Personalized Privacy Assistant to Protect People's Privacy in Smart Home Environment

Yaxing Yao
Syracuse University
Syracuse, NY 13210, USA
yyao08@syr.edu

Abstract
The goal of this position paper is to introduce one potential idea for my dissertation research. As smart home IoT devices are becoming pervasive, their ability to collect sensitive data of end users risk users' privacy. Through a three-step project, I aim to develop a personalized privacy assistant which can provide users more transparency of the data collection practices in a smart home environment and help people make more informed privacy decisions. I further introduced a case study using a similar methodology in the context of online behavioral advertising.

Author Keywords
Personalization; privacy; smart home; the Internet of Things

ACM Classification Keywords
H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous; See [http://acm.org/about/class/1998/]: for full list of ACM classifiers. This section is required.

Introduction
The idea of user-controllable privacy system is not new. For example, Loccacino is a system that can help people to manage their location sharing privacy policy [10, 8, 3]. It is consisted of three components, including a contextual instant messenger, a people finder application, and a phone-based application for access control [3], and is de-

signed to empower users to effectively control their privacy in location-based social network systems [10]. Inspired by this work, I hope to create a system that can empower users to be more aware of data collection and manage their privacy based on their own preferences in a smart home environment.

With the fast development of the Internet of Things (IoT), smart home is getting rapidly getting more popular. In a general IoT system, privacy and security are the primary requirements just like all other network computing systems [6]. This is particularly true in the context of smart home for a few reasons. Smart home systems generate a huge amount of data, thus pose great privacy risks to users. A report by the Federal Trade Commission has shown that fewer than 10,000 households that have smart home IoT devices can generate 150 million discrete data points per day [2]. This massive amount of data allows a variety of analyses which are not possible using other less rich data [2]. IoT devices in smart home can directly collect sensitive personal information, such as precise geolocation, financial information or health information. More importantly, IoT devices can collect other types of information, such as personal habits and physical conditions over time. Such information will allow an entity to infer sensitive information without actually collecting them [7].

From 2005 to 2010, there was a wave of studying assistive technology in smart home for older people for medical or health purposes [1, 4, 5], however, given the recent development of IoT and smart home technologies, there are needs in research to not only understand people's privacy perceptions of smart home technologies, and how do these concerns change across different contexts and over time, but also build systems to give people more controls about their privacy, and make more informed privacy decisions (e.g., auto-configuration support for smart home [6]). The most recent and related research is done by Zeng et al., who conducted a study on understanding end users' security and privacy concerns with smart home [12]. They identified a number of privacy and security concerns people have about their smart home devices, such as continuous video recording, data collection and mining, network attack on local networks, and account/password hacking, etc. [12] My proposed work aims to study this problem from a different perspective in a bigger scope, in which I aim to create a personalized privacy assistant that empowers smart home IoT users to better manage their privacy.

In the following section, I first introduce my proposed research agenda in smart home. Then I circle back to my current project regarding a privacy assistant in online behavioral advertising (OBA), which is conducted in a different context, but adopt a similar methodology. I use this OBA project as a case study to help the audiences better understand the underlying logic of my proposed research.

Personal Privacy Assistant

This study will solely focus on smart home IoT. The reasons I choose to focus on smart home are because (1) quantity, heterogeneity and complex interactions of home devices, (2) home is one's castle (deemed very private and thus people are likely to have strong privacy expectations), and (3) home is a rich social environment with complex cultural norms and power dynamics (e.g., parents vs. children).
In a smart home environment, typically there is a variety of IoT devices (e.g., AI voice assistant, smart TV, thermostat, light bulb, smart toys, etc). Generally, these devices are collecting an extensive amount of data from the end users, including general information (e.g., product model, usage), personal identifiable information (e.g., name, email, address), and some sensitive information (e.g., health data,

sleep data). These data can be used for many purposes (e.g., inferring new data about the users, price discrimination, profiling and targeted ads, sharing or selling user data to third parties [7, 6, 9]) that the end users may or may not be aware of.

My idea is centered around improving transparency and awareness of data collection inside a smart home environment and helping users to make more informed decisions about their privacy and to better control their privacy. There are three components in this plan.

The first component is an empirical study to understand people's privacy concerns of smart home IoT technologies, why they have those concerns, and what controls they expect to have towards these technologies in terms of privacy. The outcome of this step will be users' privacy mental models of smart home IoT technologies.

The second component is a recommender system-like platform that provides end users a shopping guide for smart home IoT devices based on the privacy practices of these devices. The system will analyze different aspects of a product (e.g., data collected, data collection frequency, privacy policy), and make recommendations to potential buyers based on the product's privacy practices. This idea aims to provide privacy control before the users purchase the products, which arguably minimize the privacy risk of a device because users would not buy and use it.

The third component is a system that provides users awareness and transparency of data collection inside their smart home. The system will monitor the privacy practices of home IoT devices, learn users' contextual privacy preferences, and give users warnings if their privacy preferences are violated by the actual behaviors or practices of home IoT devices. Then the system will provide a certain level of control/suggestions so that the users can take measures to protect their privacy.

Expected Contributions
There are three expected contributions from this research.

- Understand how different contextual factors (e.g., time, people, relationships, etc.) affect people's privacy mental models in a smart home environment.
- Explore effective ways of providing users enough awareness of data collection in smart home and help users to understand the consequences of such data collection.
- Design and build systems to provide users control regarding their privacy at different times (pre-purchase, during setup, and while in use).

A Similar Case Study in OBA

The case study is about my current project. In this project, I am designing and developing a user-centered, personalized tool to block web tracking. The commercially available web tracking blockers (e.g., Ghostery) suffer from two major issues: first, they all provide a list of web trackers, many of which ordinary users do not understand; second, they all provide the same list to all users, adopting the "one-size fits all" approach. Previous research found that ordinary users care more about what information is collected than the trackers [11]. Inspired by [11], I designed an information-based web tracking blocker which can help users to understand what information can potentially be collected by web trackers. In addition, the information-based blocker can also learn users' context-based (website genre-based) privacy preferences, so that when users land on different sites, the blocker can automatically block certain types of information

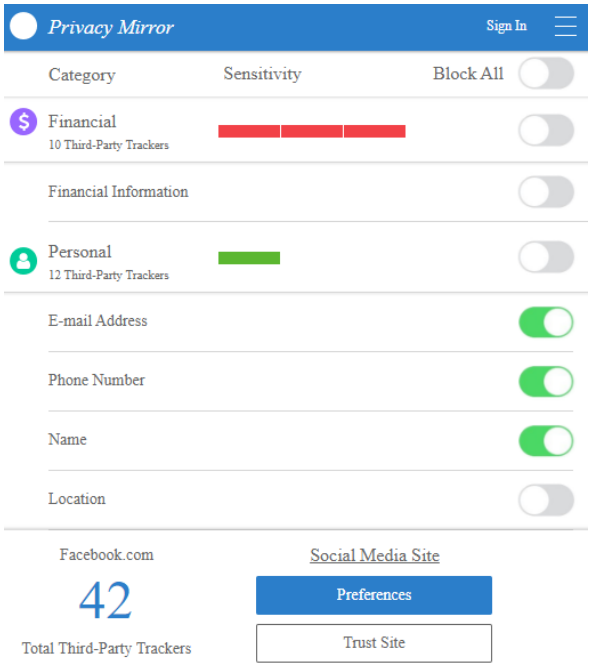

Figure 1: Initial design of an information-based blocker.

from being collected based on individual user's privacy preference. Figure 1 shows the initial design of the information-based blocker.

Conclusion

In this position paper, I lay out a potential project for my dissertation which aims to develop a personalized privacy assistant that can help users make more informed privacy decisions in the context of smart home. Through a set of studies, I expect to contribute to the privacy research of smart home by understanding different contextual factors that affect people's privacy mental models and design and build new systems to help people make more informed privacy decisions before and after purchasing smart home IoT devices. I further introduce a case study using a similar methodology in the context of OBA to demonstrate the feasiblity of such approach.

Acknowledgements

I thank my advisor Yang Wang for his invaluable advice and comments and all other collaborators that helped me with my ongoing projects and these ideas.

REFERENCES

1. Saisakul Chernbumroong, Anthony ATKINS, and Hongnian Yu. 2010. Perception of smart home technologies to assist elderly people. In *4th International Conference on Software, Knowledge, Information Management and Applications*. 4th International Conference on Software, Knowledge, Information Management and Applications, 90–97.
2. Federal Trade Commission and others. 2015. Internet of Things: Privacy & security in a connected world. *Washington, DC: Federal Trade Commission* (2015).
3. Jason Cornwell, Ian Fette, Gary Hsieh, Madhu Prabaker, Jinghai Rao, Karen Tang, Kami Vaniea, Lujo Bauer, Lorrie Cranor, Jason Hong, and others. 2007. User-controllable security and privacy for pervasive computing. In *Mobile Computing Systems and Applications, 2007. HotMobile 2007. Eighth IEEE Workshop on*. IEEE, 14–19.
4. Karen L Courtney, George Demeris, Marilyn Rantz, and Marjorie Skubic. 2008. Needing smart home technologies: the perspectives of older adults in continuing care retirement communities. (2008).

5. George Demiris, Marilyn J Rantz, Myra A Aud, Karen D Marek, Harry W Tyrer, Marjorie Skubic, and Ali A Hussam. 2004. Older adults' attitudes towards and perceptions of âĂŸsmart homeâĂŹtechnologies: a pilot study. *Medical informatics and the Internet in medicine* 29, 2 (2004), 87–94.
6. Huichen Lin and Neil W Bergmann. 2016. IoT privacy and security challenges for smart home environments. *Information* 7, 3 (2016), 44.
7. Andrew Meola. 2016. How the Internet of Things will affect security & privacy. (2016).
8. Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, and Jinghai Rao. 2009. Understanding and capturing peopleâĂŹs privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing* 13, 6 (2009), 401–412.
9. Biljana L Risteska Stojkoska and Kire V Trivodaliev. 2017. A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production* 140 (2017), 1454–1464.
10. Eran Toch, Justin Cranshaw, Paul Hankes-Drielsma, Jay Springfield, Patrick Gage Kelley, Lorrie Cranor, Jason Hong, and Norman Sadeh. 2010. Locaccino: a privacy-centric location sharing application. In *Proceedings of the 12th ACM international conference adjunct papers on Ubiquitous computing-Adjunct*. ACM, 381–382.
11. Yaxing Yao, Davide Lo Re, and Yang Wang. 2017. Folk Models of Online Behavioral Advertising. In *Proceedings of the Computer Supported Cooperative Work (CSCW)*. ACM.
12. Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. In *Symposium on Usable Privacy and Security (SOUPS)*.