Trust in Home: Rethinking Interface Design in IoT

Cigdem Sengul
Brunel University London
Cigdem.sengul@brunel.ac.uk

Arthi Manohar
Brunel University London
Arthi.manohar@brunel.ac.uk

Jiahong Chen
University of Sheffield
jiahong.chen@sheffield.ac.uk

IoT systems in smart homes present several privacy challenges. To this end, we have been running design workshops to foster community discussion and collaboration among a multidisciplinary group of experts and early-career researchers in a design workshop. Through these creative design workshops, we aim to deepen understanding of the security, privacy, identity and trust issues with four use cases namely i) smart health, ii) smart appliances, iii) smart toys and iv) home security. Our work aims to build on previous creative approaches, and the findings from the workshop to provide a valuable insight to both further research and industrial implementation.

Privacy, Security, IoT devices, data protection, transparency, creative engagement.

1. INTRODUCTION

The THRIDI project aims to foster collaboration within an interdisciplinary community in the area of user-friendly interfaces for IoT in smart home settings. A rudimentary and catch-all approach to safeguard IoT systems are through access control infrastructures, which require high levels of privacy and security expertise to administer them, and therefore, are not fit for addressing legibility, agency and negotiability challenges in IoT. This is an active research area, requiring interdisciplinary expertise from computer science, communications engineering, Human-Computer Interaction, user-centric design, and law. To this end, the THRIDI project fills a critical gap by using creative design approaches in eliciting understandings around the perceptions of the functions, value and ethics of IoT smart home devices among multidisciplinary stakeholders.

IoT systems in smart homes present several privacy challenges. While GDPR creates a general duty for data controllers to implement data protection by default and by design, this obligation requires taking into account the state of the art. However, the state-of-the-art approach in the smart home context is in its infancy, requiring research into building accountability and trust via the appropriate design of user interface and access control systems.

We look at the problem of designing user-friendly interfaces from the lens of legibility, negotiability, agency - a framework proposed by the Human-Data Interaction Framework [7]. A well-known legibility challenge is due to the lack of appropriate interfaces for users to see the extent and the nature of the data collected ([1], Amazon Ring doorbells). User agency is also hard to achieve when devices are shared by different users with different relationships (e.g., housemates or family members). Similarly, the negotiability of data sharing may not be apparent to the users, as their privacy preferences and data sharing context change over time (e.g., changing needs for care in a smart home designed for healthcare scenarios).

One of the key issues in bringing legibility, agency and negotiability to user interfaces is users' lack the experience or knowledge to control the current IoT systems [2]. For instance, the technology for safeguarding personal data typically requires identity and access control systems. However, for access control to enhance user privacy and trust, authorisations should reflect a user's personal preferences and interests. Hence, the quality of protection of these access control models is only effective to that extent that users can express their privacy needs, and are aware of the potential risks of permitting data sharing [3]. This requirement entails that the IoT allows for end-user control, providing the users with the agency to tweak and personalise the way their data is shared and access is managed [4]. Such design would need to take into account the constraints of resources, time, attention and skills of the users, as well as their priorities in everyday life [5]. To this end, the THRIDI project initiates a community discussion and collaboration among a multidisciplinary group of experts and early career researchers. The first two-day workshop ran in November 2020. Following the success of the first workshop and subsequent reflections on possible improvements, we have organised a more compact edition of the workshop as part of BHCI 2021.

2. WORKSHOP AIMS AND OBJECTIVES

The THRIDI workshop aims to understand the challenges to legibility, agency and negotiability for data sharing in IoT and how to build user trust. The participants consider the technical, legal and business barriers and opportunities that will shape the implementation. The following table shapes all the design activities and discussions throughout the workshop.

	Legibility	***Agency***	**Negotiability**
Dynamic environment	Ensuring clear presentation of contextual factors	Ensuring conscious and affirmative action on context changes	Ensuring users can easily change their privacy preferences
Cognitive load	Avoiding information overload during set-up	Designing user-friendly consent prompts	Designing user-friendly reminders for privacy preferences
Lack of technology experience	Designing defaults that are representative of users' privacy inclinations	Ensuring poor knowledge of rights does not lead to poor privacy judgements	Ensuring adequate user participation
The multiplicity of people affected	Presenting information on situations when multiple people affect or are affected by data sharing	Ensuring control of data sharing, especially handling different personal relationships	Ensuring user preferences are in line with relationship dynamics
Regulatory compliance	Presenting rights in an understandable format	Facilitating users to exercise control over their personal data	Facilitating users to exercise their rights

Table 1. *Challenges to legibility, user agency and negotiability in the context of smart home IoT systems*

The workshops, so far, hosted designers, technologists, practitioners and HCI researchers from both academia and the industry who are already working in or who have an interest in IoT or data protection in smart homes, to share common experiences, challenges, and best practices, and to develop an agenda for future research. When selecting participants, we aimed to generate a balance of academia/industry, research areas, career stage, strategic awareness, and emphasised multidisciplinarity.

The format of the workshop was structured around four chosen use cases namely:

- Home Security
- Smart Toys
- Smart health
- Smart Appliances

These topics created a space for attendees to present and discuss their work, sharing expertise, as well as common experiences and challenges.

2.1 Workshop structure

Ice breaker activity

Participants were paired to complete the ice breaker activity. They were asked to fill out a short biography that unpacked some of the following questions:

What skills do you bring to the group discussion?
What are you expecting to gain from the two-day workshop?

These responses helped the facilitators to understand participants' expectations, and moreover the ice-breaker boards were left on Miro boards for the participants to familiarise other participants throughout the sessions.

Reflection and SWOT Analysis

Facilitators carefully selected 9 images for each use case to reflect activities that closely relate to the chosen IoT home use case. The images were prompts for participants to discuss i) what they liked about the product, ii) what they wished were different and iii) what they wished they knew or understood about them. The discussions were captured on post-its via their respective Miro boards and later grouped through a SWOT analysis.

Card Sorting Activity

The Card sorting activity consisted of two parts, the first part consisted of a set of cards focusing on images that represented Privacy and generic metaphors.

In the first part, the participants were shown 10 images representing Privacy. Example: Padlock, Bedroom, Living Room, Wallet etc. In the second part of card sorting activity, participants were shown 10 images that were more generic and represented metaphors. The images were inspired from the New Metaphor toolkit [6]. Example: Clouds, tinted window, adapters, ladder etc. Participants had 30 minutes to complete both this session, the outcome would reflect how the participants categorised the cards the most important to least important and any

other categories that would best fit the images. The project team carefully chose the images to be generic and at the same time relatable to all use cases.

Scenario cards
The scenario cards consist of two distinctive scenarios drafted specific to the use cases, where the participants were prompted with a series of questions to understand how they would respond to the given situations. Each scenario was carefully drafted such that it would help us understand how participants perceived trust and privacy within IoT home devices. Each scenario was discussed within the respective group and the discussions were captured via Miro by the facilitators.

Design Fiction and Role playing activity
A template was designed to allow participants to visualise the future of the specific use case. Participants were asked to imagine what the future would look like in 2050 where technology has advanced. This activity was aimed to introduce one way to deal with multiple futures and investigate the opportunities speculative approaches offer when it comes to highly complex socio-technical problems. Following the design fiction activity, one of the stories was chosen by the team where participants were asked to choose different roles to put themselves in an imaginary situation as various stakeholders.

3. Initial Findings from THRIDI Workshop

3.2 3.1. Home Security
Discussions ranged from transparency, usability, health and security risks posed by the devices. Alternative uses for home security and surveillance devices, such as monitoring plants and possibly to impose curfews for teenage family members, were considered. Concerns on data privacy as a user was also raised especially with devices installed in private spaces like bedrooms. Participants indicated the lack of design considerations that could help bring trust to the users such as transparency and legibility.

3.3 Smart Toys
Several themes emerged with respect to legibility and discussion revolved around data protection of minors, privacy labelling schemes, policies for Internet connectivity at home, and explainability of machine learning. The need for educating users as well as manufacturers and software developers have been emphasised. Participants expressed that there should be efforts in educating them as makers of technology and not only consumers of technology, especially when children are engaged with digital technology from a very young age. Discussions also demonstrated that there was a need for the privacy policy to be written age-appropriate to young users.

3.4 Smart health
Preliminary findings from the discussion indicated the themes emerged around the convenience such technologies bring to the users, using technologies for good (altruism), considering inclusive design principles when designing user interfaces. Participants raised concerns around information overload especially when designing for elderly users. critical perspectives were discussed when measuring data that is hard to quantify such as sleeping. Potential non-intrusive ways were discussed as possible solutions.

3.4 Smart Appliances

Discussions were mainly around what transparency challenges typical smart appliances are facing and what alternative approaches can help address the lack of genuine legibility to users. One theme especially salient in “smartified” conventional appliances (e.g. fridge, vacuum cleaner) is that there seemed to be some over-promise about whether the connected features are indeed needed. Participants indicated that physicalisation of data uses may help retain privacy.

4. Conclusion and Future Works

IoT systems in smart homes present several privacy challenges. While GDPR creates a general duty for data controllers to implement privacy by default and privacy by design, this obligation requires taking into account the state-of-the-art. However, the state-of-the-art in the smart home context is in its infancy, requiring research into building accountability and trust via the appropriate design of user interface and access control systems.

THRIDI workshops create a strong sense of collegiality and generate lively discussions. We hope to continue fostering community discussion and collaboration among a multidisciplinary group of experts and early-career researchers in design workshops.

Workshop Organisers

Dr Cigdem Sengul is a Senior Lecturer in Computer Science at Brunel University. Cigdem has more than ten years of experience in research and development in mobile and wireless networks in both academia and industry. Her work has been published in more than 50 journal and conference publications. Cigdem is a passionate advocate of increasing diversity awareness in computing. She is the Communication and Outreach Chair of ACM Women-Europe. Cigdem has experience in conference organisation in different capacities: TPC co-chair in Wireless Days 2015, Poster and Student

Research Competition co-chair in ACM Sigcomm 2015, N2Women session organiser in Mobicom 2020.

Dr Arthi Manohar is a Lecturer in Design, Brunel Design School at Brunel University London. Arthi is a design researcher, investigating the relationship between social design and technology. Her research and teaching explores the role of human values by investigating the relationship between social design and technology. Arthi has successfully organised 10 Design led workshops in the past 3 years as part of conferences and research projects which included researchers, designers and practitioners.

Dr Jiahong Chen is a Lecturer in Law at University of Sheffield. His research interests include data protection law, cybersecurity law, law and AI, data ethics and internet regulation. He completed his PhD on big data and data protection law at Edinburgh Law School, and subsequently worked at University of Nottingham as a Research Fellow in IT Law. His research has been published in leading peer-reviewed journals, such as *International Data Privacy Law*, *European Data Protection Law Review* and *Artificial Intelligence and Law*. He has also been actively engaged with policymakers to create substantial impact;he has given oral evidence to UK parliamentary inquiries as an expert witness and submitted responses to public consultations, many cited in the final reports.

3. REFERENCES

[1] J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun and H. Haddadi, "Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach," in Proceedings of the Internet Measurement Conference (IMC '19), 2019.

[2] J. Ullrich, A. G. Voyiatzis and E. R. Weippl, "The Quest for Privacy in the Consumer IoT," 2016.

[3]S. Wachter, "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR," Computer Law and Security Review, vol. 34, no. 3, p. 436–449, 2018.

[4] G. Broenink, J.-H. Hoepman, C. v. Hof, R. v. Kranenburg, D. Smits and T. Wisman, "The Privacy Coach: Supporting customer privacy in the Internet of Things," arXiv:1001.4459v1, 2019.

[5] I. v. Ooijen and H. U. Vrabec, "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective," J Consum Policy, p. 91–107, 2019.

[6] D. Lockton, D. Singh, S. Sabnis, M. Chou, S. Foley, and A. Pantoja. New Metaphors: A Workshop Method for Generating Ideas and Reframing Problems in Design and Beyond. In Proceedings of the 2019 on Creativity and Cognition (C&C '19). Association for Computing Machinery, New York, NY, USA, 319–332. DOI:https://doi.org/10.1145/3325480.3326570. 2019

[7] R. Mortier, H. Haddadi, T. Henderson, D. T. McAuley, and J. Crowcroft. 'Human-Data Interaction: The Human Face of the Data-Driven Society'. https://doi.org/10.2139/ssrn.2508051. 2014