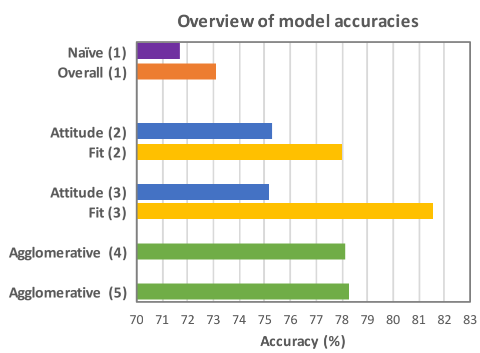



Figure 4.5: Accuracy of our clustering approaches

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 5.9, "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.

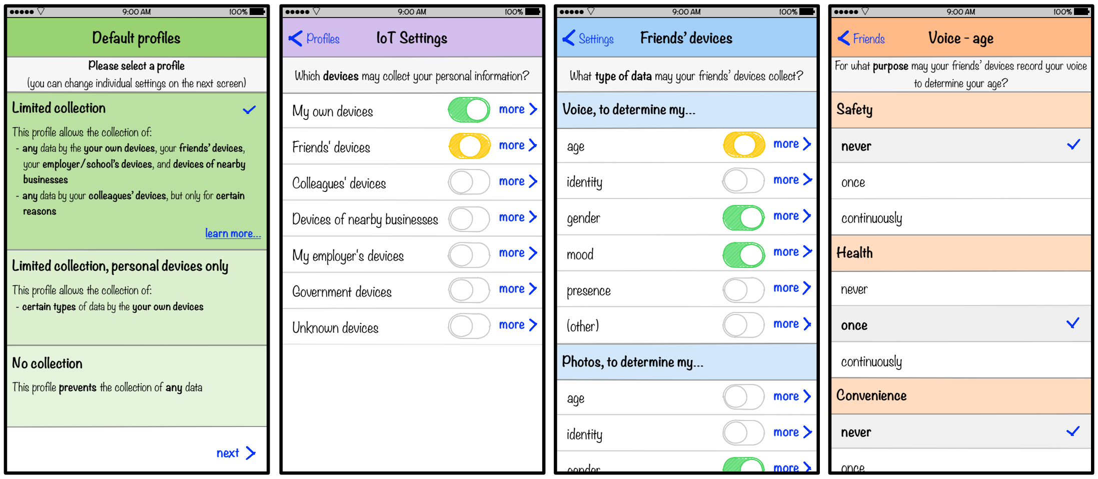



Figure 4.6: From Left, Screen 1 shows three default settings, Screen 2,3 and 4 shows layered interface

### 4.3.6 Discussion of Machine Learning Results

Figure 4.5 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. [18]).

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

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

## 4.4 Privacy-setting Prototypes

Designers of IoT privacy-setting interfaces face a difficult challenge. Since there currently exists no system for setting one's privacy preferences for public IoT scenarios, designers must rely on existing data such as the Lee and Kobsa [12] dataset to inform the design of these interfaces. Moreover, even for the simplified scenarios in this dataset, a privacy-setting interface will likely be complex, as it requires users to navigate settings for 7 types of recipients (**who**), 24 types of information (**what**), 4 different locations (**where**), 6 purposes (**reason**), and decide whether they want to allow the collection once or continuously (**persistence**). 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.

### 4.4.1 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 5.3. 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.

### 4.4.2 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 4.2), we can create a "smart default" setting that is 73.10% accurate on average. In this version, the IoT settings for all devices are set to 'off', except for 'My own device', which will be set to the middle option. Table 4.7 shows the default settings at deeper levels. As this default setting is on average only 73.10% accurate, we expect users to still change some of their settings. They can do this by navigating the manual settings interface.

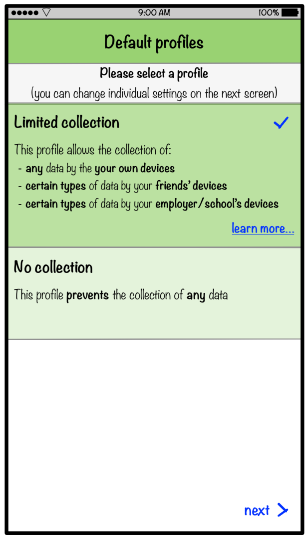
### 4.4.3 Smart Profiles

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 4.4), we can attain an accuracy of 81.54%. Screen 1 in Figure 5.3 shows a selection screen where the user can choose between these profiles. The "Limited collection" profile allows the collection of any information by the user's own devices, their friends' devices, their employer/school's devices, and devices of nearby businesses. Devices of colleagues are only allowed to collect information for certain reasons. The "Limited collection, personal devices only" profile only allows the collection of certain types of information by the user's own devices. The "No collection" profile does not allow any data collection to take place by default.

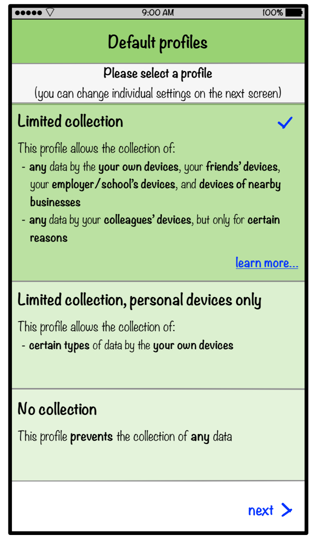
Once the user chooses a profile, they will move to the manual settings interface (Screens 2–4), where they can further change some of their settings.

## 4.5 Summary

In this chapter, we have presented the following:




(a) 2-profile choice interface




(b) 3-profile choice interface

- 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 [12] 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 5

# Recommending Privacy Perference for Household IoT

## 5.1 Introduction

In Chapter 4, we have discussed recommending privacy preference for general IoT users. In this chapter, we present the work completed to date in the areas of designing for privacy for Household IoT. We extend and improve upon the previously-developed data-driven approach to design privacy-setting interfaces for users of household IoT devices.

In general IoT scenarios that discussed in Chapter 4, five parameters, (**who, what, reason, persistance, and where**), in total were given to users as the dimensions when they are making privacy decisions. However, these dimensions are not appropriated in household IoT scenarios because of following reasons:

- In Chapter 4, we found that ”where” does not have significant effect on disclosure decisions; also the usage environment of household IoT systems/devices are always in users' home. Moreover, the structure of users' houses are different from case to case, it would be too complicated if we define ”where” to a more finer-granulated level, such as bedroom, kitchen, etc., Hence there there is no need to retain the parameter ”where”.
- “Persistence” of tracking is more relevant in public IoT, where encounters are often ephemeral, hence persistent tracking is less common than in household IoT.

- "storage" and "action" allow us to explore secondary uses of the information; something we learned from the qualitative feedback in our previous study was a prominent concern among users.

Because of the above reasons, we conducted a new user study focusing on household IoT in particular, and further refine our approach to allow us to create more carefully tailored user interfaces. 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 [?]. This results in more complex decisions, and thereby advances our previous approach.

The main contributions of our paper are:

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

## 5.2 Experimental Setup

To develop our data-driven design approach, we collected a new dataset of users' privacy behaviors in various IoT contexts. In this section, we first discuss the factorial procedure by which we developed 4608 highly specific IoT scenarios, as well as the questions we asked participants to evaluate these scenarios. We then describe the participant selection and experimental procedures used to collect over 13500 responses from 1133 participants.

### 5.2.1 Contextual Scenarios

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

The scenarios asked participants to imagine that they were owners and active users of the presented IoT devices, trying to decide whether to turn on or off certain functionalities and/or data sharing practices. To avoid endowment effects, the scenarios themselves made no indication as to whether the functionality was currently turned on or off (such endowment effects were instead introduced by manipulating the framing of the Decision question; see section 5.2.2). An example scenarios is: *"Your smart TV (Who) uses a camera (What) to give you timely alerts (Purpose). The data is stored locally (Storage) and used to optimize the service (Action)."* This scenario may for example represent a situation where the smarthome system has detected (via camera) a delivery of package and then alerts the user (via the smart TV) about its arrival. In this particular scenario we note that the video data is stored locally to optimize service; this could mean that the smarthome system uses the video stream to (locally) train a package detection algorithm. Similarly, another example of scenario is: *"Your Smart Assistant uses a microphone to detect your location in house. The data is stored on a remote server and shared with third parties to recommend you other services."* Similarly, this scenario could represent a situation where the smarthome has detected (via microphone) it's user's location in the house and this information is shared to smart assistant. In the scenario, the data is stored on remote server and shared with third parties so that it can recommend additional services (like weather or local transportation) via third parties to the user.

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

The parameters used in the current study deviate from the ones in the Lee and Kobsa [12] dataset. In our previous work we observed that the *Where* parameter in this dataset did not have a significant effect on user decision making [?], hence we removed it from the scenarios in the current study. Likewise, in public IoT encounters are often ephemeral, so persistent tracking is rather uncommon. Hence, we removed *Persistence* of tracking from the scenarios as well, since this parameter is much more relevant in public IoT than in household IoT. The original *Reason* parameter is similar to the current *Purpose* and *Action* parameters, although the reasons/purpose for tracking are obviously different in public IoT than in household IoT. Moreover, we learned from the qualitative feedback in our previous study that the secondary use of information was a prominent concern among users of IoT systems. Hence, we consider *Purpose* as the primary purpose of tracking, separate from *Action*, a secondary purpose that requires *Storage*—a parameter we added because it is possible for household IoT systems to operate (and thus store data) locally, and because the sharing of data with third parties is not as common in household IoT as in public IoT.

### 5.2.2 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. A screenshot of the questions asked about each scenario is depicted in Figure **??** in the Appendix.

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).

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

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

### 5.2.3 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, average accuracy of ¿ 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 (see below).

The study participants represented a wide range of ages, with 9 participants less than 20 years old, 130 aged 20-25, 273 aged 25-30, 418 aged 30-40, 175 aged 40-50, 80 aged 50-60, and 43 participants over 60 years old (5 participants did not disclose their age). This significant increase in participants over the Lee and Kobsa [12] 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 depicted in Figure **??** in the Appendix. If they got any of these questions wrong, they would be asked to read the transcript of the video and re-answer the questions. The transcript is depicted in Figure **??** in the Appendix.

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", see Figure **??** in the Appendix), and there was an additional attention check question asking participants about the remaining time to finish the study (which was displayed right there on the same page, see **??** in the Appendix). Participants rushing through the experiment and/or repeatedly failing the attention check questions were removed from the dataset.

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

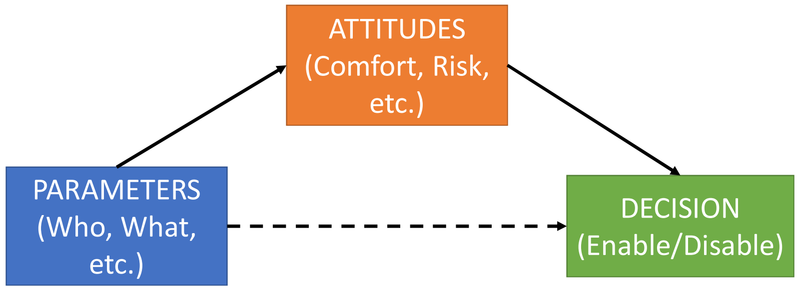



Figure 5.1: Different tests conducted for mediation analysis

## 5.3 Inspecting Users' Decisions

In this section we explain the different regression analyses performed on the dataset to understand how different scenario parameters affected the decisions made by participants. We begin by explaining the effects of scenario parameters on participants' decision to enable or disable the feature mentioned in the scenario. Similar to Bahirat et. al., we also present the results of the mediation analysis, which are on the lines of attitude-behavior models [**?**, 1]. As shown in Figure 5.1, we test whether participants' attitudes mediate the effects of the scenario parameters on their decisions. This mediation analysis involves the following tests:

**Test 1**: The effect of parameters (Who, What, Purpose, Storage, Action) on attitudes (Risk, Comfort, Appropriateness, Expectedness and Usefulness).

**Test 2**: The effect of attitudes on decision.

**Test 3**: The effect of both parameters *and* attitudes on decision.

If, tests 1 and 2 are significant and test 3 reveals a drastic reduction in the conditional direct effect of parameters, then we can say that the effects of scenario parameters on participant's decision are mediated by their attitudes [**?**].

Finally, we present a post-hoc analysis of differences between individual levels of the parameters on attitudes and decision.

### 5.3.1 Effect of scenario parameters on decision

To understand the effect of the scenario parameters on participants' allow/reject decision, we developed a *generalized linear mixed effects regression* (*glmer*) with a random intercept (to account for repeated measures on the same participant) and a logit link function (to account for the fact

Table 5.2: Effect of scenario parameters on decision

| Model | $\chi^2$ | *df* | *p*-value |
|---|---|---|---|
| $decision \sim (1\|sid)$ | | | |
| +storage | 1487.76 | 2 | $< .0001$ |
| +purpose | 206.97 | 11 | $< .0001$ |
| +what | 202.48 | 3 | $< .0001$ |
| +who | 195.91 | 7 | $< .0001$ |
| +action | 77.20 | 3 | $< .0001$ |
| *Interactions* | | | |
| +what:who | 138.03 | 77 | $< .0001$ |
| +who:purpose | 87.92 | 21 | $< .0001$ |
| +what:purpose | 68.30 | 33 | .0002 |

that the outcome variable is binary). We used a forward stepwise approach, where we added the strongest remaining parameter into the model into the model at each step and then comparing it using ANOVA tests against the previous model. If new parameter makes a significant improvement to the previous model, it has a significant overall effect on the outcome variable. Once all significant main effects are added to the model, two-way interaction effects are tested one by one.

Table 5.2 shows the effects of the parameters on the allow/reject decision. All parameters had a significant effect. Particularly, **Storage** had the strongest effect on participants' decisions, followed by **What**, **Who** and **Purpose** (all similar) and finally **Action**.

Moreover, we find many significant interaction effects, but some of them are not substantial compared to the main effects[2]. Substantial two-way interaction effects were observed between **Who**, **What** and **Purpose**. It should be noted that the interactions are added separately, not accumulatively. This reduces overfitting and multicollinearity.

### 5.3.2 Effect of scenario parameters on attitudes

Test 1 of the mediation model is a test of the effect of the scenario parameters on participants' attitudes. For this we developed a separate *linear mixed effects regression model* (*lmer*) model with a random intercept (to account for repeated measures on the same participant) for each dependent variable (Risk, Comfort, Appropriateness, Expectedness and Usefulness), using the scenario parameters as independent variables. As in the previous section, we took a forward stepwise approach.

Tables 5.3-5.7 show the effects of the parameters on the different attitudes. All param-

[2]Very small but still significant interaction effects are a common occurrence in the analysis of large datasets.

Table 5.3: Effect of scenario parameters on appropriateness

| Model | *df* | $Chi.Sq.$ | *p*-value |
|---|---|---|---|
| $appropriateness \sim (1\|sid)$ | 3 | | |
| +storage | 5 | 2346.19 | $< .0001$ |
| +what | 16 | 398.63 | $< .0001$ |
| +purpose | 19 | 359.98 | $< .0001$ |
| +who | 26 | 179.09 | $< .0001$ |
| +action | 29 | 91.05 | $< .0001$ |
| *Interactions* | | | |
| +what:who | 106 | 167.01 | $< .0001$ |
| +who:purpose | 50 | 113.73 | $< .0001$ |
| +what:purpose | 62 | 55.67 | .0081 |

Table 5.4: Effect of scenario parameters on comfort

| Model | *df* | $Chi.Sq.$ | *p*-value |
|---|---|---|---|
| $comfort \sim (1\|sid)$ | 3 | | |
| +storage | 5 | 2822.57 | $< .0001$ |
| +what | 16 | 391.10 | $< .0001$ |
| +purpose | 19 | 381.69 | $< .0001$ |
| +action | 22 | 113.68 | $< .0001$ |
| +who | 29 | 90.57 | $< .0001$ |
| *Interactions* | | | |
| +what:who | 106 | 132.86 | $< .0001$ |
| +who:purpose | 50 | 89.20 | $< .0001$ |
| +what:purpose | 62 | 58.24 | .0043 |

eters had a significant effect on all attitudes. Substantial two-way interaction effects were again observed between **Who**, **What** and **Purpose**. Again, the interactions are added separately, not accumulatively.

### 5.3.3 Effect of attitudes on decision

Test 2 of the mediation model is a test of the effect of participants' attitudes on their allow/reject decision. We perform this test by creating a *glmer* model with a random intercept and a logit link function. Using a forward stepwise approach, we find that all attitudes except **Expectedness** have a significant effect on decision (see the top part of Table 5.8). Specific effects are as follows:

- Each 1-point increase in **Comfort** (measured on a 7-point scale) results in a 2.30-fold increase in the odds that the participant will allow the scenario ($p < 0.001$).
- Each 1-point increase in **Usefulness** results in a 2.09-fold increase in the odds that the par-

Table 5.5: Effect of scenario parameters on risk

| Model | *df* | $Chi.Sq.$ | $p$-value |
|---|---|---|---|
| $risk \sim (1\|sid)$ | 3 | | |
| +storage | 5 | 47240.72 | $<$ .0001 |
| +purpose | 16 | 421.08 | $<$ .0001 |
| +action | 19 | 355.65 | $<$ .0001 |
| +who | 26 | 81.35 | $<$ .0001 |
| +what | 29 | 70.64 | $<$ .0001 |
| *Interactions* | | | |
| +what:who | 106 | 77.14 | 0.0017 |
| +who:purpose | 50 | 19.91 | $<$ .0001 |
| +what:purpose | 62 | 37.19 | 0.0352 |

Table 5.6: Effect of scenario parameters on usefulness

| Model | *df* | $Chi.Sq.$ | $p$-value |
|---|---|---|---|
| $usefulness \sim (1\|sid)$ | 3 | | |
| +what | 5 | 939.91 | <.0001 |
| +storage | 12 | 457.36 | <.0001 |
| +purpose | 23 | 401.18 | <.0001 |
| +action | 26 | 328.88 | <.0001 |
| +who | 29 | 117.57 | <.0001 |
| *Interactions* | | | |
| +what:who | 106 | 214.48 | <.0001 |
| +who:purpose | 50 | 184.48 | <.0001 |
| +what:purpose | 62 | 85.39 | <.0001 |

Table 5.7: Effect of scenario parameters on expectedness

| Model | *df* | $Chi.Sq.$ | $p$-value |
|---|---|---|---|
| $expectedness \sim (1\|sid)$ | 3 | | |
| +storage | 5 | 841.24 | $<$ .0001 |
| +who | 16 | 425.92 | $<$ .0001 |
| +what | 19 | 422.31 | $<$ .0001 |
| +purpose | 22 | 231.98 | $<$ .0001 |
| +action | 29 | 29.45 | $<$ .0001 |
| *Interactions* | | | |
| +what:who | 106 | 262.80 | $<$ .0001 |
| +who:purpose | 50 | 138.73 | $<$ .0001 |
| +what:purpose | 62 | 84.89 | $<$ .0001 |

Table 5.8: Effect of attitudes on decision; conditional effects of parameters are added subsequently

| Model | $\chi^2$ | *df* | *p*-value |
|---|---|---|---|
| $decision \sim (1\|sid)$ | | | |
| +Comfort | 7934.72 | 1 | $<$ .0001 |
| +Usefulness | 1249.51 | 1 | $<$ .0001 |
| +Appropriateness | 149.15 | 1 | $<$ .0001 |
| +Risk | 10.90 | 1 | .0009 |
| +Expectedness | 1.62 | 1 | .201 |
| *Adding Scenario Parameters* | | | |
| +action | 0.332 | 3 | 0.953 |
| +what | 13.871 | 11 | 0.2401 |
| +purpose | 3.60 | 3 | 0.3069 |
| +storage | 14.57 | 2 | 0.0006 |
| +who | 24.53 | 7 | 0.0009 |

ticipant will allow the scenario ($p < 0.001$).

- Each 1-point increase in **Appropriateness** results in a 44% increase in the odds that the participant will allow the scenario ($p < 0.001$).
- Each 1-point increase in **Risk** results in a 14% decrease in the odds that the participant will allow the scenario ($p < 0.001$).
- **Expectedness** had no signficant influence on the participant's decision (p = 0.201).

The strongly significant relationship between attitudes and behavior is interesting in light of the "privacy paradox" [?], an attitude-behavior gap that has been studied extensively by privacy researchers. Arguably, the privacy paradox is an artifact of the fact that *general* privacy concerns (which are commonly high) do not match *specific* behaviors (which subsequently ignore these general concerns). Since in our study attitudes and behaviors are measured at the same contextual level, their relationship is much stronger than in other studies. This may explain why we do not find an attitude-behavior gap.

### 5.3.4 Mediation analysis

With tests 1 and 2 of our mediation analysis confirmed, we conduct test 3 by adding the scenario parameters to the *glmer* of participants' decisions on their attitudes. The bottom half of Table 5.8 shows these conditional effects of the significant scenario parameters on participants' allow/reject decision, controlling for their attitudes. **Action**, **What** and **Purpose** are no longer

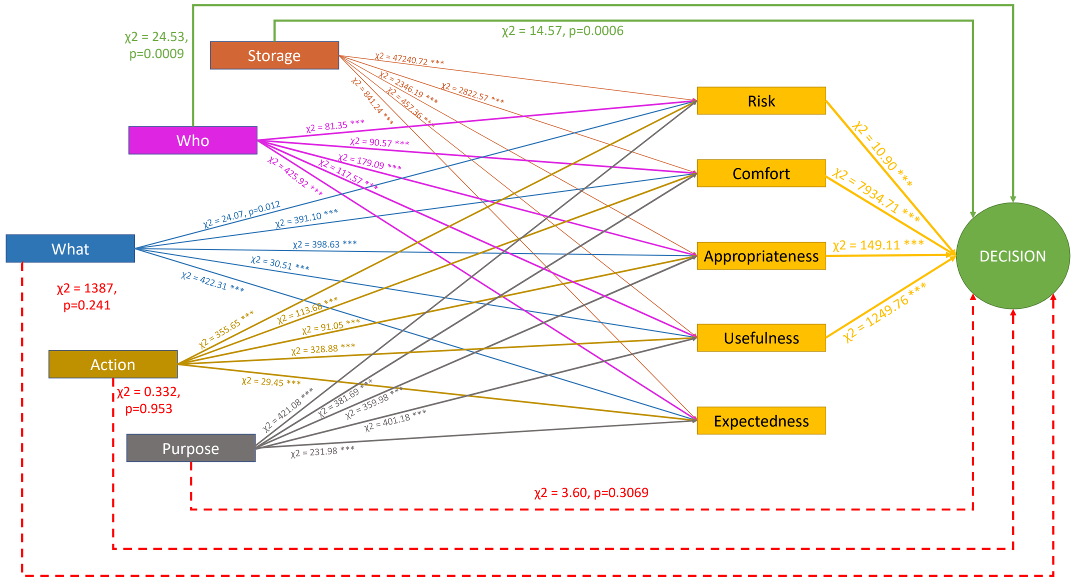



Figure 5.2: Final mediation model.

significant in this model, suggesting that these effects are *fully mediated* by participants' attitudes. **Storage** and **Who** are still significant, but their conditional effects are smaller than their marginal effects on decision (without controlling for attitude, see Table 5.2). Their $chi^2$s are reduced drastically by 98% and 87%, respectively. Overall, there was a substantial mediation effect. Figure 5.2 shows the final model mediation model.

### 5.3.5 Post-hoc Results

To understand the effects of different values of each parameter on participants' various attitudes and their allow/reject decision, we conducted post-hoc tests using Tukey's method to adjust $p$-values to account for familywise error. This subsection highlights the key insights from these tests. For an overview of the differences between parameter values, the reader is invited to visually inspect them by referring to Figures **??**-**??** in the Appendix.

**Storage**: Participants perceive more risk ($d$ range $= [0.568, 1.707]$, all $ps < .001$), are less comfortable ($d$ range $= [0.538, 1.741]$, all $ps < .001$) and find it inappropriate ($d$ range $= [0.436, 1.550]$, all $ps < .001$) when their information is shared to 'third parties' or 'stored on a remote server' as compared to when it is stored 'locally'. Participants also found it less useful to share their information with third parties as compared to storing it locally or on a remote server ($d$

range = $[0.28, 1.02]$, $p < .001$). Interestingly, participants expected it less that the information is stored locally rather than stored on remote server or shared to third parties ($d$ range = $[0.212, 0.894]$, all $p$s $< .001$). Finally, the odds of enabling a feature when information is stored locally were 1.96 times higher than when information is stored on a remote server ($p < .001$) and 8.36 times higher than when information is shared with third parties ($p < .001$).

**Action**: Participants were less comfortable ($d$ range = $[0.158, 0.348]$, all $p$s $< .001$) and found it more risky ($d$ range = $[0.145, 0.262]$, all $p$s $< .001$) when their information is used to give them recommendations instead of optimizing services or giving them insight into their behavior. Sharing information was also found less useful ($d = 0.293$, $p < .001$) and less appropriate ($d = 0.256$, $p < .001$) for recommendation purposes as opposed to when the scenario did not specify any purpose. Participants also expected it less ($d = 0.123$, $p = .0021$) when their information was being shared for recommendation purposes as opposed to when the scenario did not specify any purpose. Finally, the odds of enabling a feature for recommendation purposes were 1.53 times lower as opposed to when the scenario did not specify any purpose ($p < .001$). Additionally, the odds of enabling a feature for optimization purposes were 1.65 times higher than for recommendation purposes ($p < .001$) and 1.26 times higher than for giving behavioral insights ($p < .001$).

**Purpose**: Participants found it inappropriate ($d$ range = $[0.343, 0.411]$, all $p$s $< .001$) when information is collected for the purpose of detecting their presence in the house as compared to the purposes of automating operations or giving timely alerts, and it was even more inappropriate to collect information for the purpose of detecting their location in the house ($d$ range = $[0.163, 0.574]$, all $p$s $< .001$). Participants also found it more risky when information is used for location detection as compared to presence detection ($d = 0.598$, $p < .001$), but they found it less risky to share information for the purpose of giving timely alerts or for automating operations ($d$ range = $[0.550, 0.601]$, $p$ range = $[0.002, 0.004]$). Participants also found it more useful when information is collected for the purpose of providing alerts ($d = 0.558$, $p < .001$) or for automating operations ($d = 0.603$, $p < .001$) compared to the purpose of detecting their location in the house. Finally, the odds of enabling a feature were 1.29 times higher for detecting their presence in house than for detecting their location ($p = 0.0002$). Moreover, the odds of enabling a feature for the purpose of giving timely alerts and automating operations were 1.59 ($p < .001$) and 1.65 ($p < .001$) times higher respectively.

**Who**: Participants expected it more that their smart security systems will access information as compared to other devices such as their smart HVAC, TV, alarm and washing machine ($d$

range = $[0.267, 0.618]$, all $p$s $< .001$). Users perceived data access by their security systems as more useful compared other devices like their smart refrigerator, washing machine, TV and HVAC ($d$ range = $[0.386, 0.627]$, all $p$s $< .001$). Participants were more comfortable ($d = 0.196$, $p = .002$) and found it less risky ($d = 0.263$, $p < .001$) for their security systems to access collected data as compared to their smart lighting systems. Also, participants were more comfortable ($d$ range = $[0.173, 0.356]$, all $p$s $< .05$) and found it less risky ($d$ range = $[0.256, 0.338]$, all $p$s $< .05$) for their lighting systems to access collected data compared to their smart assistant, TV and alarm clock. Finally, the odds of users enabling access to their smart security system were higher than to their smart refrigerator and washing machine by 1.8 times($p < .001$), their smart TV by 1.7 times ($p < .001$) and their smart alarm clock by 1.6 times ($p < .001$). We found similar results for participants' smart assistant which had odds higher than their smart TV (1.76 times higher, $p < .001$), their smart alarm clock (1.68 times higher, $p < .001$), their smart washing machine (1.90 times higher, $p < .001$) and their smart refrigerator (1.85 times higher, $p < .001$).

**What**: This parameter had twelve different values and there were numerous combinations that were significant when we checked the post-hoc effects. We limit our discussion to the differences between the 'Smart Assistant' and the other values of this parameter, because these specific differences are consistently significant. The reader is invited to inspect Figure **??** in the Appendix for other differences. Participants found it more appropriate ($d$ range = $[0.213, 0.756]$, all $p$s $< .001$) and useful ($d$ range = $[0.365, 0.683]$, all $p$s $< .01$) when information collected by their smart assistant was being accessed as compared to other devices like cameras or microphones. The participants also found it less risky ($d$ range = $[0.385, 0.759]$, all $p$s $< .05$) and were more comfortable ($d$ range = $[0.430, 0.821]$, all $p$s $< .01$) to grant access to information collected by their smart assistant than their camera or microphone. Participants also expected more to share information collected by their smart assistant as compared to other devices such as cameras ($d = 0.62$, $p < .01$), microphones ($d = 0.39$, $p < .01$), or their smart alarm clock ($d = 0.21$, $p = .027$). The odds of giving access to information collected by their smart assistant were higher than for cameras by 2.7 times ($p < .001$), microphones by 1.8 times ($p < .001$), their Smart TV by 1.15 times ($p < .001$) and their smart washing machine by 1.8 times ($p < .001$).

### 5.3.6 Defaults and Framing

As outlined in section 5.2.2, 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. We analyze the effects of defaults and framing in a separate paper [2]. In short, 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. For a more thorough discussion of the effects of defaults and framing, we refer the reader to [2].

### 5.3.7 Discussion

We split this section in two parts: First, we discuss the consequences of our analyses—and especially our post hoc test results—for the development and adoption of household IoT devices. Second, we discuss how our results can inform the design of household IoT privacy-setting interfaces.

#### 5.3.7.1 Consequences for the development and adoption of household IoT devices

In the introduction we mentioned that privacy risk is an increasingly important barrier to the adoption of household IoT devices. Interestingly, though, in our study Comfort, Usefulness and Appropriateness had a stronger effect on users' allow/reject decisions than Risk. This suggests that IoT devices with a trust-inspiring design, a strong value proposition, and a clear explanation of the appropriateness of their data collection practices can overcome initial perceptions of privacy risk.

The trade-off between Comfort, Usefulness and Appropriateness embodies an interesting trade-off: Usefulness is associated with the utility of a feature, whereas Appropriateness is a contextual evaluation (is this acceptable given the *situation*?) and Comfort is a self-relevant evaluation (is this acceptable for *me*?).

The interaction between **What**, **Who**, and **Purpose** also suggests that users make context-relevant evaluations: scenarios are not accepted based on the sum of their components; rather, certain combinations of devices and purposes are more acceptable than others. While this is outside the scope of the current paper, future work could look into this context-dependency to find specific synergistic combinations.

The **Storage** parameter had the most significant influence on participants' decision and all attitudes, but most prominently on Risk. ($chi^2$ = 47240.72, $p < .001$). This indicates that users' risk perceptions are mostly dependent on the way household IoT systems store and share their data. Household IoT device manufacturers who want to reduce risk perceptions may want to opt for storing all data locally instead of on a remote server (something users are actually more likely to expect).

Finally, the **Action** parameter had the least significant influence. Arguably, once users allow information to be collected, they care less about how exactly it is being used (or possibly, they do not expect to be able to control how it is being used).

#### 5.3.7.2 Designing for IoT by prioritizing parameters

The results of our analyses uncover an intuitive reality about our household IoT scenarios, namely, they consist of two somewhat separate parts: On the one hand, there is a device (**Who**) that accesses information collected by another device (**what**), for a purpose certain **Purpose**. At the same time, this the collected information may be stored somewhere (**Storage**) and some **Action** may be performed on it.

For the first aspect, we observed substantial interaction effects between all the three parameters, indicating that users want to make intricate decisions about what information is going where and for what purposes. Specifically, Unlike Bahirat et. al. [**?**], we cannot use an interface with a separate 'layer' for each parameter; the interaction effects suggest that when uses decide on one parameter, they inherently take another parameter into account. Therefore the settings interface for device/sensor management should show all three parameters at the same time to allow users to make these decisions.

For the second aspect, data storage had a very strong impact, while the action had the weakest impact. Additionally, there were no interactions between these two parameters, nor did they interact with any of the other parameters. This suggests that data storage and use can be separated in our privacy-setting interface.

## 5.4 Privacy-Setting Prototype Design

Designers of household IoT privacy-setting interfaces face a difficult challenge. Since there currently exists no centralized system for setting one's household IoT privacy settings, designers must rely on existing data (cf. [12]) or self-collected survey results (cf. this paper) to inform the design of these interfaces. Moreover, these privacy-setting interfaces will likely be complex, as they require users to navigate settings for the collection of various types of data for multiple purposes across various devices.

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*.

In this section we present our prototype, which is based on the observations made from our statistical analysis. Section 5.6 extends this prototype to cover findings from our machine learning analysis to create default privacy profiles, but before we do so, we first want to design an intuitive interface that gives users manual control over their privacy settings. This interface should be able to present a vast amount of settings information in a concise and understandable manner, and allow some users to set their settings with little effort at a coarse level while still allowing others to spend the effort to micro-manage their privacy settings in more detail.

Our statistical analysis (see Section 5.3) reveals what the most significant parameters are in our dataset, as well as which parameters interact with each other. The results show that the *Storage* parameter had by far the strongest effect on participants' decision to enable/disable the smart home feature described in the scenario. After Storage, *Who*, *What* and *Purpose* had similar-sized effects. Moreover, we found fairly strong significant two-way interaction effects between these parameters.

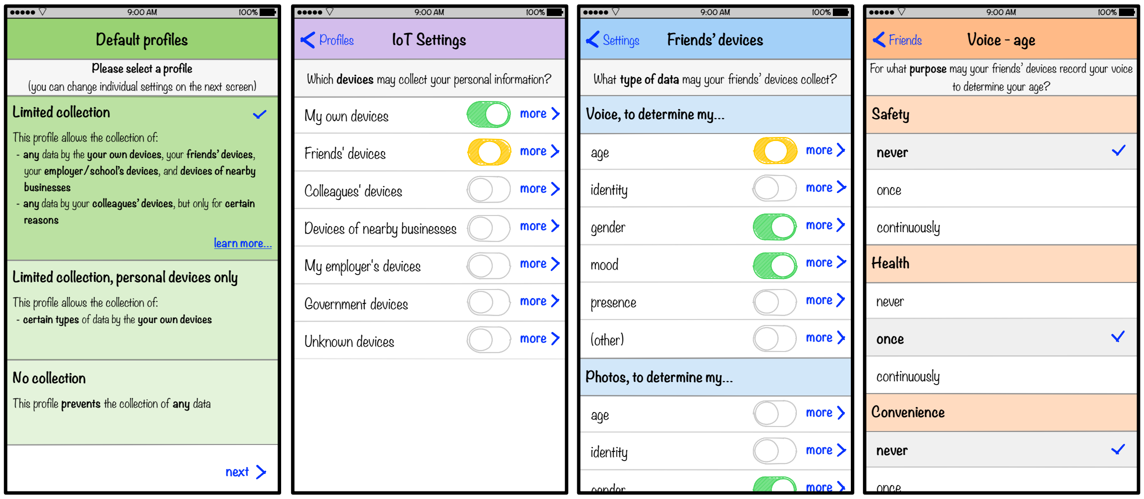



Figure 5.3: From left, screen 1 is the landing page of our manual settings interface, screen 2 is the Device/Sensor Management page, screen 3 shows the explanation when you click on "I want to learn more", and screen 4 is the Data Storage & Use page.

Finally, the *Action* parameter had a weak but still significant effect.

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

**Device/Sensor Management:** This screen (Figure 5.3, screen 2) allows users to control the *Purposes* for which each device (*Who*) is allowed to access data collected by itself, other devices, and the smart home sensors installed around the house (*What*). This screen has a collapsible list of data-collecting devices and sensors (*What*). For each device/sensor, the user can choose what devices can access the collected data (*Who*; in rows), and what it may use that data for (*Purpose*; in columns).

In the example of Figure 5.3, the user does not give the 'Refrigerator' access to information collected by the 'Smart Assistant' for any of the four purposes, while they give the 'Smart TV' access to this data for the purpose of giving 'timely alerts'. In this example the 'Smart Assistant' is allowed to use its own data to 'automate operations' and to 'know your location in your home'.

Showing *Who*, *What* and *Purpose* at the same time allows users to enable/disable specific combinations of settings—the significant interaction effects between these parameters suggest that this is a necessity. The icons for the *Purpose* requirement allow this settings grid to fit on a smartphone or in-home control panel. We expect that users will quickly learn the meaning of these icons, but they can always click on 'I want to know more' to learn their meaning (see Figure 5.3, screen 3).

**Data Storage & Use:** This screen (Figure 5.3, 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 (see Figure **??** in the Appendix), so this presentation is justified. For 'Data Use', the users can choose to enable/disable the use of the collected data for various secondary purposes: behavioral insights, recommendations, service optimization, and/or other purposes.

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

## 5.5 Predicting users' behaviors

In this section we predict participants' *enable/disable* decision using machine learning methods. Our goal is to find suitable default settings for our IoT privacy-setting interface. Consequently, 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. 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. Moreover, by using J48 decision trees, the amount of pruning for the model can be easily manipulated to investigate the trade-off between the accuracy and parsimony. We therefore use J48 throughout our analysis.

Using Java and Weka's Java library [**?**] for modeling and evaluation, we implement progressively sophisticated methods for predicting participants' decisions. After discussing naive (enable/disable all) solutions and One Rule Prediction, we first present a cross-validated tree learning solution that results in a single "smart default" setting that is the same for everyone. Subsequently, we discuss three different procedures that create a number of "smart profiles" by clustering the participants and creating a separate cross-validated tree for each cluster. For each procedure, we try various numbers of clusters and pruning parameters. The solutions with the most parsimonious trees and the highest accuracies of each approach are reported in Table 5.9; more detailed results of the parsimony/accuracy trade-off are presented in Figures 5.7, 5.9, 5.12 and 5.16 throughout the paper, and combined in Figure 5.20.

### 5.5.1 Naive Prediction Model

We start with the naive or "information-less" predictions. Compared to our previous work [**?**], our current dataset shows that it is even less amenable to a 'simple' default setting: it contains 6335 *enable* cases and 7241 *disable* cases, which means that predicting *enable* for every setting gives us a 46.74% prediction accuracy, while making a *disable* prediction for every setting gives us an accuracy of 53.26%. In other words, if we disable all information collection by default, only 53.26% users will on average be satisfied with this default settings. Moreover, such a default setting disallows any 'smart home' functionality by default—arguably not a solution the producers of smart appliances can get behind.

Table 5.9: Comparison of clustering approaches (highest parsimony and highest accuracy)

| Approach | Inital clusters | Final # of profiles | Complexity (avg. tree size/profile) | Accuracy |
|---|---|---|---|---|
| Naive (enable all) | 1 | 1 | 1 | 46.74% |
| Naive (disable all) | 1 | 1 | 1 | 53.26% |
| One Rule (Fig. 5.4) | 1 | 1 | 3 | 61.39% |
| Overall (Fig. 5.7) | 1 | 1 | 8 | 63.32% |
| | 1 | 1 | 264 | 63.76% |
| Attitude-based clustering (Fig. 5.9) | 2 | 2 | 2 | 69.44% |
| | 2 | 2 | 121.5 | 72.66% |
| | 3 | 3 | 2.67 | 72.19% |
| | 3 | 3 | 26.67 | 73.47% |
| | 5 | 4 | 3 | 72.61% |
| | 5 | 4 | 26 | 73.56% |
| Agglomerative clustering (Fig. 5.12) | 1133 | 4 | 2 | 79.4% |
| | 1133 | 5 | 2.4 | 80.35% |
| | 1133 | 6 | 3.17 | 80.60% |
| Fit-based clustering (Fig. 5.16) | 2 | 2 | 2 | 74.43% |
| | 2 | 2 | 151.5 | 76.72% |
| | 3 | 3 | 7 | 79.80% |
| | 3 | 3 | 65.33 | 80.81% |
| | 4 | 4 | 9.25 | 81.88% |
| | 4 | 4 | 58.25 | 82.41% |
| | 5 | 5 | 4.2 | 82.92% |
| | 5 | 5 | 51.4 | 83.35% |

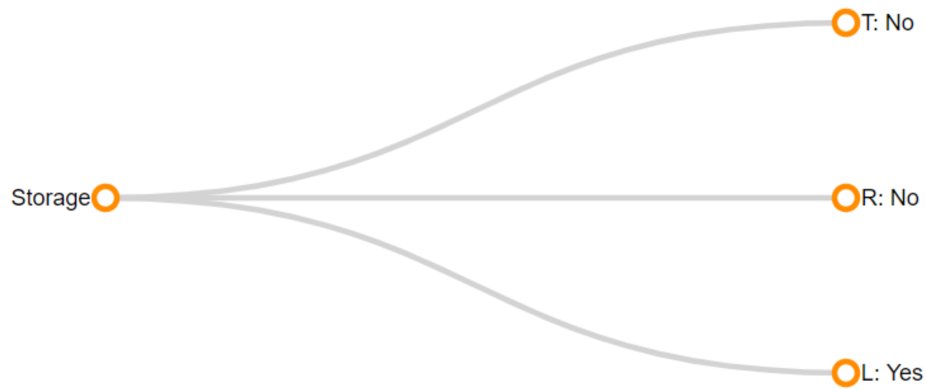



Figure 5.4: A "smart default" setting based on the "One Rule" algorithm (4 nodes, accuracy: 61.39%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

Table 5.10: Confusion matrix for the One Rule prediction

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

### 5.5.2 One Rule Prediction

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

As shown in Figure 5.4, the OneR model predicts users' decision solely based on the **Storage** parameter with an accuracy of 61.39%. Based on this model, if we enable all information-sharing *except* with third parties, we will on average satisfy 61.39% of users' preferences—a 15.3% improvement[3] over the naive "disable all" default. Note, though, that this default setting is overly permissive, with 3262 false positive predictions (see Table 5.10).

### 5.5.3 Overall Prediction

Moving beyond a single parameter, we create a "smart default" setting by predicting the *enable/disable* decision with all scenario parameters using the J48 decision tree algorithm. The resulting tree has an accuracy of 63.76%. As shown in Figure 5.5, this model predicts users' decision

[3] 61.39 / 53.26 = 1.153

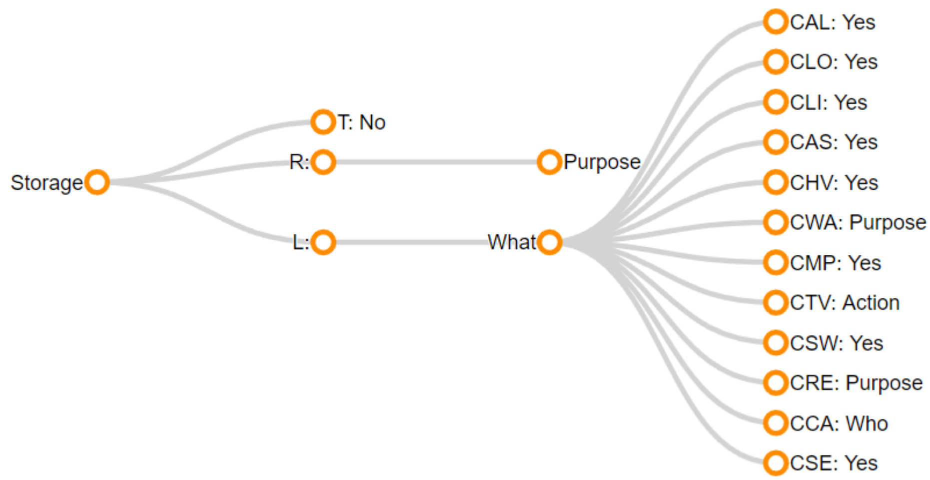



Figure 5.5: A "smart default" setting with 264 nodes (accuracy: 63.76%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

Table 5.11: 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 [**?**] contained only 49 nodes, whereas the "smart default" for our current dataset has 264 nodes. Compared to *One Rule* algorithm, which only has 4 nodes in its decision tree and is thus much easier to explain, the accuracy improvement of Smart Default is only 3.8%. This highlights the trade-off between parsimony and prediction accuracy that we have to make when developing "smart default" settings. On the upside, though, the prediction of the J48 decision tree algorithm is more balanced, with a roughly equal number of false positives and false negatives (see Table 5.11).

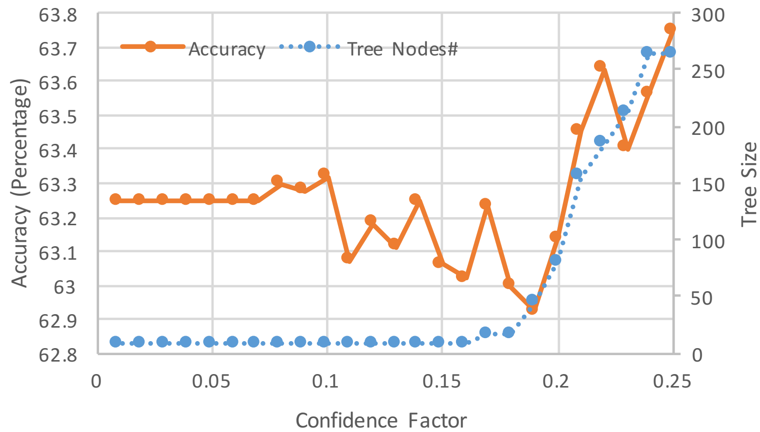



Figure 5.6: Accuracy and parsimony (tree size) of the smart default change as a function of Confidence Factor

To better understand the parsimony/accuracy trade-off, we vary the degree of model pruning to investigate the effect of increasing the parsimony (i.e., more trimming) on the accuracy of the resulting “smart default” setting. The parameter used to alter the amount of post-pruning performed on the J48 decision trees is called Confidence Factor ($CF$) in Weka, and lowering the Confidence Factor will incur more pruning. We tested the J48 classifier with a Confidence Factor ranging from 0.01 to 0.25 (the default setting in Weka) with an increments of 0.01.

Figure 5.6 displays the accuracy and the size of the decision tree as a function of the Confidence Factor. The X-axis represents the Confidence Factor; the left Y-axis and the orange line represent the accuracy of the smart default setting; the right Y-axis and the dotted blue line represent the size of the decision tree for that setting. The highest accuracy, 63.75%, is achieved with the 264-node decision tree produced by $CF = 0.25$. The lowest accuracy, 62.9%, is achieved with the 44-node decision tree produced by $CF = 0.19$. When $CF \leq 0.16$, the decision tree contains only 8 nodes. The 8-node profile with the highest accuracy is produced by $CF = 0.10$ with an accuracy of 63.32%.

Figure 5.7 summarizes accuracy as a function of parsimony. The X-axis represents the number number of nodes in the decision tree (more = lower parsimony); the Y-axis represents the accuracy of the decision tree. The figure shows the most accurate J48 solution for any given tree size, and includes the One Rule and Naive predictions for comparison. Reducing the tree from 264 to 8 nodes incurs a negligible 0.67% reduction in accuracy. This decision tree is shown in Figure 5.8, and is still 3.1% better than the One Rule prediction model and 18.9% better than the naive “disable

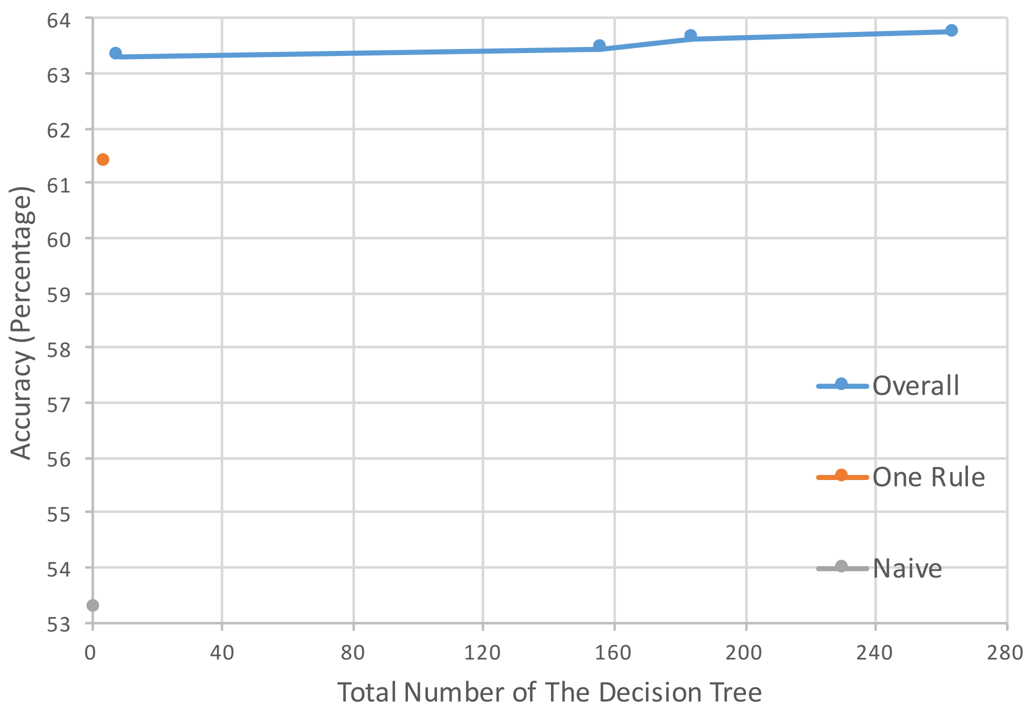



Figure 5.7: Parsimony/accuracy comparison for Naive, One Rule, and Overall Prediction

all" default. This more parsimonious "smart default" setting can easily be explained to users as follows:

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

While the "smart default" setting makes a considerable improvement over a naive default, there is still a lot of room for improvement—even our best prediction model only correctly models on average 63.76% of the user's desired settings. This should come at no surprise, as one of the most consistent findings in the field of privacy is that people differ substantially in their privacy preferences [11]. 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 [**?**]. Our previous work therefore moved beyond "smart default" settings by clustering participants with similar privacy preferences and creating a

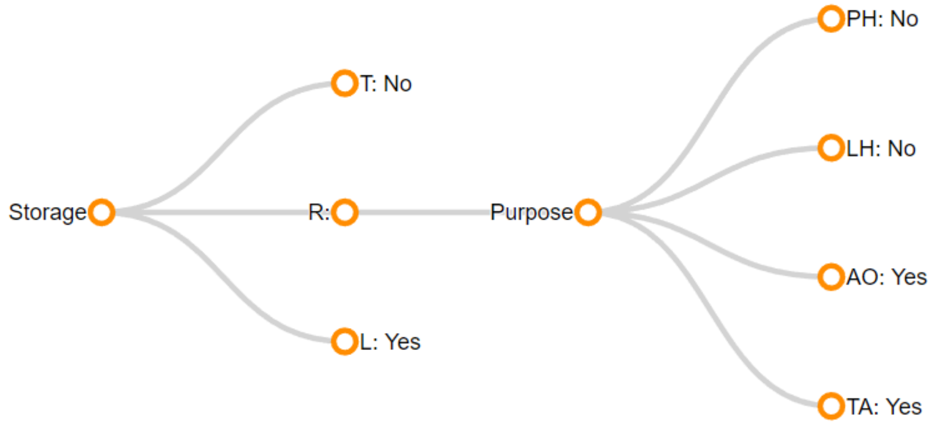



Figure 5.8: A "smart default" setting with only 8 nodes (accuracy: 63.32%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

set of "smart profiles" covering each of the clusters [?]. The idea is that the accuracy of the tree for each cluster will likely exceed the accuracy of our overall prediction model.

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

### 5.5.4 Attitude-Based Clustering

As shown in Figure 5.1, our statistical results indicate that the effects of scenario parameters on users' decisions are mediated by their attitudes (Risk, Comfort, Appropriateness, Expectedness and Usefulness). Therefore, our first attempt to develop "smart profiles" is to cluster participants with similar attitudes towards the 12 scenarios they evaluated. We averaged the values per attitude across each participant's 12 answers, and ran a *k-means* clustering algorithm to divide them into 2, 3, 4, 5, and 6 clusters. We then added the participants' cluster assignments back to our original dataset, and ran the J48 decision tree algorithm on the dataset with this additional *Cluster* attribute for each number of clusters, varying the Confidence Factor from 0.01 to 0.25 with increments of 0.01. The results are summarized in Figure 5.9, 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


Figure 5.9: Parsimony/accuracy comparison for attitude-based clustering

each subtree/cluster. Note that for some solutions two clusters end up with the same decision tree, which effectively reduces the number of profiles by 1.

For the 2-cluster solutions (the blue line in Figure 5.9), the highest accuracy is 72.66%, which is a 14.0% improvement over the best single "smart default" setting. However, this tree has an average of 121.5 nodes per profile. In comparison, the most parsimonious solution has only 1 node ("disable all") for one of the clusters, and 3 nodes ("disable sharing with third parties") for the other cluster (see Figure 5.10). This solution still has an accuracy of 69.44%, which is still an 8.9% increase over the best single "smart default" setting.

For the 3-cluster solutions (the orange line in Figure 5.9), the highest accuracy of 73.47% is achieved by a set of trees with 26.67 nodes on average (a minimal improvement of 1.1% over the best 2-cluster solution, but with simpler trees), while the most parsimonious solution has a "disable all" and an "enable all" tree, plus a tree that is the same as the most parsimonious smart default setting (see Figure 5.8). This solution has an accuracy of 72.19%, which is a 4.0% increase over the most parsimonious 2-cluster solution.

The 4-cluster solutions (the grey line in Figure 5.9) all result in "over-clustering": all solu-

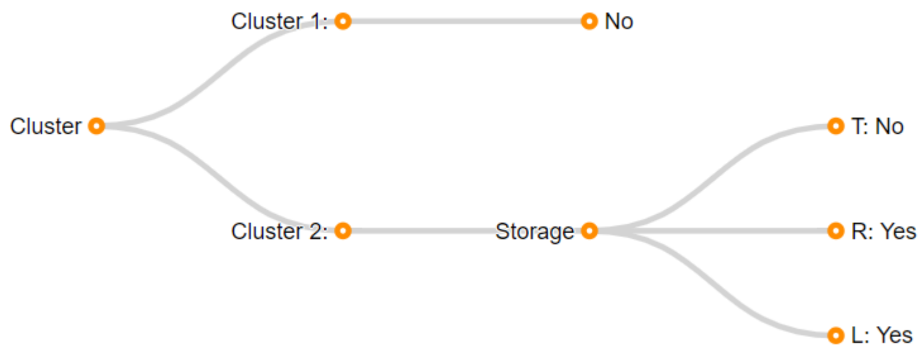



Figure 5.10: The most parsimonious 2-profile attitude-based solution (2 nodes/profile, accuracy: 69.44%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

tions based on the 4-cluster *Cluster* parameter result in two profiles with the same subtree, effectively resulting in a 3-profile solution. The accuracy of these solutions is actually lower than the accuracy of similar 3-cluster solutions, so we will not discuss them here.

The 5-cluster solutions (the yellow line in Figure 5.9) are also "over-clustered", resulting in 4 profiles. The highest accuracy of 73.56% is achieved by a set of trees with 26 nodes—this is about the same accuracy and parsimony as the most accurate 3-cluster solution. The same holds for the most parsimonious 5-cluster solution, which has a similar accuracy and parsimony as the most parsimonious 3-cluster solution.

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

Reflecting upon the attitude-based clustering results, we observe in Figure 5.9 that there is indeed a trade-off between accuracy and parsimony: the most parsimonious results are less accurate, but the most accurate results are more complex. Moreover, the 2-profile solutions are about 5% less accurate than the 3-profile solutions at any level of complexity. The 4-profile solutions do not improve the solution much further, though.

The 3-profile solution with an average of 18.33 nodes per profile and 73.26% accuracy provides a nice compromise between accuracy and parsimony. Part of this decision tree is shown in Figure 5.11: it contains one "disable all" profile, one "enable all" profile, and a more complex profile with 55 nodes that disallows sharing with third parties and allows remote and local storage depending on the purpose (not further shown).

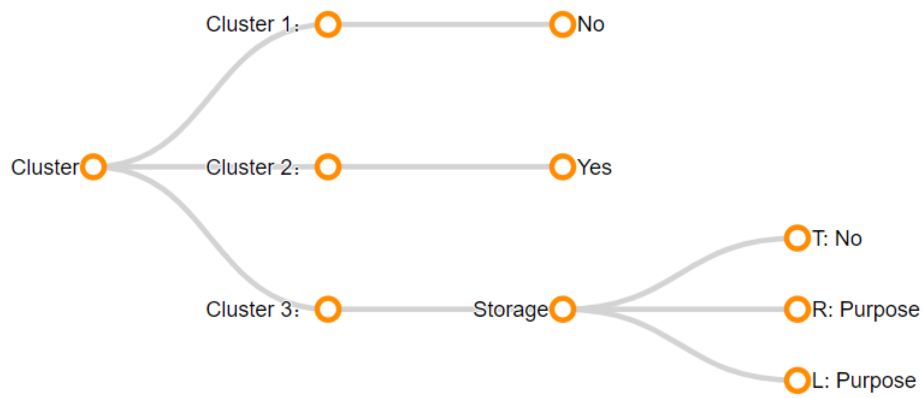



Figure 5.11: A 3-profile solution example of attitude-based clustering (18.33 nodes/profile, accuracy: 73.26%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

### 5.5.5 Agglomerative Clustering

The attitude-based clustering approach requires knowledge of users' attitudes towards the household IoT information-sharing scenarios, which may not always be available. We developed an alternative method for finding "smart profiles" that follows a hierarchical bottom-up (or agglomerative) approach, using users' decisions only. This method first fits a separate decision tree for each participant, and then iteratively merges these trees based on similarity. In our previous work [**?**] 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

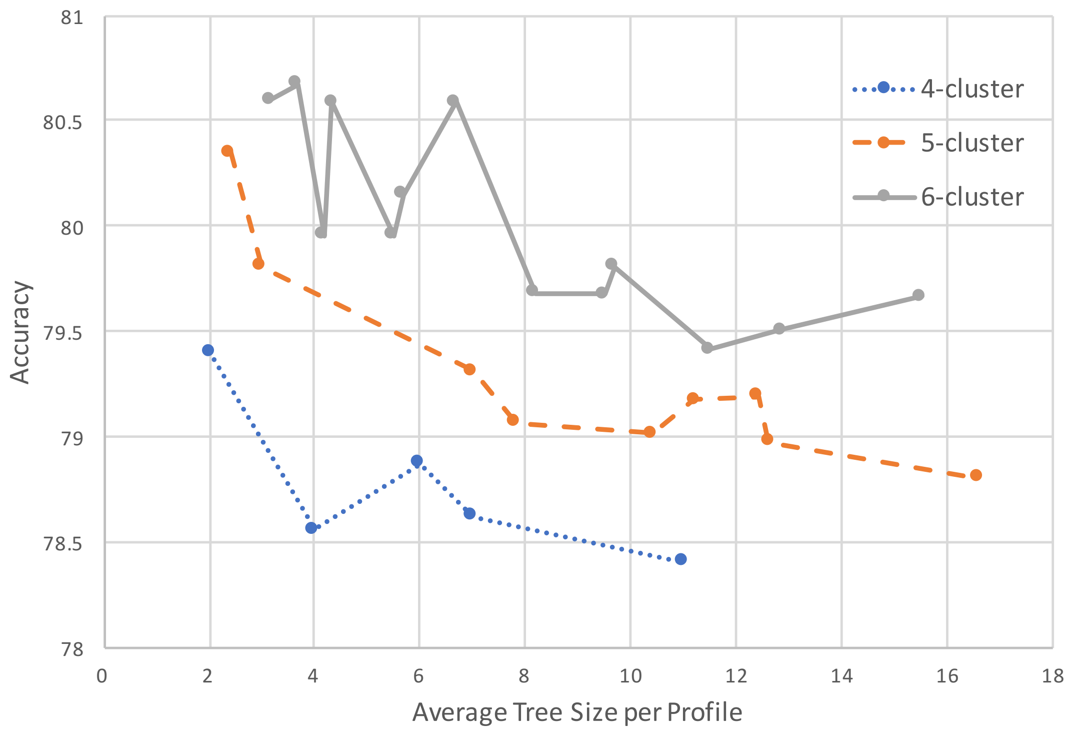



Figure 5.12: Parsimony/accuracy comparison for agglomerative clustering

the entire procedure is repeated with 20 random starts to avoid local optima.

To fit the trees, we use the J48 classifier with a Confidence Factor ranging from 0.01 to 0.25 with increments of 0.01. Surprisingly, smaller tree sizes result in a *higher* accuracy for agglomerative clustering (see Figure 5.12). This suggests that without extensive trimming, our agglomerative approach arguably overfits the data, resulting in a lower level of cross-validated accuracy.

The best 4-cluster solution has an average of 2 nodes per profile and an accuracy of 79.40%—a 24.53% improvement over the "smart default", and a 7.9% increase over the most accurate 5-cluster/4-profile attitude-based clustering solution. The decision trees are shown in Figure 5.13: aside from the "enable all" and "disable all" profiles, there is a "disable sharing with third parties" profile and a "local storage only" profile.

The best 5-cluster solution has an average of 2.4 nodes per profile and an accuracy of 80.35%—a 26.02% improvement over the "smart default", but only a 1.2% improvement over the 4-cluster agglomerative solution. The decision trees are shown in Figure 5.14: it has the same profiles as the 4-cluster solution, plus an "allow automation and alerts, but don't track my presence

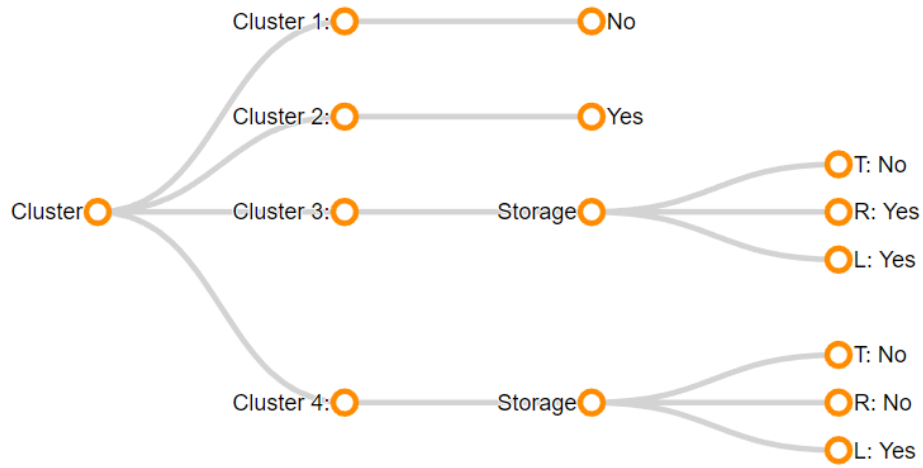



Figure 5.13: The best 4-profile agglomerative clustering solution (2 nodes/profile, accuracy: 79.40%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

or location in the house" profile.

Finally, the best 6-cluster solution[4] has an average of 3.17 nodes per profile and an accuracy of 80.68%—a 26.54% improvement over the "smart default", but no substantial improvement over the 5-cluster agglomerative solution. The decision trees are shown in Figure 5.15: it has the same profiles as the 5-cluster solution, plus a profile that allows local storage for anything, plus remote storage for any reason except for user profiling (i.e., to recommend other services or to give the user insight in their behavior).

### 5.5.6 Fit-Based Clustering

We now present a "fit-based" clustering approach that, like the agglomerative approach, clusters participants without using any additional information. Instead, it uses the fit of the tree models to bootstrap the process of sorting participants into different clusters. The 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

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

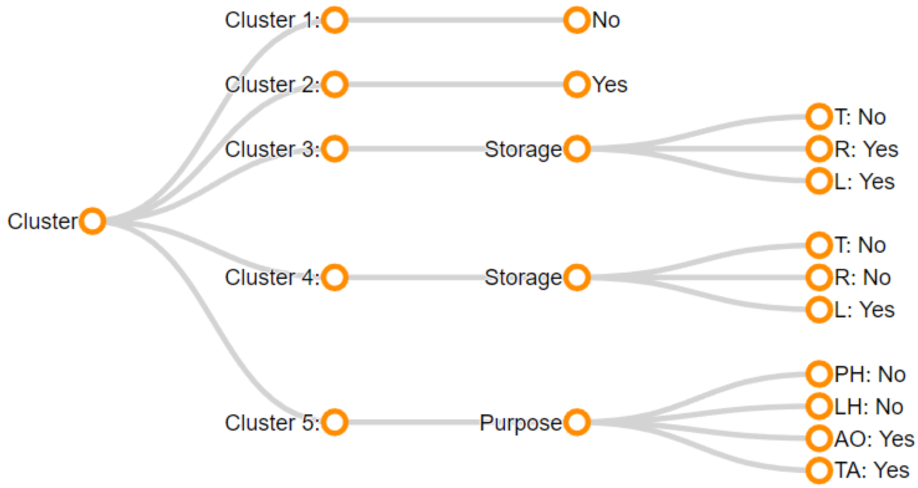



Figure 5.14: The best 5-profile agglomerative clustering solution (2.4 nodes/profile, Accuracy: 80.35%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

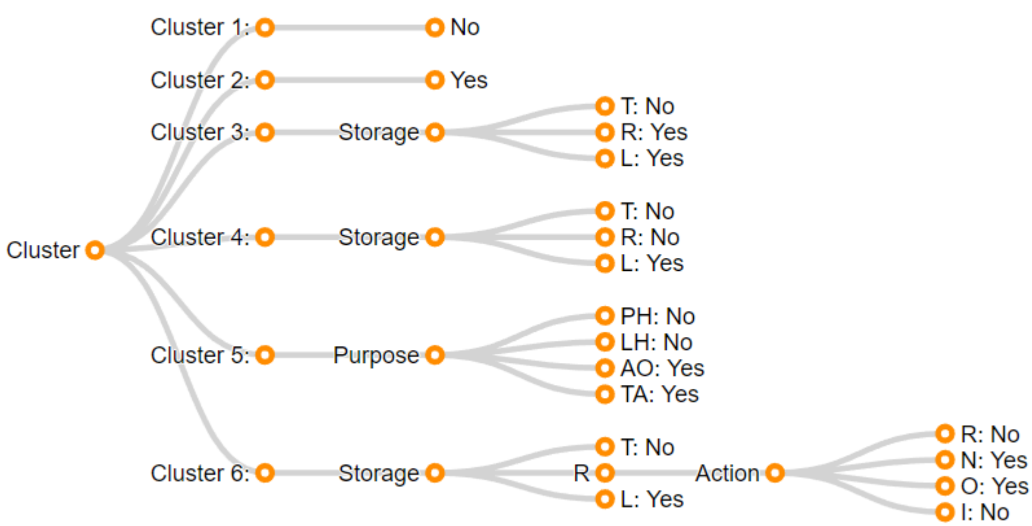



Figure 5.15: The best 6-profile agglomerative clustering solution (3.17 nodes/profile, Accuracy: 80.68% ). Parameter value abbreviations correspond to the "code" column in Table 5.1.

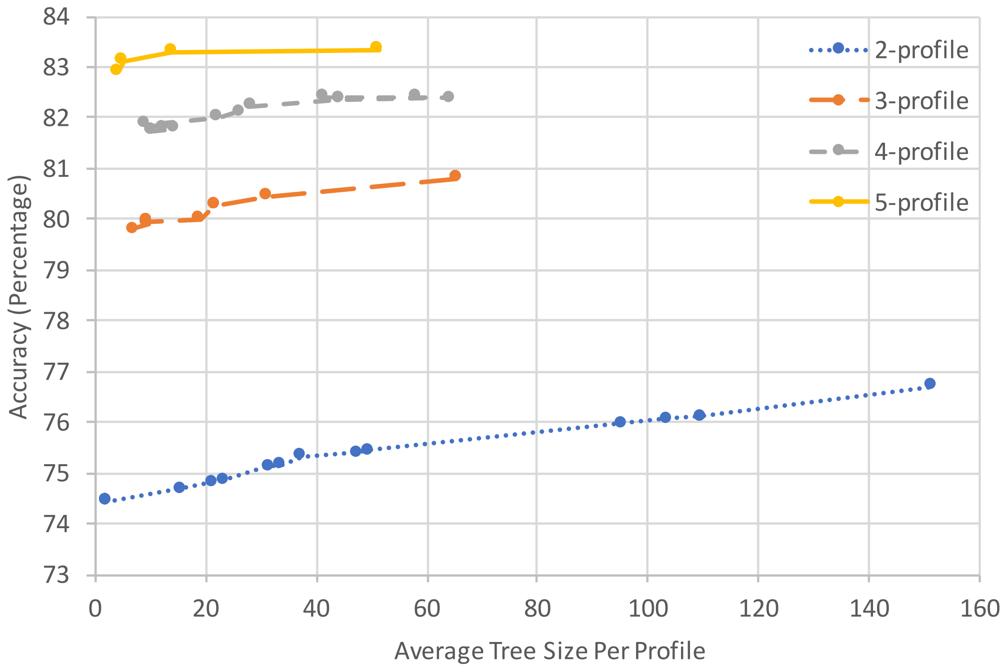



Figure 5.16: Parsimony/accuracy comparison for fit-based clustering

different group, we switch the participant to this group. Once all participants are evaluated and put in the group of their best-fitting tree, the tree in each group is re-learned with the data of the new group members. This then prompts another round of evaluations, and this process continues until no further switches are performed.

- **Repeat**: Since this process is influenced by random chance, it is repeated 1,000 times in its entirety to find the optimal solution. Cross-validation is performed in the final step to prevent over-fitting.

We perform this approach to obtain 2-, 3-, 4-, and 5-cluster solutions. To fit the trees, we use the J48 classifier with a Confidence Factor ranging from 0.01 to 0.25 with increments of 0.01. The best results are summarized in Figure 5.16.

For the 2-cluster solutions (the blue line in Figure 5.16), the highest accuracy is 76.72%—a 20.33% improvement over the "smart default" setting and a 5.6% improvement over the most accurate 2-cluster attitude-based solution. However, this tree has an average of 151.5 nodes per profile. The most parsimonious solution is exactly the same as the most parsimonious 2-cluster attitude-based solution (see Figure 5.10), but with a higher accuracy (74.43%).

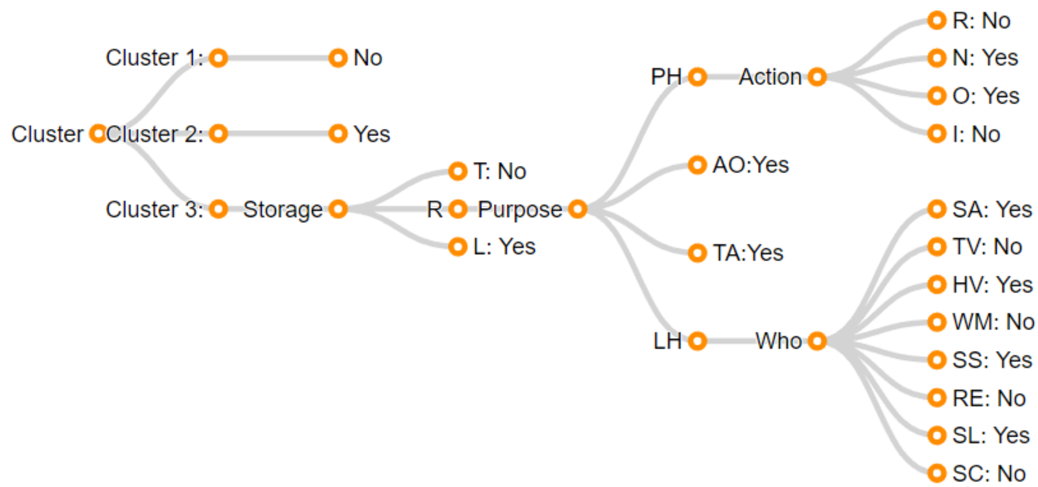



Figure 5.17: The most parsimonious 3-profile fit-based solution (7 nodes/profile, accuracy: 79.80%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

For the 3-cluster solutions (the orange line in Figure 5.16), the highest accuracy of 80.81% is achieved by a set of trees with 65.33 nodes on average. This is a 26.74% improvement over the "smart default", a 10.0% improvement over the most accurate 3-cluster attitude-based solution (but at a cost of lower parsimony), and a 5.2% improvement over the best 2-cluster fit-based solution. The most parsimonious solution, on the other hand, has 7 nodes on average, with an accuracy of 79.80%, thereby still outperforming all other 3-profile solutions. The decision trees for this solution are shown in Figure 5.17.

For the 4-cluster solutions (the grey line in Figure 5.16), the highest accuracy of 82.41% is achieved by a set of trees with 58.25 nodes on average. This is a 29.25% improvement over the "smart default", a 3.8% improvement over the 4-cluster agglomerative solution (but at a cost of lower parsimony), and a 2.0% improvement over the best 3-cluster fit-based solution. The most parsimonious solution, on the other hand, has 9.25 nodes on average, with an accuracy of 81.88%. It still outperforms all other 4-profile solutions, but the agglomerative solution is more parsimonious. The decision trees for this solution are shown in Figure 5.18.

For the 5-cluster solutions (the yellow line in Figure 5.16), 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%.

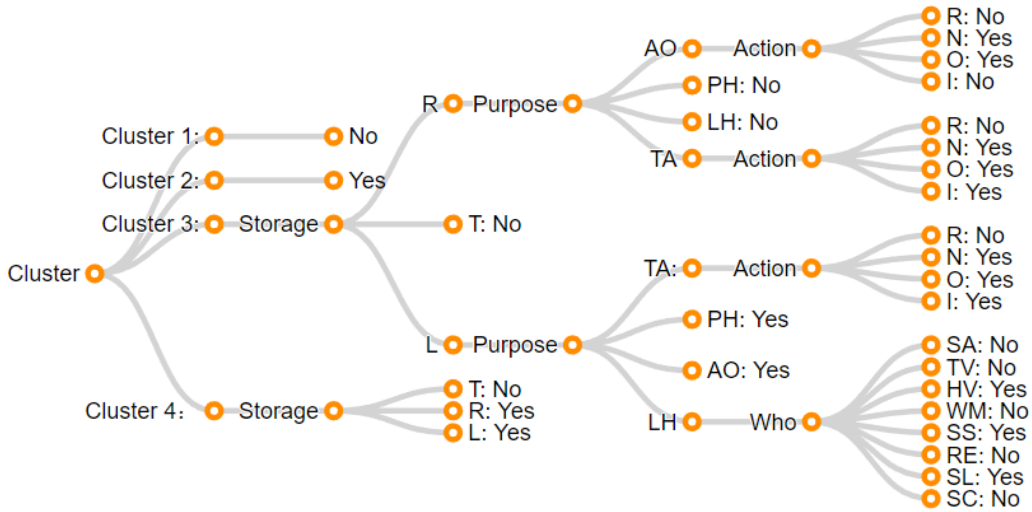



Figure 5.18: The most parsimonious 4-profile fit-based solution (9.25 nodes/profile, accuracy: 81.88% ). Parameter value abbreviations correspond to the "code" column in Table 5.1.

It still outperforms the 5-profile agglomerative solution, but it is slightly less parsimonious. The decision trees for this solution are shown in Figure 5.19.

### 5.5.7 Discussion of machine learning results

Figure 5.20 shows a comparison of the presented approaches. The X-axis represents the parsimony (higher average tree size per profile = lower parsimony); the Y-axis represents the accuracy. While the "smart default" setting makes a significant 15.3% improvement over the naive default setting ("disable all"), we observe that having multiple "smart profiles" substantially increases the prediction accuracy even further. The fit-Based clustering algorithm performs the best out of all the approaches, followed by agglomerative clustering and attitude-based clustering.

The most parsimonious 2-profile fit-based solution (with an accuracy of 74.43%) is the *simplest* of all "smart profile" solutions: one profile is simply "disable all", while the other profile is the same as our OneR solution: "disable sharing with third parties". In fact, these profiles are so simple, that one might not even want to bother with presenting them to the user: in our current interface (see Figure 5.3) these defaults are incredibly easy for users to implement by themselves.

The same is true for the 4-profile agglomerative clustering solution (see Figure 5.13) and the 5-profile agglomerative clustering solution (see Figure 5.14): these profiles involve little more

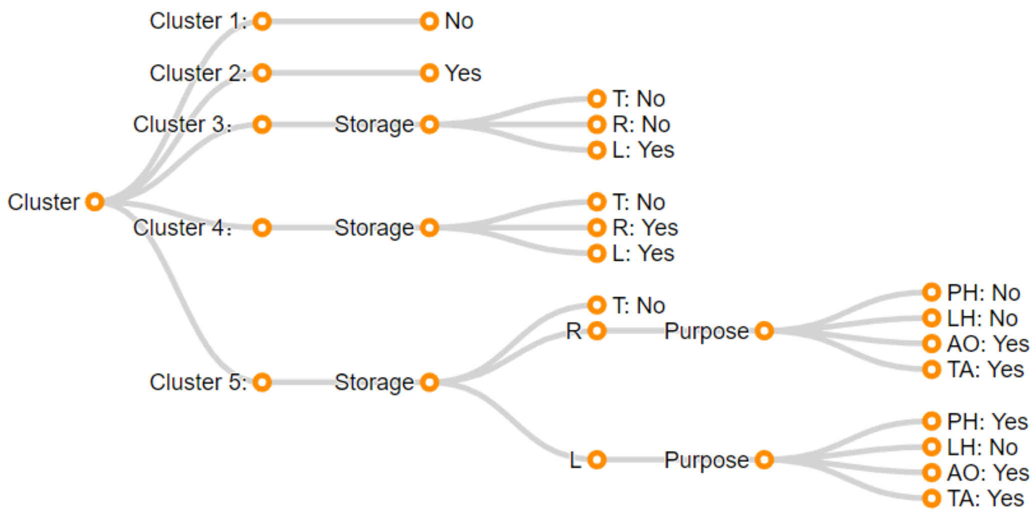



Figure 5.19: The most parsimonious 5-profile fit-based solution (4.2 nodes/profile, accuracy: 82.92% ). Parameter value abbreviations correspond to the "code" column in Table 5.1.

than a single high-level setting, which users can likely easily make by themselves.

The 5-profile fit-based solution is the *most accurate* of all "smart profile" solutions. The most parsimonious 5-profile fit-based clustering solution (Figure 5.19) has an accuracy of 82.92%. It has the following five profiles:

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

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

There is another 5-profile fit-based solution with a slightly higher accuracy (83.11%) and a reasonably simple tree (5 nodes/profile on average). This solution is shown in Figure 5.21. In

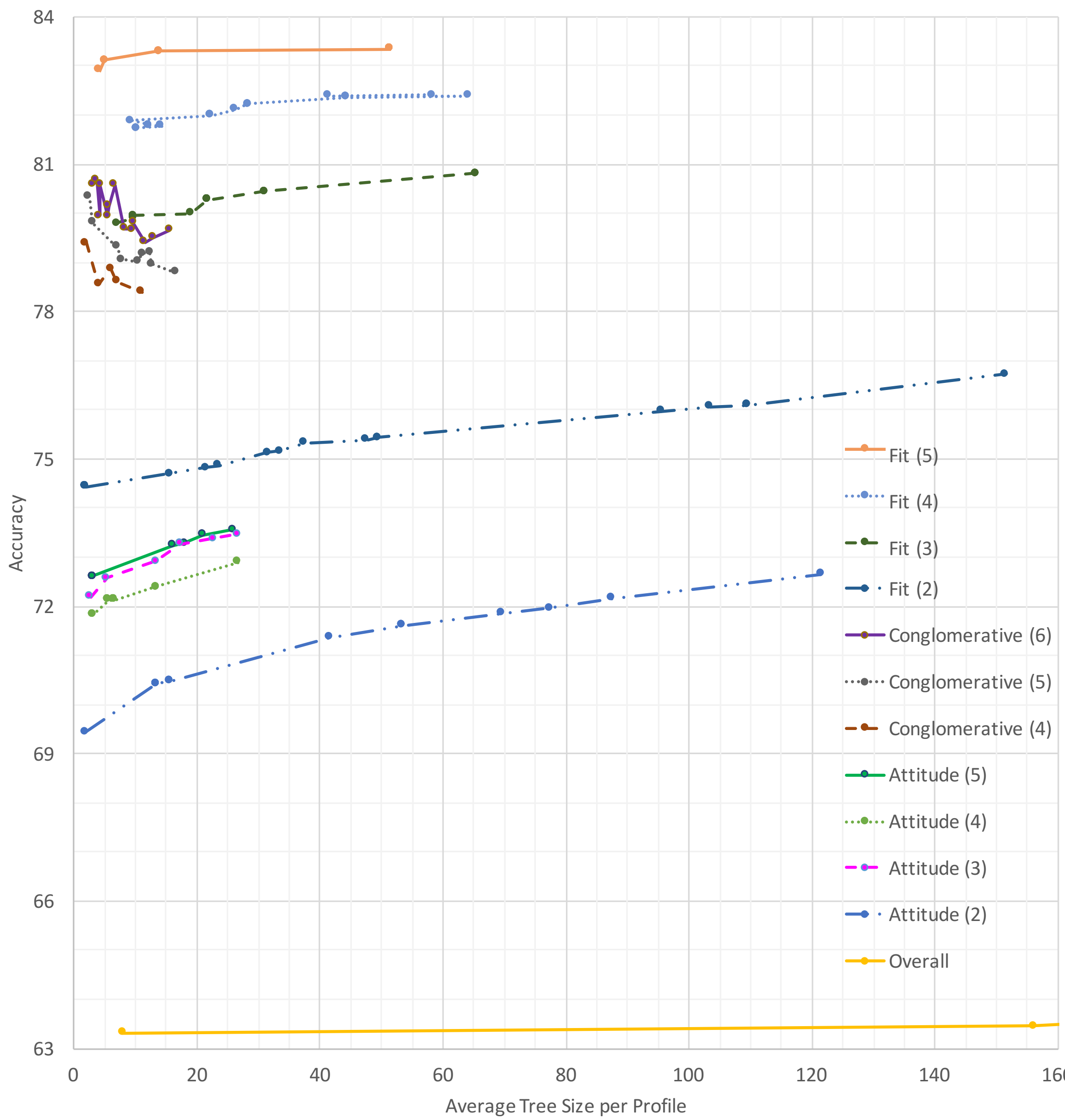



Figure 5.20: Summary of All our Approaches

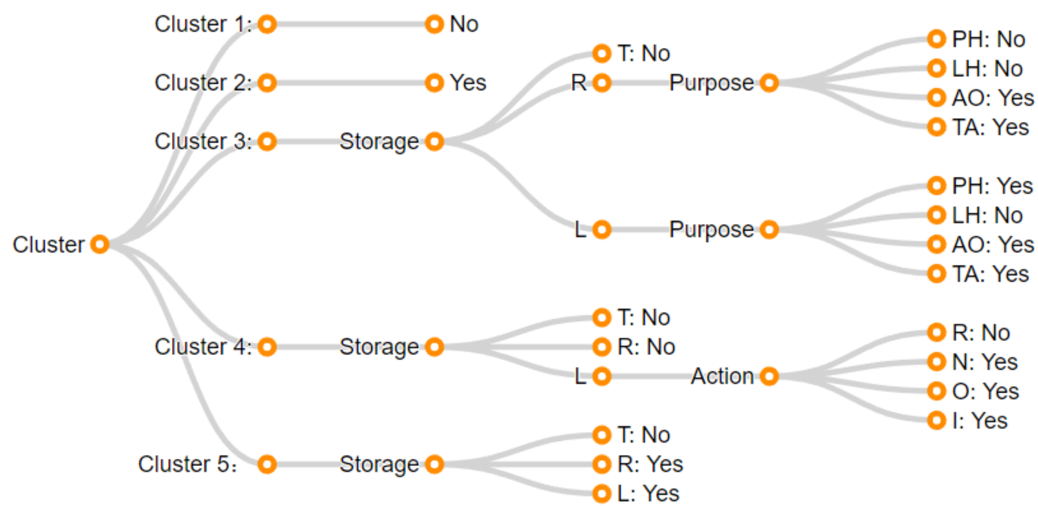



Figure 5.21: A good 5-profile fit-based clustering solution (5 nodes/profile, Accuracy: 83.11%). Parameter value abbreviations correspond to the "code" column in Table 5.1.

this solution, the third profile ("enable local storage only") is replaced by a slightly more complex profile ("enable local storage only, but not to recommend other services"). This profile specifies an additional interaction between **Storage** and **Action**. The next section will present a settings interface that accommodates this profile as well.

Other usable solutions are the 3-profile fit-based solution (Figure 5.17) or the 4-profile fit-based solution (Figure 5.18. However, like almost all of the less parsimonious solutions, these profiles involve higher-order interaction effects, e.g. between **Storage**, **Purpose**, and **Action**; and between **Storage**, **Purpose**, and **Who**. Consequently, a rather more complex interface is needed to accommodate these default profiles.

## 5.6 Privacy-Setting Prototype Design Using Machine Learning Results

In Section 5.4 we developed a prototype interface that household IoT users can use to manually set their privacy settings (see Figure 5.3). Our machine learning analysis (Section 5.5) resulted in a number of interesting solutions for "smart profiles" that would allow users of this interface to set their privacy settings with a single click (i.e., a choice of profile). While some of these profiles can be integrated in our prototype (e.g., the most parsimonious 2-profile fit-based solution and the 4-profile and 5-profile agglomerative solutions) other profiles have an interaction effect between variables that are modeled as independent in our current prototype interface (e.g., the two 5-profile fit-based solutions presented in Figures 5.19 and 5.21).

In this section we therefore present two modified prototypes that are designed to be compatible with these two 5-profile solutions. These two solutions are not the most accurate, but they produce a parsimonious set of profiles that require only minimal alterations to our interface design. They thus provide the optimal trade-off between reduction accuracy, profile parsimony, and interface complexity.

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

This machine learning solution (Figure 5.19) requires an interaction between the *Storage* parameter and the *Purpose* parameter—two parameters that are controlled independently in the prototype in Figure 5.3. Our solution is to slightly alter the interface, and add the profile selection page at the beginning of the interface (see Figure 5.22):

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


Figure 5.22: Design for 5-Profile solution presented in Section 5.6.1. 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.

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

The alternative machine learning solution presented in Figure 5.21 requires an additional interaction between the *Storage* parameter and the *Action* parameter. This requires us to slightly alter the interface again (see Figure 5.23):

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

### 5.6.3 Reflection on design complexity

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

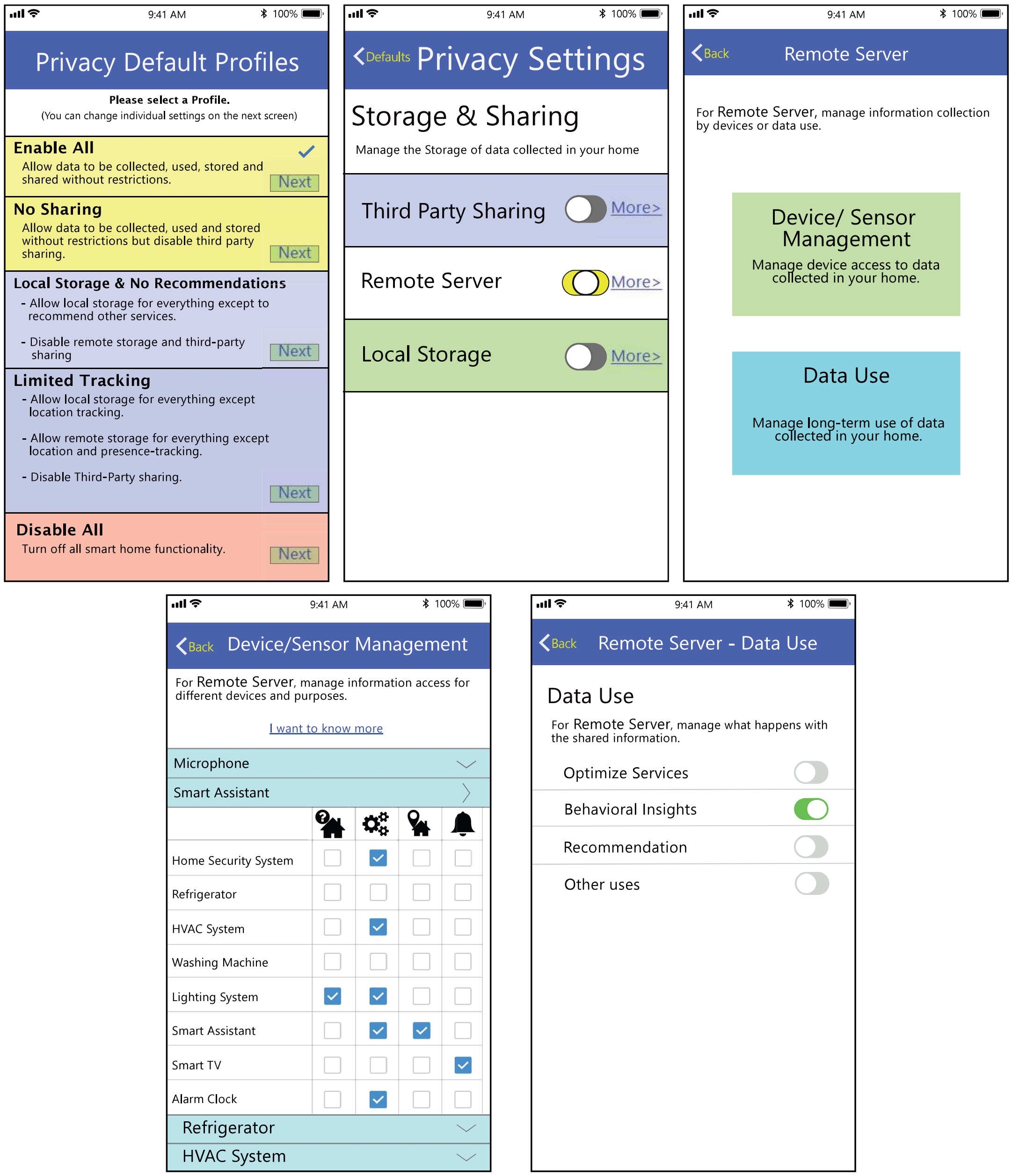



Figure 5.23: Design for 5-Profile solution presented in Section 5.6.2. From top left, screen 1 is the profile selection page, screen 2 is the slightly altered Data Storage page, screen 3 follows the 'More' button to offer access to screen 4 (bottom left, the Data Use page) and screen 5 (bottom right, the Device/Sensor Management page).

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.

# Chapter 6

# Recommending Privacy Perference for Fitness IoT

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

## Chapter 7

# Proposed Work

# Chapter 8

# Conclusion

# Appendices

# Bibliography


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

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

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

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

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

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

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

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

[9] 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.

[10] 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.

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

[12] 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.

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

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

[20] 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.

[21] 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.

[22] 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.

[23] 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.