Informing The Future of Data Protection in Smart Homes

Martin J Kraemer
Dept. of Computer Science
University of Oxford
martin.kraemer@cs.ox.ac.uk

William Seymour
Dept. of Computer Science
University of Oxford
william.seymour@cs.ox.ac.uk

Reuben Binns
Dept. of Computer Science
University of Oxford
reuben.binns@cs.ox.ac.uk

Max Van Kleek
Dept. of Computer Science
University of Oxford
max.van.kleek@cs.ox.ac.uk

Ivan Flechais
Dept. of Computer Science
University of Oxford
ivan.flechais@cs.ox.ac.uk

ABSTRACT

Recent changes to data protection regulation, particularly in Europe, are changing the design landscape for smart devices, requiring new design techniques to ensure that devices are able to adequately protect users' data. A particularly interesting space in which to explore and address these challenges is the smart home, which presents a multitude of difficult social and technical problems in an intimate and highly private context. This position paper outlines the motivation and research approach of a new project aiming to inform the future of data protection by design and by default in smart homes through a combination of ethnography and speculative design.

INTRODUCTION

The General Data Protection Regulation elevated design guidelines referred to as Data Protection by Design and by Default to legal requirements within the EU. Manufacturers and designers are now required to consider data protection during the design process, making sure they comply with fundamental principles and requirements. Yet, it is non-obvious how such value-driven and abstract goals are to be translated into actual design requirements, let alone what designs that achieve such goals would look like, e.g. [3, 19].

CHI'19 Workshop on New Directions for the IoT: Automate, Share, Build, and Care, May 2019, Glasgow UK

WHAT DOES DPBD/D MEAN FOR BUSINESSES?

Excerpt of guidelines from the UK Information Commissioner's Office (ICO)

- Consider data protection part of design and implementation of systems, services, products and business practices.
- Make data protection a core functionality of data processing
- Anticipate and prevent privacy-invasive events before they occur
- Only process and use personal data that is needed for the organisation's purposes(s)
- Ensure that personal data is automatically protected in any IT system, service, product, and/or business practice
- Adopt a 'plain language' policy for any public documents
- Provide individuals with tools so they can determine how their personal data is being used
- Offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

Meanwhile, bad practices by large companies continue to come to light through whistle blowers and data breaches, highlighting the power imbalance between companies and their users, with the resulting public outcry underlining the need for better privacy protection. If this imbalance is to be addressed, and if companies are to comply with legal requirements, then more informed ways of approaching data protection are required [11, 19]. Of all the contexts that data protection by design applies to, the home is a particularly interesting place to research these issues because of its fundamental position in social life and the fact that smart home devices are becoming increasingly ubiquitous and unobtrusive [11, 18].

Research on smart device usage in the home has highlighted how dichotomies between users and administrators can also lead to power imbalances [9]. Configuration and maintenance of smart devices is typically carried out by a specific householder while the use of these devices might be shared with many, leading to conflicts and tensions between users [9, 15]. To avoid such situations, promoting inclusivity and collaboration between inhabitants through product design is paramount. While novel technology is often reported to be the cause of these issues, it also offers the key to addressing and preventing them.

In this position paper we present an outline of our ongoing research project which seeks to inform the future of Data Protection by Design and by Default (DPbD/D) in smart homes. We plan to achieve this by informing speculative design through ethnography and discussions with industry experts at partner organisations to map out the design landscape offered by DpbD/D. Specifically, we aim to:

(1) better understand the social embeddedness of technology use, individual and communal privacy practices
(2) develop and prototype reusable artefacts for DpbD/D
(3) evaluate and extend our findings in collaboration with industry and regulatory stakeholders to create applicable and actionable outputs

BACKGROUND & PRIOR WORK

The GDPR's principle of data protection by design and by default (see sidebar) is based on previous notions of privacy by design [2], with the aim of designing for higher-level values such as autonomy and privacy [3, 19]. A recent literature review of HCI design contributions for Privacy by Design highlights how many existing contributions used design to either solve a problem or to support and inform privacy decision making [19].

We agree that it is valuable for researchers to "explore people and situations and to critique, speculate, or present critical alternatives", especially where this is used to unravel "entangled relationships among the social, technical, and legal" [19]. This resonates well with others who reviewed the emerging field of privacy engineering and identified the need for more contextual research to fill in the gaps

between principle driven privacy regulation, a user-centred socio-technical perspective, and feature driven or problem-solving engineering practices [3]. We address the need for this research through our focus on *individual and communal privacy* for which, to the best of our knowledge, no theory of privacy exists [11, 19].

This need is illustrated by Lau et al. in their paper on smart voice assistants, where they argue the need for better privacy choice controls, a form of privacy enhancing technology (PET) [12]. PETs in user interfaces of devices allow individuals to state preferences for data collection, processing, and dissemination practices [13]. Despite these efforts, reports of questionable company practices and data leaks continue to cause power imbalances between users and manufacturers [4, 21]; on learning about data practices and repercussions of data breaches, experts and non-experts alike express feelings of "bewilderment, resistance, and sometimes resignation" [14, p. 3]. Prior work has identified related challenges for the individual user, e.g. abstract and a priori decision making [1], grasping the meaning of these settings [13], and challenges of appropriating products to fit their needs [12]. The complexity of navigating these situations is exaggerated through communal use, embedded in existing social order and dynamics, e.g. [5, 6, 20], and so a related power imbalance can be found within communities such as households sharing internet-connected devices [9, 20].

If Data Protection by Design and by Default is to become a tangible goal in software development and its benefits reality for users, then a holistic approach to understanding user needs and practices, producing artefacts for software and product design, and evaluating these with industrial and regulatory stakeholders are all required. Our prior research equips us with the required knowledge and skills to tackle this complex challenge.

RESEARCH APPROACH

Our previous research into transparency tools for smartphone apps [17], smart home devices (under submission), as well as other prior work [16] has explored the mental models and coping strategies that are used to navigate the complex information flows generated by smart devices in the home.

We have also explored the space of home technology use and support in our prior research from a security perspective [15]. Other prior work has also reviewed existing privacy literature to devise a road map for privacy research in the home [11]. From this, we have taken the initial step of exploring smart device usage through a series of interviews focusing on questions of procurement, daily use, and problem solving with internet-connected devices. We are currently working on using these insights to improve contextual design approaches and techniques with regards to usable security and privacy (under submission).

ETHNOGRAPHIC STUDY DESIGN

Ethnographic interview (⋄) study with ethnomethodology as analytic lens (n = 5-8 households)

Our visits will focus on

(A) existing practices with internet-connected, smart technology
(B) process of negotiating device placement, configuration, and potentially usage—after households choose from a pool of *'invasive'* devices, removing the economic entry barrier (see (T))
(C/D) routine use of devices and problem solving in relation to privacy as such practices evolve over time

With the above in mind, the project aims to further explore the unique privacy needs arising in smart homes, as well as the design techniques required to meet those needs. The three main stages of the project are as follows:

(1) An ethnographic longitudinal study to explore and understand individual and communal digital privacy practices pertaining to smart home devices and their privacy choice controls
(2) The prototyping of new tools, interfaces, and approaches to smart home privacy, informed by the longitudinal study, including co-design sessions with smart home users
(3) Discussions with smart home product designers, product teams, and compliance officers to understand how these alternative design approaches might be integrated into their DPbD/D processes

Individual and Communal Digital Privacy Practices

To disentangle the problem space of individual and communal digital privacy practices of smart home device use, we propose an ethnographic approach with ethnomethodology as analytic lens [7, 8]. We choose ethnomethodology as analytic lens because of its focus on how members of the household accomplish their goals and how they consider others in so doing, i.e. how they make their own actions accountable; and because of its value to system design and software development [7].

We will spend 6 months working with participating households, learning about their experience with existing and new smart technology (see sidebar). For this purpose, we offer households a number of smart devices from a pool of selected hardware—the mundanity that we are interested in is the use of internet-connected technologies embedded in social life. Ethnography with ethnomethodology as analytic lens allows us to observe the social embeddedness [6, 10] of technology use—"Humans are here to stay. Technologies come and go" – Tom Rodden, [7, p. 14].

Prototyping and Evaluating Design Artefacts

The second part of the project involves rapidly prototyping devices and interfaces that embody the implementation of data protection by design and by default in smart home devices, as informed by the results of the intial phase of the project. This space will be explored through iterative conceptual ideation, prototyping, development, followed by lightweight evaluation of a range of speculative prototypes, encompassing a range of different interfaces, features and UI design patterns. A small number of the initial outlines will be developed into functional prototypes.

The aim of these prototypes is to understand how alternative approaches to DPbD/D might better serve the needs identified of device users. We will also be exploring how alternative forms of transparency can help users develop useful and functional mental models of the internal logic and data processing practices of smart devices. By creating prototypes that back up transparency with

well reasoned follow on actions, we aim to support users in developing and realising their personal privacy preferences, including through better use of their legal rights as data subjects.

Integrating DPbD/D into Product Design

To identify and develop a range of DPbD patterns from an industry perspective, the final stage of the project will use focus groups targeted at developers, designers, and data protection compliance officers involved in the design of smart home devices and services to understand how the insights and artefacts that have been produced through stages one and two can be incorporated into the product lifecycle. Participants for the focus groups will be drawn from our industrial partners.

OUTLOOK

Effectively investigating the perceptions and behaviours that shape how people use IoT devices in the most private space in their lives is fraught with challenges. Through the combination of an HCI research approach with aspects of social science methodology and speculative design, we hope to explore the highly complex and idiosyncratic issues posed by the use of smart devices in the home. At the workshop, we hope to discuss the challenges around inclusively and effectively involving all users in the home with DPbD/D, sharing our insights with others and soliciting feedback on our own methods.

ACKNOWLEDGEMENTS

This research is part of our initiative 'Informing the Future of Data Protection by Design and by Default in Smart Homes' at the University of Oxford. Martin Kraemer and William Seymour are supported by the UK Engineering and Physical Sciences research council (EPSRC) through grant number P00881X/1.

Our project page:
https://www.cs.ox.ac.uk/projects/fosh/

REFERENCES

[1] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE security & privacy* 3, 1 (2005), 26–33.

[2] Ann Cavoukian. 2010. *The 7 Foundational Principles Implementation and Mapping of Fair Information Practices.* Technical Report. Information and Privacy Commissioner of Ontario. 10 pages. www.ipc.on.ca/images/Resources/gps.pdf

[3] Aaron Ceross and Andrew Simpson. 2018. Rethinking the Proposition of Privacy Engineering. In *Proceedings of the 2018 New Security Paradigms Workshop.* ACM, forthcoming.

[4] Andy Crabtree and Richard Mortier. 2016. Personal Data, Privacy and the Internet of Things: The Shifting Locus of Agency and Control. *SSRN* (2016), 1–20. https://ssrn.com/abstract=2874312

[5] Andy Crabtree, Richard Mortier, Tom Rodden, and Peter Tolmie. 2012. Unremarkable networking: the home network as a part of everyday life, In Proceedings of the Designing Interactive Systems Conference. *Proceedings of the Designing Interactive Systems Conference. ACM.*, 554–563.

[6] Andy Crabtree, Tom Rodden, Peter Tolmie, Richard Mortier, Tom Lodge, Pat Brundell, and Nadia Pantidi. 2015. House rules: the collaborative nature of policy in domestic networks. *Personal and Ubiquitous Computing* 19, 1 (2015), 203–215.

[7] Andy Crabtree, Mark Rouncefield, and Peter Tolmie. 2012. *Doing Design Ethnography* (1 ed.). Springer-Verlag London.

[8] Andy Crabtree, Peter Tolmie, and Will Knight. 2017. Repacking 'Privacy' for a Networked World. *Computer Supported Cooperative Work: CSCW: An International Journal* 26, 4-6 (2017), 453–488.

[9] Christine Geeng and Franziska Roesner. 2019. Who's In Control?: Interactions In Multi-User Smart Homes. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI'19.* ACM, forthcoming.

[10] Murray Goulden, Peter Tolmie, Richard Mortier, Tom Lodge, Anna Kaisa Pietilainen, and Renata Teixeira. 2018. Living with interpersonal data: Observability and accountability in the age of pervasive ICT. *New Media and Society* 20, 4 (2018), 1580–1599.

[11] Martin J Kraemer and Ivan Flechais. 2018. Researching Privacy in Smart Homes : A Roadmap of Future Directions and Research Methods. *IET Conference Proceedings* (2018), 1–10.

[12] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (nov 2018), 102:1—-102:31.

[13] M.C. Schraefel, R. Gomer, A. Alan, E. Gerding, and C. Maple. 2017. The Internet of Things: Interaction Challenges to Meaningful Consent at Scale. *Interactions* 24, 6 (Nov. 2017), 27–33.

[14] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.

[15] Norbert Nthala and Ivan Flechais. 2018. Informal Support Networks: an investigation into Home Data Security Practices. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 63–82.

[16] Irina Shklovski, Scott D Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, 2347–2356.

[17] Max Van Kleek, Reuben Binns, Jun Zhao, Adam Slack, Sauyon Lee, Dean Ottewell, and Nigel Shadbolt. 2018. X-Ray Refine: Supporting the Exploration and Refinement of Information Exposure Resulting from Smartphone Apps. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, 393.

[18] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2015. Smart homes and their users: a systematic analysis and key challenges. *Personal and Ubiquitous Computing* 19, 2 (2015), 463–476.

[19] Richmond Y Wong and Deirdre K Mulligan. 2019. Bringing Design to the Privacy Table - Broadening "Design" in "Privacy by Design" Through the Lens of HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*. ACM, forthcoming. https://doi.org/10.1145/3290605.3300492

[20] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security (SOUPS'17)*. USENIX Association, Berkeley, CA, USA, 65–80.

[21] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 200:1–200:20.