Recommending Privacy Settings for Internet-of-Things

A Dissertation Proposal by
Yangyang He
Jan 2019

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

Approved By:

Dr. Bart P. Knijnenburg
Advisor/Committee Chair

Dr. Larry F. Hodges
Committee Member

Dr. Alexander Herzog
Committee Member

Author's Publications on this topic

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

1. **He, Y.** (2019): Recommending Privacy Settings for IoT. In 24th International Conference on Intelligent User Interfaces (IUI '19 Companion), March 17–20, 2019, Marina del Ray, CA.
2. **He, Y.**, Bahirat, P., Knijnenburg, B.P. (2018): A Data Driven approach to Designing for Privacy in Household IoT. ACM Transactions on Interactive Intelligent Systems (TiiS).
3. Sanchez, O., Torre, I., **He, Y.**, Knijnenburg, B.P. (2018) Recommending User Privacy Preferences for Fitness IoT. User Modeling and User-Adapted Interaction (UMUAI).
4. Bahirat, P., **He, Y.**, Knijnenburg, B.P. (2018): Exploring Defaults and Framing effects on Privacy Decision Making in Smarthomes. To appear on Interactive Workshop on the Human aspect of Smarthome Security and Privacy, SOUPS 2018, Baltimore, U.S.A.
5. Bahirat, P., **He, Y.**, Menon, A., Knijnenburg, B.P. (2018): A Data-Driven Approach to Developing IoT Privacy-Setting Interfaces. IUI2018, Tokyo, Japan.

Outline

List of Tables

List of Figures

Chapter 1

Introduction

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

As estimated by Gartner [13], over 21 billion Internet-of-Things (IoT) devices will be in use by 2020. With its rapidly accelerating growth, IoT technology has a huge potential for social impact. However, this potential also comes with a number of key security and privacy concerns. These include facilitation of the collection of large amounts of consumer data, using that data in ways unexpected by the consumer, and security of data [44, 79]. When users are considering adopting new IoT devices, they want to take the benefit of using those smart connected electronic devices by sharing and disclosing certain personal information to get a more personalized experience. However, such disclosed information could be accessed by other smart devices owned by themselves, other people, organizations, government, or some third-parties with good or bad purpose, which brings

privacy risks to the users. It is not surprising that privacy concerns have been identified as an important underlying obstacles to the adoption of the IoT technology [32, 53].

In IoT environments, all the IoT devices are intended to collect information from the users to realize their functionality. Technical solutions can be used to minimize the data collected for such functionality [34, 49, 73], but arguably, any useful functionality would necessitate at least some amount of personal data. Therefore, users will have to manage a trade-off between privacy and functionality: a solution that is fully privacy preserving will be limited in functionality, while a fully functionality IoT solution would demand extensive data collection and sharing with others. Research has shown that user employ a method called *privacy calculus*—i.e. that they make disclosure decisions by trading off the anticipated benefits with the risks of disclosure [9, 36, 64]. However, as the diversity of IoT devices increases, it becomes more and more difficult to keep up with the many different ways in which data about ourselves is collected and disseminated. Although generally users care about their privacy, few of them in practice find time to read the privacy policies or the privacy-settings carefully that are provided to them. There are several reasons for this problem: i) Users will pay more attention to the benefit than potential risks from using IoT devices or services. ii) The privacy policies are too long, or the privacy setting of such devices are too complicated, making users irritated to finish reading/setting them. iii) As the number IoT devices rapidly increases, the numbers and options of privacy setting for all the IoT devices will also increase exponentially. Moreover, each device will have its own fine-grained privacy settings (often hidden deep within an unassuming "other settings" category in the settings interface), and many inter dependencies exist between devices—-both in privacy and functionality. Therefore, there is a large chance that users would make inconsistent privacy decisions that either limit functionality of their IoT devices or that do not protect their privacy in the end. In addition, the current user interface for setting privacy preferences of present IoT devices is imperfect even for a smartphone, not to mention the complexity of manually setting privacy preferences for numerous different other IoT devices. Hence, there is an urgent demand to solve the following research question:

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

Prior research (chapter 2) has explored different approaches to this problem in other domains, including providing transparency, Privacy nudges. However, neither of them provides a satisfying solution in the IoT domain. Providing transparency and control does give users the free-

dom of managing their privacy in IoT according to their own privacy decisions, but privacy decision making is often not rational [32]. Thus, such extra transparency and control may increase the difficulty of setting appropriate privacy for users. Privacy nudges are usually implemented in the form of prompts, which will create constant noises given that the IoT systems usually work in the background. At the same time, they lacks the personalization to the inherent diversity of users' privacy preferences and the context-dependency of their decisions.

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

In this proposal, I first present the background and related work of this proposal in Chapter 2. Then, I present three studies on recommending privacy settings for different IoT environments, namely generalize/public IoT in Chapter **??**, household IoT in Chapter **??**, and fitness IoT in Chapter **??**, respectively. One should observe that the above three studies follow an decreasing order in terms of the IoT context scope. In the first study, I focused on the privacy decision on the entities collecting information from the users, while in the following two studies the context was moved to a more narrow environment (household IoT and fitness IoT), which shifts the focus to a more contextual evaluation of the content or nature of the information. This explains why in the first two studies, the dimensions used to analyze the context are the parameters of the corresponding IoT scenarios; and for the third study, the focus is on the fitness tracker permission questions. Note that the above three work all utilized a " data-driven design" — We first use statistical analysis (applicable to the first two work) and machine learning techniques on the collected user data to gain the underlying insights of IoT users' privacy decision behavior; and then a set of "smart" privacy default/profiles were created based on these insights, and finally design a set of interfaces to incorporate these privacy default/profiles. Users can apply these smart default/profiles by either a single click (applicable to the first two work) or answering a few related questions (applicable to the third work). The current biggest limitation for such "data-driven" approach is that we didn't test any of the presented interfaces, so we don't know what level of complexity (both in terms of the user interface and the in terms of the profiles). Thus for my proposed work, I will address this limitation by discussing our proposed study to evaluate the new interface of recommending privacy-settings

for household IoT in Chapter **??**. Finally, I conclude this proposal in Chapter **??**.

Chapter 2

Background

2.1 IoT Technology

The term "Internet of Things" (IoT) was first introduced by Kevin Ashton in the context of supply chain management in 1999 [2]. Atozri et al. define IoT as a pervasive presence around us of a variety of things or objects - such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing scheme, are able to interact with each other and cooperate with their neighbors to reach common goals [3]. As various wireless sensor technologies (e.g. RFID, embedded sensors, and actuator nodes) and artificial intelligence advance rapidly during the last two decades, the definition of the IoT has evolved to more broad covering wide range of monitoring and control applications based on a network of sensing and actuating devices that controlled remotely through the Internet in many fields, such as tracking, transportation, household usage, healthcare and fitness [39, 62, 31, 30, 24]. IoT can benefit both organizations and individual consumers in all above mentioned domains by enhancing data collection, enabling real-time response, improving access and control of internet-connected devices, increasing efficiency, productivity, and satisfaction [75, 52]. With such huge social and economic potential, IoT is estimated to grow rapidly by a wide range of well-respected organizations. For example, Gartner [13] has predicted over 21 billion IoT devices will be in use by 2020; IoT product and service suppliers will generate incremental revenue exceeding $300 billion. IDC forecasts a global market for IoT will grow from $1.9 trillion in 2013 to $7.1 trillion in 2020. However, there exist several key security and privacy concerns associated with the rise of the IoT, including data processing and storage, privacy and security

breach, etc [75, 44, 79].

Previous studies mostly focused on the technical issues of IoT technologies [16, 37, 60]. For example, Uckelmann et al. systematically explained the architecture of future IoT [67]. Chen et al. present a vision of IoT's applications in China [8]. Guinard et al. described the IoT's best practices based on the web technologies and proposed several prototypes using the web principles, which connect environmental sensor nodes, energy monitoring systems, and RFID-tagged objects to the web [23]. However, little attention has been devoted to, from the perspective of individual consumers, understanding how will the user of IoT will trade off the above mentioned benefits and privacy concerns of IoT technology when they consider adopting it [1, 19, 45].

Furthermore, researchers identified the security and privacy issues as the major challenges for consumer acceptance of the IoT technology's user-oriented IoT applications (Medaglia & Serbanati, 2010) [30]. Arguably, if the user find their privacy demands can not be satisfied (e.g. it's confusing to) when using IoT devices after adopting them, they would probably finally give up using these devices.

2.2 Model the Acceptance of IoT

2.2.1 Technology Acceptance Model

The technology acceptance model (TAM) is arguably the most popular model that explains how users come to accept and use a technology [11]. TAM suggests that an individual's *Behavioral Intention* to Use an information technology is significantly dependent upon the individual's perception of *Perceived Usefulness* and *Perceived Ease Of Use* of that information technology. Specifically, perceived usefulness is the extent to which an individual believes that using a particular information technology will have a positive impact on his/her performance. Perceived ease of use is the extent to which an individual perceives that using a particular information technology will be free of effort. TAM also proposes that perceived ease of use can explain the variance in perceived usefulness. TAM have applied to a wide range of technology adoption contexts [77], such as the adoption of PC [71], smartphones [47], mobile marketing [5], Internet banking [51], facebook [38, 55], and online shopping [20].

2.2.2 UTAUT

The unified theory of acceptance and use of technology (UTAUT) is a technology acceptance model proposed by Venkatesh et al. [72]. Compared to TAM, UTAUT model identifies four key factors: 1) performance expectancy, 2) effort expectancy, 3) social influence, and 4) facilitating conditions related to predicting behavioral intention to use a technology and actual technology use primarily in organizational contexts. The first three factors are theorized and found to influence behavioral intention to use a technology, while behavioral intention and facilitating conditions determine technology use. UTAUT also identifies four moderators (i.e., age, gender, experience, and voluntariness).

These relationships are also confirmed by Weerakkody, ElHaddadeh, Al-Sobhi, Shareef, and Dwivedi (2013) [39] in the context of electronic government, or electronic learning (Wang et al., 2009) [45], cloud computing (Lian, 2015) [43], and electronic commerce. Figure 2 shows the conceptual model of UTAUT. The key variables of UTAUT is developed based on the similarities with other variables from other theories and models. For example, performance expectancy is considered similar to perceived usefulness in TAM. Table 1 shows the core variables of UTAUT. Venkatesh et al. (2003) [38] combined the previous models of technology adoption to come up with UTAUT which is design specifically to investigate users' acceptance of a new technology and it has explanatory power higher than previous models such as TAM. Thus, the UTAUT model is suitable for understanding the acceptance of IoT services.

2.2.3 The Acceptance of IoT

Researchers have attempted to identify the factors that affect the acceptance of IoT by customers. For example, Gao and Bai (2014) [16] investigated the factors that affect the acceptance of IoT in China. Mainly, their study used the factors of TAM such as perceived ease of use and perceived usefulness along with other factors such as trust, social influence, perceived enjoyment, and perceived behavioral control. A total of 368 respondents have participated in the study. The results indicate that perceived usefulness, perceived ease of use, social influence, perceived enjoyment and perceived behavioral control have significant effect on behavioral intention to use the IoT. Acquity Group, (2014) [1] investigated the concerns of customers to adopt the IoT. A total of 2000 customers in US have been surveyed. The findings showed that awareness of the technology, usefulness, price

(cost), security, privacy are the main concerns of the customers.

2.3 Privacy in IoT

One of the key features of IoT environments is that they have a high potential for providing personalized services to their users [69, 14, 21]. For example, Russell et al. [57] 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. [25] propose an approach to personalize services in (household) IoT using the Global Public Inclusive Infrastructure's [70] preference set to describe an individual's needs and preferences, and then adapting a smart environment accordingly.

Researchers have shown that privacy plays a limiting role in users' adoption of personalized services [65]. For example, Awad and Krishnan [4] show that privacy concerns inhibit users' use of personalized services, and Sutanto et al. [63] demonstrated that privacy concerns can prevent people from using a potentially beneficial personalized application. Kobsa et al. [35] 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 [50, 26, 27], and researchers therefore claim that both the benefits and the risks meet a certain threshold [66], or that they should be in balance [7].

The argument that using user-generated data for personalization can result in privacy concerns has also been made in IoT environments [78]. One of the first examples in this regard was the work by Sheng et al. [61], 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 [48, 43]. 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 [10]. Likewise, Jayraman et al.'s privacy preserving architecture aggregates requested data to preserve user privacy [28].

Other research has considered IoT privacy from the end-user perspective [18], 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 [68]) 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 [76], and Feth et al. investigated the creation of understandable and usable controls [18]). 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.

2.4 Existing Privacy Control Schemes

Previous studies in mobile privacy (e.g.,[17]) have proven that mobile interfaces lack the potential to provide the necessary user privacy information and control for both Android and iOS systems [41]. Several solutions from literature have been proposed from then on to improve mobile privacy protection and offer users more privacy control (e.g., [6]). These leads into rapid improvement of privacy management of current mobile systems (i.e., from Android 6.0+ and iOS 5.0+), providing more control on the user's privacy settings.

Android permission systems can be mainly categorized as Ask On Install (AOI) and Ask On First Use (AOFU) privacy models [**?**, **?**]. In AOI[1] (Android 5.9 and below), the permissions are asked in bulk before installing a TP app. The user's option is only to allow or deny all, which clearly gives less privacy control. Also, only a few number of users read and pay attention to the install time permissions, and even fewer than this can understand their meaning [17, **?**]. These issues made room for TP apps that manage app privacy such as Turtleguard [**?**] and Mockdroid [6].

On the other hand, the AOFU model [**?**] (Android 6.0 and above) only asks permissions during the first use of an app and when an app uses a specific feature that needs the respective permission. In this case, the user grants the permission during the actual provision of the service and will be able to weigh his willingness to share vs the utility of the app. The user can also revisit and review permissions in their phone privacy settings for each app. This model makes user more

[1] `https://support.google.com/googleplay/answer/6014972?co=GENIE.Platform%3DAndroid&hl=en`

informed and gives them more control as the previous model does not allow users to be informed effectively[**?**]. Moreover, it has been proven that interactive notification is more efficient in informing users request access[**?**]. It is noteworthy to discuss this two models as currently, 34% of the Android users are still using the AOI model[2].

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

In smartphone domain, privacy nudging is an effective scheme to increase users' awareness [**?**]. Privacy nudging allows users to be informed and aware on both their privacy settings and how the third party applications access their data [42, **?**]. It has been showed that 78.7% [42] of the privacy recommendation were adopted by the smartphone users. However, such nudging are problematic for IoT, because IoT devices are supposed to operate in the background. Moreover, as the penetration of IoT devices in our homes continues to increase, nudging would become a constant noise which users will soon start to ignore, like software EULAs [22] or privacy policies [29]. At the same time, Privacy nudges lack the personalization and provide general recommendation.

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

[2] `https://developer.android.com/about/dashboards/index.html`

2.5 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 [59]. This approach can be further simplified by grouping recipients into relevant semantic categories, such as Google+'s *circles* [74]. Taking a step further, Raber et al. [54] 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 [76]. 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.

2.6 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) [33]. 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. [58] 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. [46] 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. [12] 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. [40] 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. [15], 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. [56] 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.

Bibliography

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

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

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

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

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

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

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

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

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

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

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

[12] 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.

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

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

[15] 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.

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

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

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

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

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

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

[22] 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.

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

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

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

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

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

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

[29] 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.

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

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

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

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

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

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

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

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

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

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

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

[41] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I Hong. Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings. pages 199–212, 2014.

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

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

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

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

[46] 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.

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

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

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

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

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

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

[53] PwC. Smart home, seamless life: Unlocking a culture of convenience, 2017. [Online; accessed 1-Jan-2019].

[54] 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.

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

[56] 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[74] 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.

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

[76] 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.

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

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

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

Appendices