This is a repository copy of *Inclusive privacy control at home for smart health*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/id/eprint/202578/

Version: Accepted Version

Book Section:
Manohar, A., Sengul, C. and Chen, J. orcid.org/0000-0002-1970-6762 (2023) Inclusive privacy control at home for smart health. In: Hayes, S., Jopling, M., Connor, S. and Johnson, M., (eds.) Human Data Interaction, Disadvantage and Skills in the Community: Enabling Cross-Sector Environments for Postdigital Inclusion. Postdigital Science and Education . Springer Cham , pp. 151-176. ISBN: 9783031318740

https://doi.org/10.1007/978-3-031-31875-7_9

This version of the book chapter has been accepted for publication, after peer review (when applicable) and is subject to Springer Nature’s AM terms of use, but is not the Version of Record and does not reflect post-acceptance improvements, or any corrections. The Version of Record is available online at: http://dx.doi.org/10.1007/978-3-031-31875-7_9

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Inclusive Privacy Control at Home for Smart Health

Arthi Manohar, Brunel University London, Uxbridge, UK, Arthi.Manohar@brunel.ac.uk, Cigdem Sengul, Brunel University London, Uxbridge, UK, & Jiahong Chen, University of Sheffield, Sheffield, UK

Abstract

Trust in Home: Rethinking Interface Design in IoT (THRIDI) project initiated a community discussion and collaboration among a multidisciplinary group of experts and early-career researchers in a series of design workshops. The THRIDI workshops have been designed based on the Human-Data Interaction (HDI) framework. The workshops use several methods to elicit discussion, ranging from card sorting to scenario analysis, on privacy perceptions in smart home settings and current barriers to achieving more trustable interactions with IoT devices. We demonstrate how creative workshops are useful in enabling critical reflection and knowledge exchange in a multidisciplinary context providing a useful bridge between radically different disciplines. The workshops brought together diverse viewpoints, and participants often emphasised the need for meaningful engagement with underrepresented and marginalised stakeholders across the entire technology design, development, and deployment processes. This chapter reports on the findings related to inclusivity that have arisen from discussions on health-related technologies in smart homes.

Keywords: Human-Data Interaction, Smart Health, Internet of Things, Privacy, Trust, Smart Homes, Design Thinking,

Introduction

Internet of Things (IoT) systems in smart homes present several privacy challenges. While General Data Protection Regulation (GDPR) creates a general duty for data controllers to implement data protection by default and by design, the state-of-the-art in the smart home context is in its infancy. Therefore, further multidisciplinary research is needed to build accountability and trust in home systems. To this end, we have adopted the Human-Data Interaction (HDI) (Mortier et al. 2014) framework and its three pillars: legibility, agency, and negotiability, to guide the appropriate design and implementation at home. As a first step, the Trust in Home: Rethinking Interface Design in IoT (THRIDI) project initiated a community discussion and collaboration among a multidisciplinary group of experts and early-career researchers in design workshops.

This chapter presents how we have built on the HDI framework to create design workshops composed of interactive, creative sessions to help unbox complex smart home technologies and support multidisciplinary understandings. Our workshops use several methods to elicit discussion, ranging from card sorting to scenario analysis, on privacy perceptions in smart home settings and barriers to legibility, agency, and negotiability. We report on the findings from two workshops conducted as part of the HDI network[1] plus and the British Human-Computer Interaction (BHCI) conference[2].

THRIDI workshops focused on four use cases: smart health, home security, smart appliances, and smart toys. Among all our use cases, inclusivity issues arise from discussions on health-related technologies in smart homes. Therefore, we present our findings on two smart-health scenarios, where discussions revolved around privacy and the ethical implications of installing, using and sharing data from smart health devices. We use these discussions to

[1] https://hdi-network.org/

[2] https://bcshci.org/

explore the privacy perceptions of end-users and highlight the importance of digital inclusion through exploring legibility, agency, and negotiability in both physical and online contexts.

A key observation in all workshops was the difference in perceptions of what can be considered private and varying sensitivities and expectations of privacy in smart homes. This difference is intriguing: our workshop participants come from different research backgrounds but can be considered more uniform in terms of technical proficiency and privacy awareness. They are also assumed to be more tech-savvy and privacy-conscious than the average user. Understanding these differences, which may manifest even in a seemingly homogeneous group, is key to understanding the obstacles to providing meaningful privacy control and achieving a more inclusive user agency at home. Reflecting on the discussions and findings from the workshops, the chapter concludes by highlighting the importance of multi-disciplinarity and inclusivity in smart-home design.

THRIDI and HDI Framework

Smart-home owners are exposed to privacy and security risks due to the well-reported vulnerabilities of connected devices (Chen et al. 2021), and these risks are expected to grow as the time spent at home increases, e.g., as a result of the Covid-19 pandemic, and the popularity of health and fitness tracking (Deloitte 2021). Therefore, it is not surprising that UK-wide legislation is in progress to establish an enforcement body to protect consumers from insecure connected consumer products (e.g., smart speakers, televisions, doorbells, and phones). However, the legislation addresses the top three issues in security - default passwords, vulnerability disclosure policies, and software updates. Considering that cyber security presents socio-technical challenges, it is necessary to consider the human factors involved as well as the computational elements to ensure and sustain the privacy and security of end users (Oltramari et al. 2015). To this end, the THRIDI project builds on the HDI framework to rethink interfaces to IoT systems in smart homes and consider specifically the impact on inclusive design.

Role of Legibility, Agency, and Negotiability in THRIDI

THRIDI is built on three core themes introduced within the HDI framework (Mortier et al. 2014).

- Legibility 'is concerned with making data and analytics algorithms both transparent and comprehensible to the people the data and processing concerns' (Mortier et al 2014: 5). 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 (Ren 2019: 267).
- Agency is concerned with giving people the capacity to manage and control their data within data systems. User agency is hard to achieve when devices are shared by different users with different relationships (e.g., housemates or family members).
- Negotiability is 'concerned with the many dynamic relationships that arise around data and data processing' (Mortier et al. 2014: 6). This theme encompasses changes in understanding and attitudes, social norms, and regulations over time.

As reflected in these themes, the perceptions of privacy in a domestic space shape how people interact with smart devices. At the same time, the situated interactions with those devices also shape the privacy perceptions in those spaces. However, understanding these interactions and acquiring the ability to control them in an accustomed or even intuitive manner takes time, a process akin to what Hardley and Richardson (2021) would consider digital placemaking. As a result, the sense of agency in a smart home is developed through a gradual, embodied experience of interacting with technological artefacts over time.

Legibility plays an important role to this end. However, Piasecki and Chen (2022:123) argue that transparency alone cannot be considered sufficient to protect vulnerable users' data. In addition, user education and training are vital not only for data protection but to enable effective data sharing. The systematic review of health-information exchanges carried out by Shen et al. (2019) show that the percentage of participants expressing privacy concern ranged from 15% to 74%, and people may withhold information due to privacy concerns. Importantly, it is noted that the patient privacy perspective is dynamic depending on the context, and experiencing the benefits of health information exchange systems increases acceptance.

Still, one cannot expect that once the data subject is informed, they will be immediately able to make informed choices and exercise their rights. For instance, the quality of protection from security systems is typically effective to the extent that users can express their privacy needs and are aware of the potential risks of permitting data sharing (Wachter 2018: 446). Therefore, IoT systems need to allow for usable end-user control, providing the users with the agency to tweak and personalise how their data is shared and access is managed (Broenink et al. 2019: 3-4). As users gain more control, it is essential to consider how to achieve and coordinate accountability amongst (joint-) controllers, especially when the 'boundaries of a smart home are remarkably more fluid' (Chen et al. 2020: 287-290).

Access control should be designed to consider the constraints of resources, time, attention, and skills of the users, as well as their priorities in everyday life (e.g., by using privacy icons, Ooijen et al. 2019: 98-99). For example, personal data custodians, and solutions like Databox (Mortier et al. 2016), solve the fundamental problem of controlling the flow of personal data by creating a central physical or virtual hub, i.e., physically or virtually hosted software with well-defined and access-controlled interfaces. However, administering these systems may require technical expertise and is an open challenge when multiple data subjects share the same set of devices, networks, and physical environments.

Agency, indeed, needs to be shared among a multitude of stakeholders when it comes to the use of data in a domestic IoT environment (Chen et al. 2020). Shared spaces challenge the more classic, over-simplistic subject-controls-object/data narrative that often perceives individuals almost as isolated atoms when exercising control. The limitations of the current individualised approach also to consent are well-documented in the literature (Mantelero 2016; Cohen 2019; Bietti 2019). (Geeng et al. 2019: 6), observing people in their smart homes for three weeks, find that 'tensions arise' among different stakeholders—including parents and children, roommates, partners, and non-occupants— at various phases of smart device use ranging from device selection and installation, regular use, to troubleshooting. They also observe a 'concentration of expertise, access, and control with the person who selects and installs smart devices at home' (Geeng et al. 2019: 1-2). For this reason, achieving agency is not just about enhancing the controllability of the data processing systems but, more importantly, about recognising the relational tensions exhibited in different aspects of control and facilitating the resolution of such tensions.

These considerations may have significant implications for inclusivity in smart homes. Some of the discriminatory effects of the accelerating adoption of smart home technologies have been discussed by Maalsen and Dowling (2020) and warrant further research. Specifically, transparency or legibility alone does not address the sense of unease where there is a delicate but potentially significant change in the smart environment that may especially impact children, older people, people with disabilities or people with domestically traumatic experiences. Their privacy perceptions of – and consequently, their trust in and control over – smart technologies could be affected by a more subtle array of factors. The onboarding process involving these users may therefore require additional care.

Negotiability might also affect the adoption of smart technologies. Meaningful control depends on the system's sensitivity to the environment's context as well as the user's situatedness (Calegari and Denti 2016: 309-312). If the decision to purchase and deploy a smart device can be seen as marking the first milestone of negotiation, then any further substantial changes in the relevant factors that have led to that decision should warrant renegotiation. Contextualised privacy expectations impact expectations of the functionalities of smart devices and vice versa. Such a two-way relationship is explored by Hardley and Richardson (2021: 333-334), who speak of digital placemaking as a function of smartphones in lockdown homes during the Covid-19 pandemic. They found out the corporeal intimacy of mobile phone users – even with the same users, same device and same domestic space – has shifted significantly towards greater 'publicness' as a place for working and socialising due to the change in the external environment, i.e. the stay-at-home restrictions.

Negotiability demands future-proofness, which is defined by Rehman and Ryan (2018: 716) (although in a different, sustainability-focused context) as follows: 'A system loses its capability if it cannot provide a solution to new requirements that emerge throughout its service such that the difference between the desired value of the system and its current value—known as the capability gap—cannot be reduced.' As such, smart homes are constantly subject to a range of changing parameters, requiring the systems to respond to these new requirements. For example, regarding changing relationships, a feature might be needed to facilitate reconfiguring control interfaces when a new member joins or an old member leaves the household. In this regard, changeawareness is an indispensable dimension of future-proofness in domestic IoT contexts.

Future-proofing design also forms an integral part of the broader inclusivity design agenda. At the moment, many IoT products targeting the generic market are often tailored only to the needs of the mainstream user segments (Zanella et al. 2020: 1), with the needs of disadvantaged, marginalised and disenfranchised users largely disregarded. Anticipating and pre-empting the eventuality that some users may go through a change in circumstances would not just lead to better support afforded to those users but also to users who are already subject to those conditions, making the system more accessible and inclusive.

Building on these related works and considerations, THRIDI workshops explore the challenges to legibility, user agency and negotiability in smart home IoT systems summarised in Table 1.

	Legibility	Agency	Negotiability
Changing homes	Ensuring a clear presentation of contextual factors which may affect disclosure behaviour	Ensuring conscious and affirmative action on context changes	Ensuring users can easily change their privacy preferences continuously through user-friendly interfaces
Cognitive load	Avoiding information overload (e.g., long privacy policies in legalese)	Designing user-friendly consent prompts regarding privacy preferences	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

Shared spaces	Ensuring transparency when multiple people are affected by data sharing (still safeguarding their privacy)	Ensuring control of data sharing, especially handling different personal relationships	Ensuring user preferences are in line with changes in relationships
Regulatory compliance	Presenting rights in an understandable format	Facilitating users to exercise control over their personal data, e.g., through consent	Facilitating users to exercise their rights, e.g., to erasure, data portability

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

THRIDI Use-Cases

THRIDI workshops were initially planned for four use-cases: 1) Home security, 2) Smart appliances, 3) Smart health, 4) Smart toys, and 5) Smart Entertainment. These use-cases were chosen due to their gaining popularity and needing further scrutiny for consumer IoT products, e.g., fitness devices and children's IoT connected IoT toys picked amongst issues that require 'urgent consideration' (Burton et al. 2021). However, Smart Entertainment was not run due to lack of participant interest. Compared to the other use-cases, the Smart Health use-case had rich inclusion discussions and hence, this chapter presents the findings from this use-case.

Smart Health is an actively researched area in IoT due to the potential of connected, interconnected, and remote medical care. Connected medical devices range from large equipment like imaging machines in hospitals and clinical settings to small wearable devices like heart rate monitors. Quantified-self is also growing in popularity with the growing use of less regulated connected fitness devices aimed at consumers. In both cases, vast amounts of health data can end up stored in the provider clouds.

According to the Ada Lovelace Institute (2020:31-33), IoT health devices bring significant complexity, such as legal challenges, understanding users' design needs, access to users' health data and users' relationship with the healthcare system. To this end, THRIDI explored i) the ethical implications of installing smart devices for healthcare and ii) privacy and ethical implications of data shared on health apps.

Inclusive design for domestic smart technologies was discussed as early as 2008 (Demiris and Hensel 2008). Similarly, the THRIDI workshops included scenarios that visualise and highlight the needs of users with diminished mental or physical abilities, especially in light of the ageing society. The design details of the workshops are presented in the following sections.

THRIDI Workshop Design

Creative Methods - A Diagnostic Tool

In THRIDI, different creative methods were explored to catalyse conversations with our interdisciplinary participants to help identify challenges. Creative methods such as speculative design (Bleecker 2009: 5) is adapted to understand participants' vision from existing to preferred state without the restrictions such as technology, politics and culture. To this end, design tools such as 'scenario cards' and 'future scaping' helped derive value from creating a fictional context through stories.

Creative methods have been explored in past studies (Marenko and van Allen, 2016; Mittelstadt et al. 2016; de Bruin and Floridi 2016, 2017) as a way to involve end-users in the co-creation and provocation of innovative human and non-human relationships to better understand uncertainties that technologies pose. More specifically, studies by (Maxwell et al. 2015; Nissen et al. 2017; Andersen 2019; Manohar and Briggs 2018) used creative approaches as a diagnostic tool to understand complex, opaque technologies such as Blockchain and AI. Such design-centric methods are arguably beginning to influence the wider, interdisciplinary research community, including Human-Computer Interaction.

Emerging technologies such as IoT often enter the market with little or no concern for design. While society adapts and technology develops, the creative approaches adopted in THRIDI will help designers re-understand their processes and re-invent new forms for a better user experience.

Workshop Design Methodology

The workshop activities were designed with three themes inspired by the HDI framework i) legibility, ii) agency, and iii) negotiability, and the activities highlighted the challenges raised within these three themes (Mortier et al. 2014 :8, see Table 1 and Table 2). The approach helped us apply various techniques such as image and text-based scenarios, card-sorting exercises, participatory design fiction, and role-playing activity designed to gain deeper insights into the user experience on IoT home devices. The workshops were structured to 'creatively engage' with participants using participatory activities to elicit understandings around the perception of the functions, values and ethics of emerging technologies and enable multidisciplinary knowledge across participants (Manohar and Briggs 2018 :2299). Miro[3] was used in both the workshops as an online whiteboard collaborative platform, where workshop design activities were predesigned and facilitated for each use case.

The activities for the one-day workshop are summarised in Table 2 and explained in detail in the next section.

HDI framework	Workshop schedule	Rationale
	Icebreaker	The icebreaker was designed for the participants to get to know their group members in a one to one setting and then share their thoughts with the wider group.
	Card sorting	Participants had 15 minutes to sort generic images of Wallet, Padlock, Door, Window, Wall, Bathroom, Bedroom, Living Room, Café, and Public Square. From 'most private' to 'least private'. The discussion was used for participants to get to know each other regarding their privacy stand.
	Reflection through image-based scenarios	Selected images showing different types of devices, users of different demographics, and shared and private spaces to prompt discussion on concerns on transparency and comprehensibility of the devices. The participants brought their examples to the discussion while reflecting on the current state-of-the art presented

[3] See https://miro.com/. Accessed 15 December 2022.

Legibility		for the use case.
	SWOT Analysis (Not included in 1-day workshop)	Discussions from reflection were then themed under SWOT analysis to identify the strengths, weaknesses, opportunities and risks of the topics participants discussed.
Agency	Scenario cards	Two distinct scenarios with exploratory questions were presented for the use cases to understand how participants perceived trust and privacy within IoT home devices.
Negotiability	Design Fiction	The future-thinking activity prompted participants to think about dynamic relationships and how individuals' and society's understanding and attitudes could change over time.
	Role-playing activity	

Table 2: Workshop participant-led activities designed according to the HDI framework

THRIDI Activities

Ice Breaker

Participants were paired to complete the icebreaker 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 workshop? These responses helped the authors understand participants' expectations, and the ice-breaker boards were left on Miro boards for the participants to familiarise themselves with other participants throughout the sessions.

Card Sorting

In the card-sorting activity, the participants were shown ten images representing privacy, e.g. generic images of Wallet, Padlock, Door, Window, Wall, Bathroom, Bedroom, Living Room, Café, and Public Square. Participants had 15 minutes to complete this session. In this 'closed card sorting activity', participants were given predetermined categories, namely 'most private' to 'least private'. The outcome would reflect how the participants categorised the cards from the most private to the least private and any other categories that best fit the images.

The images were chosen to be generic and, at the same time, relatable to all use cases. Typically, the images represented spaces within a home, such as a living room, a bedroom and a bathroom, prompting different privacy views and encouraging participants to prioritise activities, devices used in these spaces and other actors involved in different scenarios.

The card-sorting activity was used as a 'conversation tool' based on (Covey 2004:3). Participants shared their thoughts and reflections on their choices with the groups at the end of the session. The activity prompted discussions on how each participant approached privacy and helped understand participants' mental models of privacy. The activity also showed how to exchange and converge to a common language when describing privacy and its challenges.

Reflection Through Image-Based Scenarios

For each use case, nine images were selected to reflect activities closely related to each use case. The images intentionally were not named and had no description but had 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 goal is to allow the participants to share their thoughts and sometimes anecdotal experiences with the group.

The images shown in Figure 1 were presented to the participants under the Legibility theme for the Smart Health use case. The discussions were captured on post-its via their respective Miro boards.

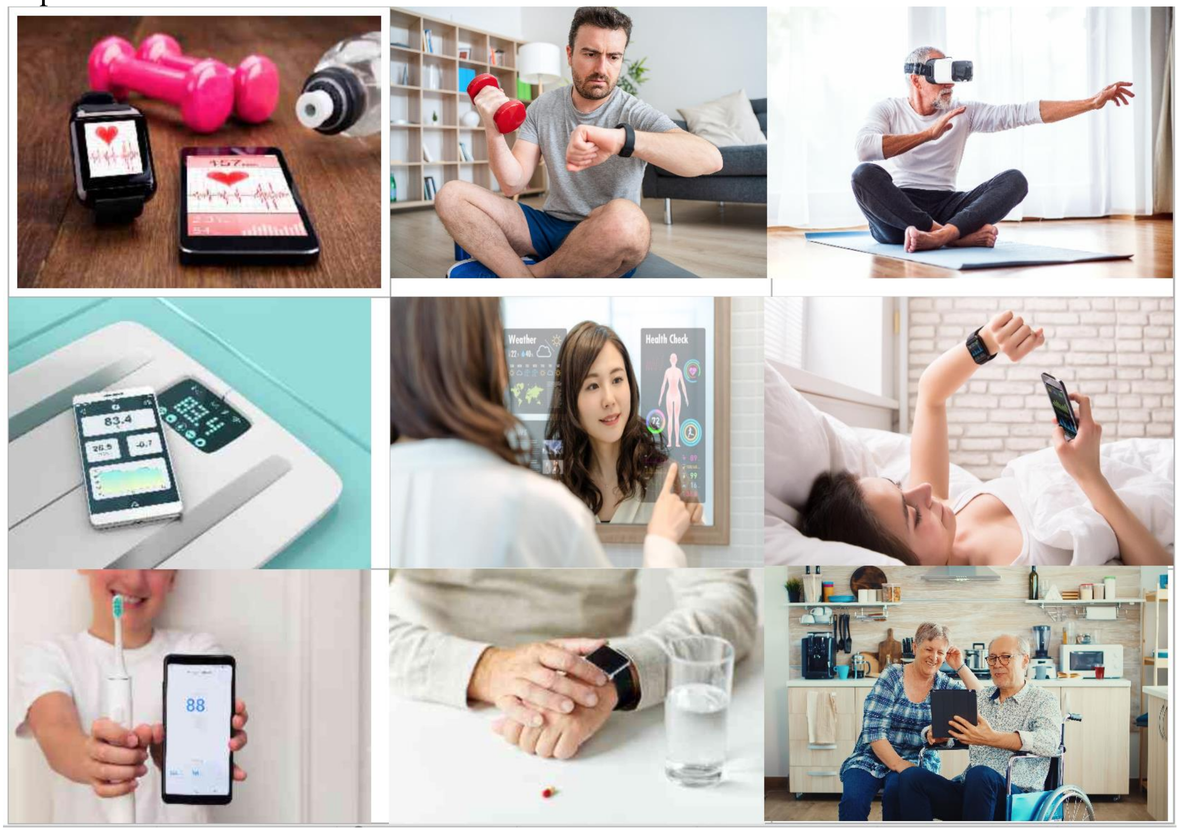


Figure 1: Nine images were presented to participants as part of the Smart Health use case. The images are representative of the challenges identified in Table 1, showing a range of health-related applications and their interfaces, the different contexts they may be used (from the bedroom, the bathroom to the living room, with varying privacy sensitivities), the multiplicity of people affected, and the presence of vulnerable people including children and older people with varying levels of technology expertise.

Scenario Cards

The scenario cards (Table 3) presented two distinct scenarios explicitly drafted for the use cases to understand how participants perceived trust and privacy within IoT home devices. The participants were prompted with a series of questions to understand how they would respond to the given situations. Scenario 1 has elements of challenges due to ‘shared spaces’, ‘cognitive load’, and ‘lack of technology experience’, while Scenario 2 ties to ‘changing homes’, ‘lack of technology experience’, and ‘regulatory compliance’). Participants had 30 minutes to complete this session, and the facilitators captured the discussions via Miro.

Scenario 1

Imagine you are running a care home for elderly residents and are now considering a plan of 'smartification', including the suggestion of installing a non-video monitoring system in private rooms in case of need for emergency assistance. The basic functions include detecting falling (objective movements that fit a particular pattern) and high body temperature, but additional sensors could also be deployed. Some of your colleagues think this is a good idea while others are more sceptical, and the same disagreement also exists among residents and their families. Some of your residents suffer from dementia or other diseases that might affect their judgement.
Scenario 2
Imagine you are subscribing to a lockdown mental health programme, partly because you have concerns about your wellbeing during an extended period of living alone and working from home. The programme involves installing an app that collects data from supported devices in your home, including your Fitbit, smartphone, smart thermostat, smart speaker, and smart TV. Lifestyle, dietary, and reading advice would be given depending on your routine activities and health data, and you designate a charity or next of kin in case potential mental health issues are detected. One day, you notice a fair amount of online adverts of books about fighting depression are being shown to you. You start to wonder: 'What is going on? Am I alright?'

Table 3: Design fiction scenarios presented to the participants as part of the Agency theme.

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 when technology has advanced. This activity aimed to introduce one way to deal with multiple futures and investigate the opportunities speculative approaches offer regarding highly complex socio-technical problems. Following the design fiction activity, the team chose one of the stories, and participants were asked to choose different roles such as Technologist, Designer, User with lower privacy concerns, User with higher privacy concerns, Legal Tech Expert and Government Regulator to put themselves in an imaginary situation as various stakeholders to discuss the chosen story.

THRIDI Workshops

The authors have organised two design workshops between November 2020 and July 2021. Due to the pandemic, the workshops were designed to run online. The first workshop was a two-day online event in November 2020, with three expert talks and 21 participants. The second workshop ran as a one-day event in July 2021 as part of the BHCI workshops with 11 participants. Therefore, the schedule was slightly altered to fit the activities within one day.

In addition to Miro, the participants communicated via Zoom for the first workshop and the Blackboard platform provided by the BHCI host for the second for group facilitation and breakout sessions. All sessions were audio-recorded, and where practical and decipherable, the audio files were transcribed.

Participant Selection

A call for Expressions of Interest (EoI) was publicised for both workshops. The calls were distributed on the project website, conference venue (BHCI 2021), and appropriate mailing lists and attendees were selected from submissions made. Applicants provided basic information such as name, background, and the selection criteria were based on two key questions: i) how their interests and expertise contribute to the multidisciplinary topic of the workshop, and ii) how they see themself fitting into the workshop with regards to online collaboration and team working.

Selection aimed to balance participation from academia and industry, representation of different research areas, career stage, strategic awareness and emphasised multi-disciplinarity. Twenty-one participants attended the first two-day workshop, and five participants participated in the Smart health use case in the designated break-out room. In the second workshop, 11 participants attended the one-day event.

Four participants engaged in the Smart health use case—Table 4 breaks down the demographics of the participants. Seven of the nine participants identified themselves as Early Career Researcher (ECRs). Six of the participants identified as coming from a Design discipline, and three from a Security and Privacy discipline. Finally, seven participants identified themselves as Female and two as Male. Participants came from an interdisciplinary background which facilitated a diverse discussion from challenges to solutions across design, systems design and law. All names have been changed (see Table 5).

The workshop agenda, a Participant Information Sheet and a Consent Form were provided to the participants before the workshop. In addition, an introductory presentation was provided to highlight the purpose of the day and how to use Miro.

Career stage (self- determined)	Applicants	Selected
Workshop 1	74.4% Early-career 25.6% Established	79.2% Early-career 20.8% Established
Workshop 2	83.3% Early-career 16.7% Established	85.7% Early-career 14.3% Established

Table 4. Make-up of participants in THRIDI workshops

Workshop 1 Pseudonyms		Discipline	Age	Workshop 2 Pseudonyms		Discipline	Age
Anna	ECR	Design	25-34	Shekar	ECR	HCI / Design	25-34
Kirsti	ECR	Design Socio technology	25-34	Sophie	ECR	HCI security and privacy	25-34
Rose	ECR	Design / HCI	35-44	Gabriela	ECR	HCI / Design	-
Lidia	ECR	HCI / Security privacy	25-34	Mary	Established	Security and privacy Data protection Law	35-44
Kumar	Est.	Design	35-44				

Table 5: Workshop 1 and 2 Smart Health Participant information table.

Workshop Reflection

Designing, facilitating, and delivering an online workshop was new to the authors. While initially, the workshops were planned to be in person due to the pandemic, they had to be hosted online. The online workshop provided a collaborative and inclusive space for participants from different parts of the world. Organising the workshop online also helped participants with childcare responsibilities to drop in and out as they preferred. This flexibility would not have been possible if the workshop had happened in person. The workshop took place in GMT; some participants from IST and PST time zones missed some sessions due to the time difference. Planning the sessions to accommodate participants' availability helped achieve an even distribution of the group and discussions.

After the HDI event, the authors applied lessons learned to create a more condensed one-day programme, choosing activities best understood and positively fed back by the participants. These changes were successfully applied in the BHCI workshop and in another event with the Security, Privacy, Identity and Trust Engagement NetworkPlus (SPRITE+), confirming the repeatability of our design with different stakeholders.

THRIDI Findings

Perceptions of Privacy

Based on preliminary analysis, card-sorting activity revealed interesting similarities and differences in perceptions of privacy (see Figure 3). Images of Bedroom (7/7), Bathroom (7/7) and Wallet (6/7) were commonly seen as the most private, whereas café (7/7) and public square (7/7) as the least private spaces. Window, Padlock, Door, and Wall were most commonly sorted as semi-private.

	Anna	Kirsti	Kumar	Shekar	Gabriela	Mary	Sophie
Bathroom	🟥	🟥	🟧	🟥	🟧	🟥	🟥
Bedroom	🟥	🟥	🟧	🟧	🟥	🟥	🟥
Wallet	🟧	🟨	🟧	🟥	🟧	🟧	🟥
Living Room	🩷	🟧	🟩	🩷	🟧	🟧	🟨
Window	🟨	🟧	🟥	🟨	🟦	🟨	🟩
Padlock	🟧	🩷	🟥	🟨	🟨	🩷	🟥
Door	🟨	🩷	🟥	🟨	🟦	🟨	🟨
Wall	🩷	🟧	🟨	🩷	🟨	🩷	🟨
Cafe	🟩	🟩	🟦	🟩	🟩	🟩	🟩
Public Square	🟦	🟦	🟩	🟦	🟦	🟦	🟦

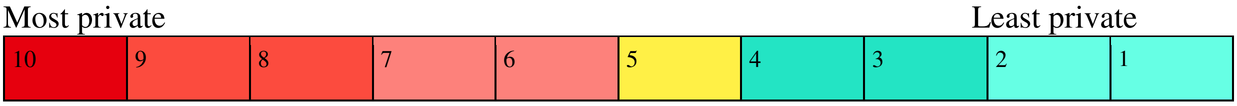


Figure 3: Participants privacy perception ranking from most private to least private visualised through heat map for Smart Health use case. (Not all participants have completed the card sorting on Miro; all names have been changed to pseudonyms.)

Participants considered that Wallet required agency, especially ‘very few people having access to data spending, for example’. Wallets were also seen to have a temporality element, depending on what it holds inside and in what context it is used, and who has access to it, especially the physical design of the wallet permitting them to reveal information about themselves when necessary. Shekar said: ‘You could see that there is a shared space with the family and possibly where my wife can go in my wallet and take some money out or show some ID to the delivery man, or something like that.’

Window (5/7) and Door (5/7) were viewed as semi-private elements that bring a certain level of control to the user – ‘window/door of its own space / own interior - depending on how visible it is’ (Anna, Workshop1). Wall had mixed responses across the two workshops. While some participants saw the Wall as an image representing privacy, others saw it as an object of ‘self-expression’ and could be interpreted at least as a semi-private element. One participant (Sophie, Workshop 2) commented on the context in which Wall is used and what people choose to have on the wall: ‘I’ve got [the] wall as not necessarily a boundary object, but I was thinking from the perspective it depends [on] what you have on the wall… people have looked to see what others have on a wall. So, it might not be the most private, depending on what you have on the wall.’

These card-sorting activities provided an early sense check about the privacy perceptions of participants. In addition, participants shared anecdotes that were hypothesised from experiences of people they knew and their own lived experiences.

> This reminds me of the time, one of my relatives, he got insurance which is related to the daily exercise that they do… (Shekar, Workshop 2)
>
> I just wanted to share, a few years ago, a doctor friend of mine, he is a medical professional… he mentioned to me… (Shekar, Workshop 2)

The analysis also showed interesting variations, e.g., Padlock or Door seen as most private, or Bathroom and Bedroom considered semi-private by some participants. These examples reveal how certain symbols might carry different connotations for different people, and the public/private concepts can be highly situational. People’s expected level of privacy in a given space can vary depending on the engaged activity; a cafe can be a public place but also can be the best place for the most intimate conversations.

A sentiment associated with a domestic space is conceivably challenging to capture due to the highly personal, mostly private, and sometimes sensitive nature of the space. The sense of privacy and control, even in a similar domestic space (e.g. living room or bedroom), can vary drastically from one user to another with subtle environmental, relational and contextual differences. Workshop discussions underline how smart devices form an essential part of the embodiment experience of making sense of the privacy parameters connected to different spaces of a smart home. Something clearly observable from the discussions was how participant’s privacy perceptions of a given home space, including, for example, the sense of privateness, sensitivity and intimacy of the same room, can change drastically with a subtle tweak of one of the internal or external variances forming the domestic environment. The factors affecting participants' privacy expectations range from political (e.g. surveillance culture in the country) to relational (e.g. presence of co-habitants) and technical (e.g. physical and data access by third parties).

Regarding the last category of technical factors, there is a common acceptance that smart devices play a significant role in our digital experience in contemporary homes. As one participant (Gabriela, Workshop 2) puts it: 'these kinds of issues, and use of smart appliances, are unexpected to certain people, spaces can actually have [a] huge impact on behaviour, and relationships and I think that would be something I think that it's important to plug out, especially, when thinking about the design of such technology.'

Perceptions of Smart Health

While the design activities aimed to trigger discussions on legibility, agency and negotiability in Human-Data Interaction, the smart health use case also triggered more general responses from THRIDI participants, which can be categorised as:

- Tech optimism vs tech mistrust,
- Designing for vulnerable people, and
- Systems thinking in smart health design.

While the discussion under each category has roots in how the participants reflected on privacy, security or data protection, they touch on different aspects of smart technology, e.g., seeing technology as an enabler for a better life or, on the flip side of the coin, a source of anxiety. The following sections summarises these discussions in these three categories.

Tech Optimism vs Tech Mistrust

The reaction to smart health technologies may be broadly categorised into (1) tech optimism and (2) tech mistrust (see Figure 3). Typically, people who are more optimistic about the technology associate smart health with wearables and quantified self. There is a general appreciation of the awareness technologies bring about information not available before. On capturing physiological measurements such as heart rate, a participant (Gabriela, Workshop 2) reflected: 'Before, we would not be tracking the heartbeat that often and as we would do if we [were] using smartwatches in our everyday lives. I think it gives a different perspective of who we are, how we operate in terms of a physical entity.'

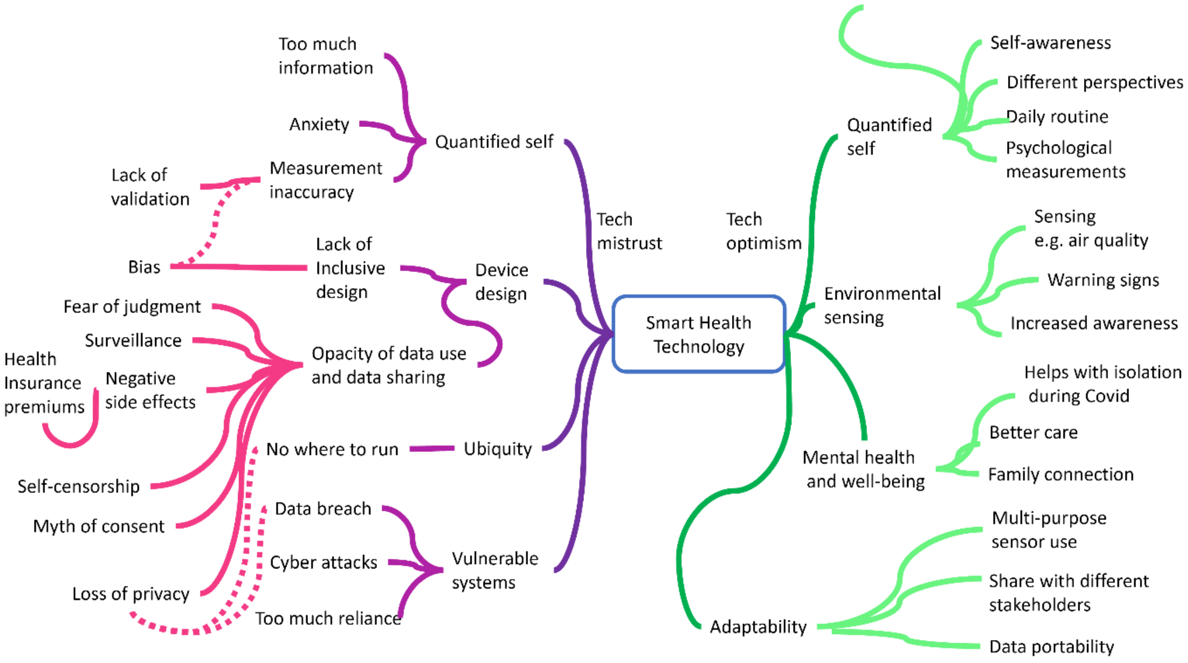


Figure 3: Discussions either veered towards tech optimism, pointing out the benefits of having more information about ourselves as well as about people under care. The same benefits also underlie the mistrust.

Participants often referred to ‘improved insights’, ‘awareness’, and improvements to their daily routine as positive aspects of technology. Also, being able to track people was considered an opportunity to detect deteriorating mental health and wellbeing and offer better care. Finally, an optimistic view of the future of these devices was also present, e.g., better data portability and multi-purpose use, enabling devices to be re-programmed for different measurements and data sharing among various stakeholders.

There is also a significant mistrust of technology. For example, despite its benefits, the quantified self is described as a reason for increased anxiety stemming from increased access to information, exacerbated by measurement inaccuracies. There was scepticism about technology for diagnosing mental health and wellbeing issues, where the lack of algorithmic validation was a cause for concern.

> What is available does not mean that it will not have false positives or even false negatives, you know, it might tell you that you are okay. When you are not really okay. And that is equally dangerous. And it might tell you that, you're having a heart attack for example, and, that is equally dangerous here you might have a heart attack just because you think the devices telling me you know, the universe is telling you that you're having one you might scare you, you might induce a panic attack. So things like that are really dangerous, you know, those are considered as biases, but there is actual bias within algorithms as well. (Shekar, Workshop 2)

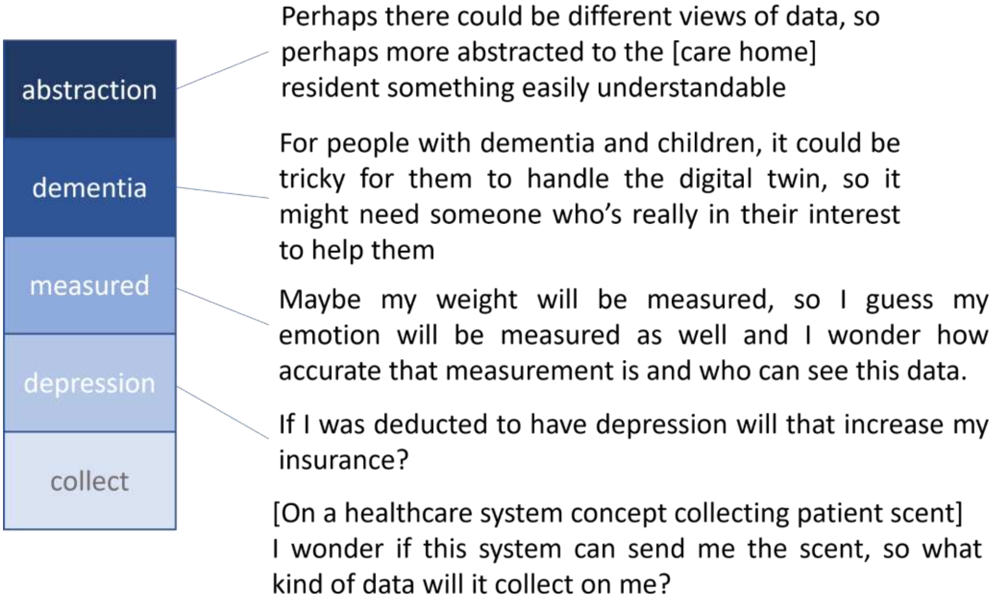
Several issues can be put under the umbrella of opacity in data use and sharing, where concerns include loss of privacy, surveillance, and fear of judgement, as well as negative side-effects like an increase in health insurance premiums. These concerns may affect take-up or lead to self-censorship, as one participant explained: ‘I assume everything is always being watched. So I think that I do not put any data out there that I am not okay with people knowing.’ (Kirsti, Workshop 1) The same participant commented: ‘I just personally do not put anything out there that I would not want anyone to know because I just assume someone is going to know it eventually.'

Finally, the ubiquity of smart devices leads to the feeling of 'there is no choice, everybody has to be involved' (Shekar, Workshop 2). As Figure 3 depicts, the negative factors often are interlinked, e.g., the general vulnerability of the current systems and devices to cyber-attacks and data breaches amplify the feeling of loss of privacy.

Designing For Vulnerable People

Workshop participants also brought a wide range of vulnerabilities into the discussion, which showed that 'individuals can be vulnerable where circumstances may restrict their ability to freely consent or to object to the processing of their personal data, or to understand its implications', matching instinctively the ICO's sentiment (Information Commissioner's Office 2022). They believed vulnerability could emerge as a result of:

- Being under temporary or permanent care, such as children, or an elderly relative, who are losing their cognitive abilities.
- Being mentally unwell, e.g., suffering from depression.
- Power imbalances that may be seen in employee-employer relationships or personal relationships.
- Power imbalances between providers and users of smart systems, as well as vulnerability due to privacy and security threats imminent in a smart home.



Perhaps there could be different views of data, so perhaps more abstracted to the [care home] resident something easily understandable

For people with dementia and children, it could be tricky for them to handle the digital twin, so it might need someone who's really in their interest to help them

Maybe my weight will be measured, so I guess my emotion will be measured as well and I wonder how accurate that measurement is and who can see this data.

If I was deducted to have depression will that increase my insurance?

[On a healthcare system concept collecting patient scent] I wonder if this system can send me the scent, so what kind of data will it collect on me?

Figure 4: The top 5 vulnerability concepts based on a word frequency analysis with generalisations

Figure 4 shows the top concepts that frequently appeared in discussions. Some of these words appear in our scenarios; however, the discussion around them organically deviated from the scenarios. The concepts and accompanying example statements illustrate that as devices continuously monitor and 'measure' not only physiological parameters but also our 'emotions' inevitably lead people to feel more exposed and more vulnerable. In addition, the fluidity of vulnerability was discussed, e.g., in the case of dementia patients, where cognitive abilities may vary at different stages of the illness. This issue presents a dilemma to caregivers who need to decide between respecting the patient's privacy and disclosing adequate information to their legal representatives. Finally, lack of technology experience has been brought up as a barrier to digital inclusion: 'for people who lack technology experience (Lidia, Workshop 1), we could try to ensure they have adequate participation'.

Systems Thinking in Smart Health Design

While the participants were shown technology examples and scenarios that affected home settings, they made links to broader data collection, e.g., connected to an external healthcare system for remote diagnosis and monitoring and, more generally, as part of smart cities. For example, a natural connection was made from sensors in toilets at home to sensors in city sewer systems. Also, sensors were expected to cover a large area beyond the control of a single user – 'so there is no choice: everybody has to be involved, or nobody is involved' (Shekar, Workshop 2).These connections directed discussions towards holistic, user-friendly systems, the same participant reinforced that such holistic approach can protect different data at a range of levels' (Anna, Workshop1). The following section highlights proposed approaches to Smart Healthcare by our participants based on the discussion presented in this section.

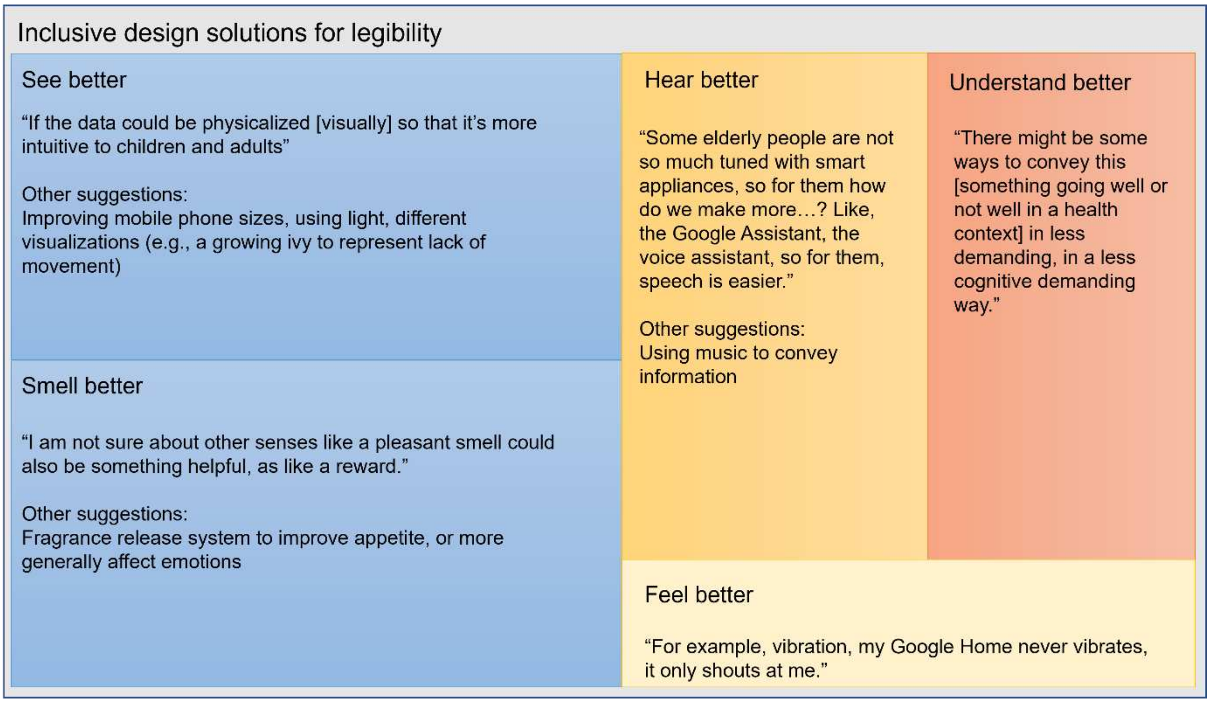
Privacy-Aware Smart Healthcare Design

Based on the privacy perceptions on smart health discussed in the previous section, privacy needs to be built into the systems. HDI framework of legibility, agency, and negotiability played again a key role to organise the discussions around designing for privacy-aware smart healthcare. In particular, the following questions raised by our participants, which are discussed in the rest of this section:

1. How should the technology makers consider users' mental capacity to make decisions on health data and the potential ethical impact? (Legibility/Agency)
2. Can the devices potentially take into account the data management system and make the process transparent to address the system's complexity? (Legibility/Agency)
3. How could better control features be designed so that control could be shared across necessary stakeholders and users with limited mental capacity while considering changes in user condition? (Agency/Negotiability)

Better Interfaces for Better Legibility and Accessibility

Question 1 was discussed mainly under two categories: (1) exploration of multimodal interfaces that will convey information differently for different users, and (2) making sure people understand the processes behind automated decision-making, especially, explainable machine learning and AI (Artificial Intelligence).



Inclusive design solutions for legibility

See better

"If the data could be physicalized [visually] so that it's more intuitive to children and adults"

Other suggestions:
Improving mobile phone sizes, using light, different visualizations (e.g., a growing ivy to represent lack of movement)

Smell better

"I am not sure about other senses like a pleasant smell could also be something helpful, as like a reward."

Other suggestions:
Fragrance release system to improve appetite, or more generally affect emotions

Hear better

"Some elderly people are not so much tuned with smart appliances, so for them how do we make more…? Like, the Google Assistant, the voice assistant, so for them, speech is easier."

Other suggestions:
Using music to convey information

Understand better

"There might be some ways to convey this [something going well or not well in a health context] in less demanding, in a less cognitive demanding way."

Feel better

"For example, vibration, my Google Home never vibrates, it only shouts at me."

Figure 5: Hierarchy chart for inclusive design solutions for legibility exploring multimodality. The bigger the box, the higher the coding frequency.

Multimodal Interfaces

The challenge is to ensure privacy awareness without creating a cognitive burden, which was one of the issues raised, especially for the elderly population. Participants envisioned multimodal interfaces where all senses are included in conveying information about the act of data collection and the data itself (see Figure 5). Visual, olfactory, and auditory inputs have been mentioned with the highest frequency, where speech interfaces were explicitly considered more user-friendly for the elderly. Better visualisation, e.g. a growing ivy to symbolise inactivity to motivate movement, was suggested for creating more understandable interfaces for children and the elderly.

On the other hand, the olfactory examples, fragrance release for motivating a specific behaviour (e.g., improving appetite) or affecting emotion, triggered ethical questions. Therefore, multimodal interfaces should be considered carefully; while they may help improve the cognitive burden on users, the purpose should be clarification and not manipulation.

Explainable AI

Machine learning and AI is playing an increasingly important role in making IoT devices smarter. In our workshops, the participants discussed several research projects where machine learning was used to detect abnormal conditions, e.g. heart rate variability to detect a heart attack early. While such advances may bring significant benefits, the boundary between an IoT device used for smart health versus a medical device is blurring. Then, the obvious questions are how these devices are regulated, prescribed and monitored.

In addition, the participants emphasised the need for Explainable AI, offering users an explanation as to why the algorithm decided on a particular output.

> With technology, specifically with AI, it is considered a myth because the algorithm itself is not open. And it is not open, not because the company has a proprietary right. It's not open because, well, it is designed that way. It's a black box, and it takes big mathematicians to understand what is going on. (Shekar, Workshop 2)

While one desired outcome with explainable AI is to improve legibility, participants also saw a potential for identifying misuse: 'If there's a problem with the algorithm, if there's any bias in it, then it could potentially be used for malicious purposes, you know, making you think that you're unwell.' (Sophie, Workshop 2)

While the advances in machine learning, e.g., deep learning, led to more efficient algorithms, explainability was somehow lost, as these systems work as 'uninterpretable black boxes', lacking mechanisms to explain their actions and behaviour (Goebel et al. 2018: 296). However, making machine decisions transparent, understandable and explainable would increase acceptance and trust, especially when AI is used for medical reasoning.

On the other hand, explainability in AI is a challenge. For now, even if explainable algorithms are deployed for medical practices, human supervision is necessary. Tjoa et al. (2021: 4809) suggest acknowledging that machine and deep learning might not be mature for large-scale deployment yet, and instead, it might be better to see them as a secondary support system.

Better Home Controllers to Overcome Power Conflicts Over Agency

One control mechanism that has repeatedly been highlighted by the participants as problematic is due to the relational tensions exhibited in shared homes. The relational dynamics augmented or transformed by smart technologies have been discussed in the workshop by three categories of scenarios, as explained below. While the participants have framed the changing dynamics as a result of technologies, the authors consider this to have also to do with the existing power conflicts, summarized in the next three sections.

Data Control Due to Imposed or Negotiated Domestic Power

One family member's control is often subject to relational and technical boundaries (co-) determined by/with other members. For example, the implications of parental control for children's agency when using smart devices have been discussed. A similar strand of discussion also concerns users with dementia. It is unclear what constitutes meaningful consent or who should give consent in these scenarios.

Domestic Power Created by Data Control

One member's control over data and device functionalities may impact the privacy, behaviour and even wellbeing of other household members. Health data is one example pointed out by the participants, who question the ethical considerations of one member consenting to share health data collected by smart devices. It should be clarified here that the concerns are beyond the unauthorised sharing of somebody else's data, but more about the separability of household health data, or even more complicated, the information about family members extractable from one's own data (e.g., genetic data).

Power Struggle with External Actors

The control (or the lack of it) by household members is also subject to technical constraints determined by actors outside the household. The increasingly ubiquitous presence of smart devices built into the domestic environment raises particular concerns among participants about whether consent would indeed be a meaningful protective mechanism. As a hypothetical but perhaps not too far-stretched case in point, there is a risk that local councils may make future social housing available on the condition that prospective residents consent to the collection of energy data or even the automated restriction on energy consumption. The power imbalance may render the consent unethical or unlawful altogether.

Summary

The agency of individual users of domestic IoT technologies is often an experience of power conflicts between household members and between them and external stakeholders. These will clearly create inclusivity risks to those who find themselves in the weaker position in such power tensions like children, adults with diminished abilities, domestic abuse victims and low-incomers. The regulatory implications of this are that policymakers might need to go beyond considering the relevant issues simply as technological issues that can be 'fixed' with technological solutions and start considering the entrenched power conflicts and the appropriate human approaches.

User-In-The Loop – (Re)Negotiability at Times of Fast Changes

As partly highlighted above, smart home environments are highly fluid and dynamic, subject to constant changes in technological, relational and contextual variables. This poses serious challenges to the very idea of negotiability in IoT contexts. The concept of negotiability is built on the presumption of foreseeability and relative stability of the near future, which provides a predictable basis for the negotiating parties to weigh up the benefits and risks. An obvious and typically straightforward to predict kind of change is life stages, for which people tend to naturally make future plans. However, there is also a range of other factors constantly changing what will come into play in smart homes, such as new devices, new software updates, new users or visitors, new third-party data recipients, and new data uses.

These changes often take place within a much shorter timeframe, with fewer opportunities for household discussions and sometimes in a much less bargainable manner. Some of these changes might be minor, but others might affect the shared understandings or principles underlying the initial negotiation. The authors, therefore, question the extent to which the negotiation that was carried out at the point of, say, deployment will remain relevant and meaningful over time.

The discussions among our participants have underlined the challenge that, even if the rights and duties had been negotiated in a genuinely informed manner in the first place (which is questionable in practice), changes in the circumstances might break up the equilibrium established previously. It should be pointed out that, while not explicitly discussed in the workshop, we assume negotiability is subject to certain constitutional constraints, such as fundamental rights not being something that can be signed away. Regarding the kinds of changes that could trigger the renegotiation, at least four such categories have been brought up spontaneously during the discussions: security measures, available updates, user conditions and relationships, and stakeholder needs.

It has been discussed, for example, how users with a deteriorating mental capacity (e.g., patients with dementia) could renegotiate ways in which they are kept informed of data uses. The importance of the ability to re-adjust privacy and otherwise configurations of smart devices has been emphasised by one participant:

> Negotiation and renegotiation of the control mechanisms and allowances [should] take place so that everyone is fully aware of in context, new needs, acceptances, and actually such activities could help people to identify their own levels of acceptance in this case, and it's absolutely fine, I think, to change opinions. (Gabriela, Workshop 2)

Enabling Negotiability with Future-Proofness

In terms of what measures could be taken to improve negotiability in smart technologies, there are suggestions by workshop participants around cognitive, legal, and technical solutions, although the focus is clearly on the last category.

Change-awareness is an indispensable dimension of future-proofness in domestic IoT contexts. One participant described the need for this feature in system design as:

> So I wonder, like, with the interface design, how could we make it more intuitive to the user that they can change their preference dynamically. Maybe at the moment, I feel very healthy, and I do not want my data to be shared, but maybe at a later stage when I need some medical help with my mentality, then probably I can open that setting again. (Lidia, Workshop 1)

Perhaps more fundamentally, and beyond interface design, it is necessary to further reflect on how the smart home infrastructures should be transformed to facilitate adjustments to change in the circumstances. Furthermore, a feature might be needed to facilitate the reconfiguration of control in the case of a new member joining the household.

This reflection should also include the physical infrastructures as well as the data ones, such as data formats that would allow, for example, increased interoperability or data sharing protocols that have taken into account the possible changes in the user's mental capacity.

It should also be noted that while the workshop discussion has primarily focused on how system design as a technical solution can be future-proof, there is no reason why the cognitive and legal measures could not be improved in a similar way. Quite the opposite, truly effective future-proofness requires efforts on all three fronts.

Conclusion: The Future Is Interdisciplinary and Inclusive

The THRIDI workshops enabled rich and crucial discussion around privacy concerns with respect to improving legibility, agency and negotiability for smart health at a time when there is a greater push for using digital tools to move care closer to or in people's homes (GOV.UK. (2022). The workshop participants touched on several areas that would benefit from an interdisciplinary and inclusive approach.

In terms of legibility, designing in privacy and trust, physicalisation of privacy (e.g. through multimodal interfaces), and algorithmic explainability were mentioned the most often. In terms of agency, the discussion focused on inclusive design, proper control and interfaces, and new privacy-enhancing technologies. One of the most emphasised control measures was the flexibility to administer devices by multiple people. The authors also observed that holistic, user-friendly solutions take the lead in terms of negotiability. Finally, participant discussions highlighted an interesting legibility and negotiability dilemma: transparency in data collection, processing, and analysis versus overwhelming users, sometimes emotionally, with too much information.

In summary, the workshops brought together diverse viewpoints, and participants often emphasised the need for meaningful engagement with underrepresented and marginalised stakeholders across the entire technology design, development, and deployment processes. The core conceptual and methodological challenges in designing for smart homes require interdisciplinary research bridging cognitive, legal, technical and design fields, while, even with our participants, the proposed solutions veer towards primarily technical. However, inclusive and holistic design approaches are needed to elicit understanding around the perceptions of the functions, values and ethics of emerging technologies.

To this end, the THRIDI workshops can serve as a model to manage discussions, possibly retrofitted around a particular product, rather than a broad use case. The THRIDI activities allow people to understand each other's privacy perceptions and expectations regarding legibility, agency, and negotiability. The workshop provides a reflective, hands-on context to debate, challenge, and ideate with an interdisciplinary group assisting the development of smart systems. Using these creative methods would help close the gap in technical understanding of opaque technologies (like IoT) and support debates among a wide range of stakeholders, ranging from designers and technologists to policymakers and end-users.

Acknowledgments

This work was supported by the Engineering and Physical Sciences Research Council (grant numbers EP/R045178/1, EP/M02315X/1, EP/ T022493/1, EP/R03351X/1).

References

Ada Lovelace Institute. (2020). The data will see you now. Datafication and the boundaries of health. https://www.adalovelaceinstitute.org/report/the-data-will-see-you-now/. Accessed 29 October 2020.

Andersen, K. (2019). The Magic Machine Workshops: Making Personal Design Knowledge. In A. Cox & V. Kostakos (Eds.), *CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-13). New York: Association for Computing Machinery. https://doi.org/10.1145/3290605.3300342.

Bietti, E. (2019). Consent as a free pass: platform power and the limits of the informational turn. *Pace Law Review, 40*(1), 7.

Bleecker, J. (2009). Design Fiction: A short essay on design, science, fact and fiction. Near Future Laboratory. https://shop.nearfuturelaboratory.com/products/design-fiction-a-short-essay-on-design-science-fact-and-fiction. Accessed 15 December 2022.

Broenink, G., Hoepman, J.-H., Hof, C. v., Kranenburg, R. v., Smits D., & Wisman, T. (2019). The Privacy Coach: Supporting customer privacy in the Internet of Things. *arXiv:1001.445.* https://doi.org/10.48550/arXiv.1001.4459.

de Bruin, B., & Floridi, L. (2017). The Ethics of Cloud Computing. *Science and Engineering Ethics, 23*(1), 21–39. https://doi.org/10.1007/s11948-016-9759-0.

Calegari R., & Denti, E. (2016). The Butlers Framework for Socio-Technical Smart Spaces. In F. Bagnoli, A. Satsiou, I. Stavrakakis, P. Nesi, G. Pacini, Y. Welp, T. Tiropanis, & D. DiFranzo (Eds.), *Internet Science: Third International Conference, INSCI 2016, Florence, Italy, September 12-14, 2016, Proceedings* (pp. 306-317). Cham: Springer. https://doi.org/10.1007/978-3-319-45982-0_26.

Cannizzaro, S., Procter, R., Ma, S., & Maple, C. (2020). Trust in the smart home: Findings from a nationally representative survey in the UK. *PLoS One*, *15*(5), e0231615. https://doi.org/10.1371%2Fjournal.pone.0231615.

Chen, J., Edwards, L., Urquhart, L., & McAuley, D. (2020). Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. *International Data Privacy Law, 10*(4), 279-293. https://doi.org/10.1093/idpl/ipaa011.

Chen, J., & Urquhart, L. (2021). 'They're all about pushing the products and shiny things rather than fundamental security': Mapping socio-technical challenges in securing the smart home. *Information & Communications Technology Law, 31*(1), 99-122. https://doi.org/10.1080/13600834.2021.1957193.

Cohen, J. E. (2019). Turning privacy inside out. *Theoretical inquiries in law, 20*(1), 1-31. https://ssrn.com/abstract=3162178

Covey, S. (2004). *The 7 Habits of Highly Effective People: Powerful lessons in person change.* New York: Free Press.

Deloitte. (2021). The connected home: Just getting started. https://www2.deloitte.com/uk/en/pages/technology-media-and-telecommunications/articles/the-connected-home-just-getting-started.html. Accessed 15 December 2022.

Demiris, G., & Hensel, B. K. (2008). Technologies for an aging society: a systematic review of "smart home" applications. *Yearbook of medical informatics, 17*(1), 33-40. http://dx.doi.org/10.1055/s-0038-1638580.

Geeng, C., & Roesner, F. (2019). Who's In Control? Interactions In Multi-User Smart Homes. In A. Cox & V. Kostakos (Eds.), *CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-13). New York: Association for Computing Machinery. https://doi.org/10.1145/3290605.3300498.

Goebel, R., Chander, A., Holzinger, K., Lecue, F., Akata, Z., Stumpf, S., Kieseberg, P., & Holzinger, A. (2018). Explainable AI: The New 42?. In A. Holzinger, P. Kieseberg, A. M. Tjoa, & E. Weippl (Eds.), *Machine Learning and Knowledge Extraction Second IFIP TC 5, TC 8/WG 8.4, 8.9, TC 12/WG 12.9 International Cross-Domain Conference, CD-MAKE 2018, Hamburg, Germany, August 27–30, 2018, Proceedings* (pp. 295-303). Cham: Springer. https://doi.org/10.1007/978-3-319-99740-7_21.

GOV.UK. (2022). A plan for Digital Health and Social Care (2022) GOV.UK. Department of Health and Social Care. https://www.gov.uk/government/publications/a-plan-for-digital-health-and-social-care/a-plan-for-digital-health-and-social-care (Accessed: January 5, 2023).

Hardley, J., & Richardson, I. (2021). Digital placemaking and networked corporeality: Embodied mobile media practices in domestic space during Covid-19. *Convergence*, *27*(3), 625–636. https://doi.org/10.1177/1354856520979963.

Information Commissioner's Office. (2022). When Do We Need to Do a DPIA? Wilmslow: Information Commissioner's Office. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/. Accessed 15 December 2022.

Maalsen, S., & Dowling, R. (2020). Covid-19 and the accelerating smart home. *Big Data & Society*. https://doi.org/10.1177/2053951720938073.

Manohar, A., & Briggs, J. (2018). Designing With Black Box Technologies and PD. In C. Storni, K. Leahy, M. McMahon, P. Lloyd, & E. Bohemia (Eds.), *Design as a catalyst for change - DRS International Conference*. London: Digital Research Society. https://doi.org/10.21606/drs.2018.296.

Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer law & security review*, *32*(2), 238-255. https://doi.org/10.1016/j.clsr.2016.01.014.

Marenko, B., & van Allen, P. (2016). Animistic design: how to reimagine digital interaction between the human and the non-human. *Digital Creativity, 27*(1), 52–70. https://doi.org/10.1080/14626268.2016.1145127.

Maxwell, D., Speed, C., & Campbell, D. (2015). "Effing" the ineffable. In S. Lawson & P. Dickinson (Eds.), *British HCI '15: Proceedings of the 2015 British HCI Conference* (pp. 208–209). New York: Association for Computing Machinery. https://doi.org/10.1145/2783446.2783593.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2), 205395171667967. https://doi.org/10.1177/2053951716679679.

Mortier, R., Haddadi, H., Henderson, T., McAuley, D., & Crowcroft, J. (2014). Human Data Interaction: The Human Face of the Data-Driven Society. *SSRN Electronic Journal.* http://dx.doi.org/10.2139/ssrn.2508051.

Mortier, R., Zhao, J., Crowcroft, J., Wang, L., Li, Q., Haddadi, H., Amar, Y., Crabtree, A., Colley, J., Lodge, T., Brown, T., McAuley, D., & Greenhalgh, C. (2016). Personal Data Management with the Databox: What's Inside the Box? In M. Yuksel & T. Wood (Eds.), *CAN '16: Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking* (pp. 49–54). New York: Association for Computing Machinery. https://doi.org/10.1145/3010079.3010082.

Oltramari, A., Henshel, D., Cains, M. G., & Hoffman, B. (2015). Towards a Human Factors Ontology for Cyber Security. In K. Blackmond Laskey, I. Emmons, P. C. G. Costa, & A. Oltramari (Eds.), *Proceedings of the Tenth Conference on Semantic Technology for Intelligence, Defense, and Security, Fairfax VA, USA, November 18-20, 2015* (pp. 26-33). http://ceur-ws.org/Vol-1523/STIDS_2015_T04_Oltramari_etal.pdf. Accessed 15 December 2022.

Van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy, 42,* 91–107. https://doi.org/10.1007/s10603-018-9399-7.

Piasecki, S., & Chen, J. (2022). Complying with the GDPR when vulnerable people use smart devices. *International Data Privacy Law,* *12*(2), 113-131. https://doi.org/10.1093/idpl/ipac001.

Rehman, O. U., & Ryan, M. J. (2018). A framework for design for sustainable future-proofing. *Journal of Cleaner Production*, *170*, 715-726. https://doi.org/10.1016/j.jclepro.2017.09.177.

Ren, J., Dubois, D. J., Choffnes, D., Mandalari, A. M., Kolcun, R., & Haddadi, H. (2019). Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach. In R. Beverly & P. Gill (Eds.), *IMC '19: Proceedings of the Internet Measurement Conference* (pp. 267-279). New York: Association for Computing Machinery. https://doi.org/10.1145/3355369.3355577.

Burton, S., Tanczer, L., Vasudevan, S., Hailes, S., & Carr, M. (2021). The UK Code of Practice for Consumer IoT Security: where we are and what next. London: The PETRAS National Centre of Excellence for IoT Systems Cybersecurity. http://dx.doi.org/10.14324/000.rp.10117734.

Shen, N., Bernier, T., Sequeira, L., Strauss, J., Silver, M. P., Carter-Langford, A., & Wiljer, D. (2019). Understanding the patient privacy perspective on health information exchange: A systematic review. *International Journal of Medical Informatics, 125,* 1-12. https://doi.org/10.1016/j.ijmedinf.2019.01.014.

Tjoa, E., & Guan, C. (2021). A Survey on Explainable Artificial Intelligence (XAI): Toward Medical XAI. *IEEE Transactions on Neural Networks and Learning Systems, 32*(11), 4793-4813. https://doi.org/10.1109/tnnls.2020.3027314.

Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law and Security Review, 34*(3), 436–449. https://doi.org/10.1016/j.clsr.2018.02.002.

Zanella, A., Mason, F., Pluchino, P., Cisotto, G., Orso, V., & Gamberini, L. (2020). Internet of things for elderly and fragile people. *arXiv:2006.05709.* https://doi.org/10.48550/arXiv.2006.05709.