



**Title of project:** Trust in Home: Rethinking Interface Design in IoT (THRIDI<sup>1</sup>)

**Associate/Partner Organisation(s):**

**Brunel University**

Cigdem Sengul – Department of Computer Science

[cigdem.sengul@brunel.ac.uk](mailto:cigdem.sengul@brunel.ac.uk)

Arthi Manohar - Department of Design

[arthi.manohar@brunel.ac.uk](mailto:arthi.manohar@brunel.ac.uk)

**University of Nottingham**

Jiahong Chen (Research Fellow) – Horizon Digital Economy Research

[Jiahong.Chen@nottingham.ac.uk](mailto:Jiahong.Chen@nottingham.ac.uk)

**Project Start Date:** 01.05.2020

**Project End Date:** 31.03.2021

<sup>1</sup> The Norse God of Knowledge



## 1. Overview

The “THRIDI” virtual two-day interdisciplinary design workshop was run on November 19-20, 2020. Out of 35 applications received, 27 were invited to attend from a wide range of institutions and organisations. Twenty-four invitees, including three expert speakers, attended the workshop and included a mix of experts from academia and early-career researchers, specialising in IoT, network security, privacy-enhancing technologies, user-interface design, law, and policy.

## 2. Workshop Objectives

The THRIDI project aims to bring together an interdisciplinary group of researchers to foster collaboration within an interdisciplinary community in the area of user-friendly interfaces for IoT in smart home settings.

Designing user-friendly interfaces are crucial to maintaining user privacy in smart home settings. A well-known legibility challenge is the lack of appropriate interfaces for users to see the extent and the nature of the data collected (Amazon Ring doorbells<sup>2</sup>). User agency is also hard to achieve when different users share devices 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 in time (e.g., changing needs for care in a smart home designed for healthcare scenarios<sup>3</sup>).

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

	<b>Legibility</b>	<b>Agency</b>	<b>Negotiability</b>
Dynamic environment	Ensuring a clear presentation of contextual factors and how they change, 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 during set-up (e.g., long privacy policies not read by the user)	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
The multiplicity of people affected	Presenting information on situations when multiple people affect or are affected by data sharing (still safeguarding their privacy)	Ensuring control of data sharing, especially handling different personal relationships, e.g., carer and the person under care in a smart home setting.	Ensuring user preferences are in line with relationship dynamics (e.g., housemates leaving and hence, have no more access to home dashboards)
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

<sup>2</sup> <https://www.bbc.co.uk/news/technology-51709247>

<sup>3</sup> <https://www.imperial.ac.uk/news/190934/20m-centre-enable-people-with-dementia/>

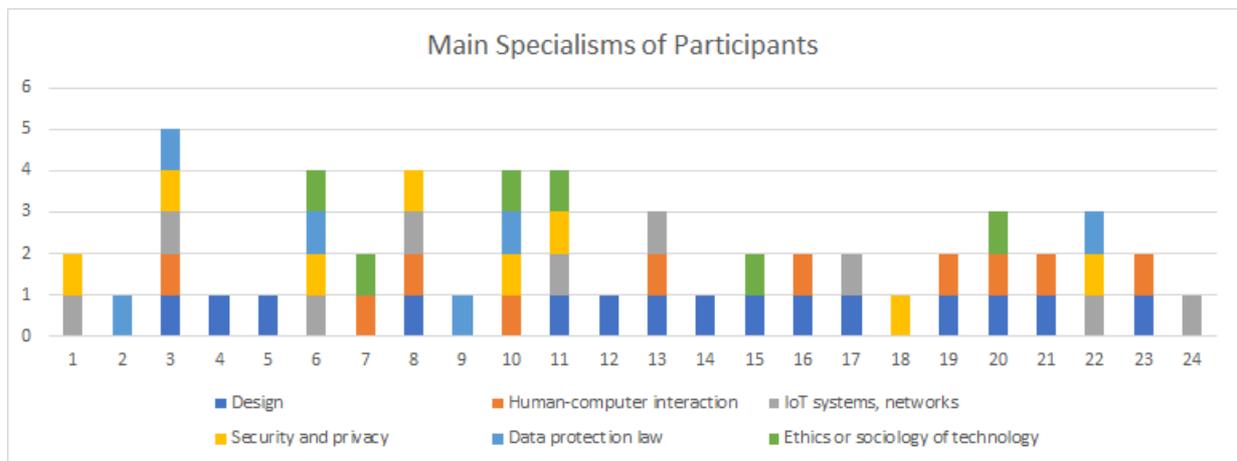


### 3. Participation

A call for Expressions of Interest was publicised on the project website, and attendees were selected from submissions made. The call form can be found [here](#).

Selection aimed to balance participation from academia and industry, representation of different research areas, career stage, strategic awareness and emphasised multidisciplinary. 50% of the participants identified as female, and 33.3% identified as male.

	Applicants	Selected
Career stage (self-determined)	74.4% Early-career 25.6% Established	79.2% Early-career 20.8% Established



A complete list of attendees and their affiliations is available in Annex 7.a.

### 4. Workshop Structure

Due to the Covid\_19 restrictions, our initial plans to run a physical workshop with ECRs had to be scrapped. Instead, we revised our project plan to run online workshops across two days and got ethical approval through Brunel University London.



## Design Workshop

Legibility, agency and negotiability in the context of four use-cases against the challenges of differences in technical knowledge, constantly changing homes, privacy fatigue, and shared ownership





The workshop focused on four use-cases. 1) Home security, 2) Smart appliances, 3) Smart health and 4) Smart toys. We have planned but not run the use-case Smart Entertainment due to the change in the number of participants on the workshop days and participant interests.

We chose Zoom and Miro as the online platforms to conduct the workshops. One of the main reasons for choosing Zoom was its ‘breakout room’ feature, which helped split the groups into four rooms, one for each use-case. Miro was used as an online whiteboard collaborative platform, where workshop activities were pre-designed and facilitated for each use-case.

The workshop agenda, Participant Information and Consent Forms were provided to the participants before the workshop. An introductory presentation was provided to highlight the purpose of the day and how to use Miro.

**Expert Talks**

The workshop started with expert talks given by Professor Abigail Durrant (Newcastle University), Dr Lachlan Urquhart (University of Edinburgh), and Dr Poonam Yadav (University of York). The speaker bios can be found in Appendix 7.b.

The speakers presented their work highlighting the different viewpoints from Human-Computer Interaction, Law and Networked Systems. Professor Abigail Durrant gave a talk on “Co-creative Research on IoT with Children”. Dr Lachlan Urquhart presented “Regulating and Designing Future Smart Buildings”. Dr Poonam Yadav’s talk focused on “A step towards building resilient, robust and trustable IoT”.

The panel session with the experts revolved around several challenges faced when designing IoT systems, including the differences between children and adults in their interaction with IoT devices; legal requirements such as transparency and consent when a building is shared by multiple occupants; designing for offline use of IoT devices to increase resilience to network outages, malfunctions, security incidents.

**Design Workshop Activities**

We have run the following workshop activities on the two-days:

<b>Ice breaker activity</b>	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: <i>What skills do you bring to the group discussion?</i> <i>What are you expecting to gain from the two-day workshop?</i> These responses helped the facilitators 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.
<b>Legibility: Reflection and SWOT Analysis</b>	Facilitators carefully selected nine images for each use case to reflect activities closely related 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 wish they knew or understood about them. The discussions were captured on post-its via their respective Miro boards and later grouped through SWOT analysis.
<b>Agency: Card Sorting Activity</b>	The Card sorting activity consisted of two parts. In the first part, the participants were shown ten images representing Privacy, e.g. Padlock, Bedroom, Living Room, Wallet. In the second part, participants were shown ten images that were more generic and represented metaphors. The images were inspired by the New Metaphor toolkit ( <a href="https://newmetaphors.com/">https://newmetaphors.com/</a> ), e.g., images of clouds, tinted window, adapters, ladder. Participants had 30 minutes to complete this session. The outcome would reflect how the participants categorised the cards from 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.
<b>Agency: Scenario cards</b>	The scenario cards consist of two distinct scenarios drafted specifically for 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 to 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.
<b>Negotiability: Design Fiction and a Role-playing activity</b>	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, the team chose one of the stories, and participants were asked to choose different roles to put themselves in an imaginary situation as various stakeholders to discuss the chosen story.

## 5. Workshop Results

### a. Legibility

As a result of the reflection and SWOT analysis, the key points raised varied according to the use-case, which we summarise below.

Discussions focused on transparency challenges and alternative approaches to address the lack of genuine legibility to users for typical smart devices. The participants questioned how useful the “smart” devices were, e.g. for conventional appliances (e.g. fridge, vacuum cleaner); one theme especially salient was the over-promise around the features that required connectivity and whether they were indeed needed.

	Home security	Smart appliances	Smart Health	Smart Toys
<b>Like</b>		<b>Simplifying daily routines</b> with smart devices, e.g. such as grocery shopping	The <b>convenience</b> of smart technologies provide their users  <b>Technologies for good</b> (altruism), applying  <b>Behavioural effects</b> of wearable products, e.g. encouraging a routine and establishing long term patterns among users.	Immersion of children in technology from a very young age and the need to <b>educate the next generation as technology makers</b> and not only consumers.
<b>Wished it were different</b>	<b>Lack of aesthetics in device design;</b> discussions <b>security risks</b> the devices might pose.  <b>Problems with data privacy in private spaces</b> like bedrooms.  <b>Lack of design considerations</b> that could help bring trust to the users, such as	<b>No clear added-value</b> from “smart” devices, and sometimes “smart” is simply a marketing trick to monetise data  <b>Complex privacy policies/warnings/updates;</b> ignored by users	<b>Information overload,</b> especially when designing for elderly users.  <b>Accuracy of measurement data,</b> e.g., sleeping data, is hard to quantify. Potential non-intrusive ways were discussed as possible solutions.  <b>Concerns around the poor design</b> when possibly devices being hacked for malicious activities.	The <b>hidden” smart features</b> of devices used for toys. The features of a smart toy that make it a ‘toy’? How is this toy still a toy when it is not connected to the internet?  <b>Sensitive data collection</b> that could go beyond the objectives set in the original label



	transparency and legibility.			
<b>Wonder how it can be</b>	<p><b>Alternative uses</b> for home security and surveillance devices from monitoring plants to setting curfews for the family's teenage members.</p> <p><b>Usability of facial recognition in a pandemic</b> (e.g. people with face masks).</p>	<b>Physicalisation of data use</b> (making data flows more tangible through appropriate visualisation) to help retain privacy	The importance of <b>digital literacy</b> and making devices user friendly for elderly users.	<b>Age-appropriate privacy policies</b> for the devices to be used by children

**b. Agency**

The card-sorting activities in this session served to understand and discuss how each participant approaches privacy, primarily in terms of agency, and was used to exchange and converge to a common language when describing privacy and its challenges. The themes that emerged included the importance of standards, the transience of footprints, public and private personas, demarcation lines between private and public spaces.

**Card Sorting from Most Private to Least Private; from Most Important to Least Important**



**Results**

During the card sorting activity, interesting similarities and differences emerged (see Tables). Images of *Bedroom*, *Bathroom* and *Wallet* were commonly seen as most private, café and public square as the least private spaces. Wallets were seen as an agency with more privacy, especially “very few people having access to data spending, for example”. *Window*, *Living Room*, *Door* and *Wall* were most commonly sorted as semi-private. *Window* and *Door* were viewed as a semi-private element that brings a certain level of control to the user “window/door of own space / own interior - depending on how visible it is”.



	Participants															
	HS 1	HS 2	HS 3	HS 4	SA 1	SA 2	SA 3	SA 4	SH 1	SH 2	SH 3	ST 1	ST 2	ST 3	ST 4	
Bathroom	9	10	8	9	10	10	10	9	10	5	10	10	9	10	10	
Bedroom	10	9	9	8	8	8	6	10	9	6	9	9	10	9	9	
Wallet	7	8	10	6	9	9	9	7	3	7	8	8	3	8	8	
Living room	8	3	7	7	5	7	5	8	8	2	6	7	8	7	7	
Window	3	6	5	4	7	6	8	4	7	9	4	2	7	6	5	
Padlock	4	5	3	10	3	4	4	6	5	8	7	4	4	3	6	
Door	6	7	4	5	4	5	3	3	4	10	3	3	6	4	4	
Wall	5	1	6	3	6	2	7	5	6	4	5	5	5	5	1	
Café	2	4	2	2	2	3	2	2	2	1	2	1	2	2	3	
Public square	1	2	1	1	1	1	1	1	1	1	1	6	1	1	2	

Participant ranking of the Cards from Most Private (10) to Least Private (1). HS (Home Security), SA (Smart Appliances), SH(Smart Health), ST(Smart Toys)

However, there were also interesting deviations, e.g. *Padlock* or *Door* seen as most private, or *Bathroom* and *Bedroom* considered semi-private by some participants. These interesting inconsistencies revealed how certain symbols might carry very different connotations for different people, and the public/private concepts can be highly situational. The expected behaviour and 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. Some participants viewed *Bedroom* as least private or semi-private, considering the number of digital technologies surrounding us; participants viewed the space as digitally well-connected.

	HS1	HS2	HS3	HS4	SA1	SA2	SA3	SA4	SH1	SH2	SH3	ST1	ST2	ST3	ST4
Different perspectives	6	7	10	9	9	7	5	6	8		10	5	10	10	4
Balancing Act	9	9	9	8	4	9	8	8	1	9	3	10	3	7	8
Signpost	2	8	6	4	8	8	7	2	5	10	8	6	9	9	9
Nest	8	5	1	10	10	6	9	9	10		7	7	5	5	6
Footprints	1	10	8	6	5	1	10	10	4	7	9	3	8	2	10
Clouds	10	6	3	1	1	10	1	7	9		1	4	7	3	7
Window	3	2	2	7	7	5	6	1	7		5	8	2	8	3
Bridge	4	3	5	5	3	4	3	3	3		6	1	6	6	5
Ladder	7	1	7	3	2	2	4	4	2	8	2	2	4	4	2
Adaptors	5	4	4	2	6	3	2	5	6		4	9	1	1	1

Participant ranking of the Cards from Most Important (10) to Least Important (1). HS (Home Security), SA (Smart Appliances), SH(Smart Health), ST(Smart Toys)

For the second set of cards, there were fewer similarities in how participants sorted the cards. Participants had a different interpretation of the images as they were meant to be abstract.

- *The Different Perspective* card was recognised as most important by some participants, reinforcing the importance of bringing perspectives from different stakeholders' views and needs when designing smart home security technologies. One participant commented: "[Maybe if ] we can just see the different perspectives, then maybe we can just overcome lots of things."
- *Balancing Act* was highly ranked, indicating the challenges in managing expectations and how the users manage different aspects of life and platforms.



- The *Signpost* card got mixed responses, as the affordance of a signpost can be temporally backwards-looking (indicating the way one has gone) or forward-looking (indicating the way ahead). For some, it was seen as the most important “signposting - most important - in terms of giving direction/guidance to users”.
- There were contradicting views on the *Nest* card, which was understood by some as future-proofing the technologies and others as indicating the complexity of the technology itself, bringing conversations on transparency.
- When interpreted as digital footprints, *the Footprints card* was seen as most important by some participants, bringing conversations on privacy and the data shared through the devices (both passive and active). A participant commented: “You should always minimise data collection. All problems start when you start to collect data. So, the least footprints you have the better in technology”, while for others, “the footprints are temporary because, at the end of the day, the environment will eliminate them.”
- The *Ladder* card was seen as unimportant by most participants; still, it was interpreted as an element or feature to help move forward or help grow.
- While the *Adaptors* card was generally considered not important, however, for one participant, it meant standards: “Without standards, we can be nowhere. We have to have some standards. So, it is very important for me”. While others questioned the utility of standards: “I agree that you rely on standards, but again as just we are witnessing today in this exercise, we are going to have different standards. We are not going to have a single standard.”

### Scenario Discussions

Following the previous activity, the groups considered two scenarios per use-case at each group.

**Home Security:** The scenarios created in the Home Security group include (i) exploring the complications of privacy implication on home security installed in a shared household, especially when third non-consented parties are involved, and ii) exploring security risks posed by domestic abuse within smart technologies. The scenarios prompted an interesting discussion around:

- How to incorporate better UI design to provide more democratic access to household members?
- Can transparency play a role in making stakeholders, including the third parties, aware of the data collected?
- How better to incorporate transparency and accountability so the devices are not used for malicious purposes such as domestic abuse?
- How can better services be designed around such devices to avoid domestic abuse within smart technologies?

**Smart Appliances:** Two smart appliance-specific scenarios included (i) two teenagers’ attempt to get drinks by tricking the smart speaker backfires and (ii) a smart vacuum cleaner used to monitor family members. Participants explored how smart technologies may both reflect and redefine domestic relationships and identities.

- The differences among households may pose severe challenges to the design of appropriate interactions with different family members, as well as to the efforts in improving digital literacy.
- The concepts of autonomy and control in the context of smart appliances may vary across households, generations, and cultures.
- Legal, regulatory, and educational questions may arise when it is unclear what the social norms are in terms of acceptable behaviour interacting with smart devices.

**Smart Health:** The smart health group explored (i) ethical implications of installing smart devices in care homes and ii) exploring privacy and ethical implications on targeted advertisements based on data shared on mental health apps. The scenarios prompted an interesting discussion around:

- How to take into account users’ mental capacity to make decisions on health data and the potential ethical impact.
- How to design better control features that could be shared across necessary stakeholders and users with limited mental capacity.
- How to take into account and avoid information overload to users, especially when sharing health data to avoid unnecessary stress.
- Can the devices potentially take into account the data management system and make the process transparent to address the system’s complexity?



**Smart Toys:** The scenarios considered two situations that involved a young child, parents, caregivers from the family, and a nanny. The smart toy capabilities changed in each scenario: (i) the smart toy that can record audio and video, and (ii) the smart toy can also perform emotion detection. The participants were asked the agency of different parties, e.g., parents, children, other family members like grandparents, and nannies, when the toy is recording and profiling based on the records. The scenarios prompted several interesting discussions on the following topics.

- Default privacy settings and their transparency on toys;
- The implications of local data storage versus cloud storage when collecting personal data at home;
- Who takes the data controller and data processor roles in home scenarios, especially when the toy is self-managed or a third-party managed product;
- Concerns around consent and profiling, specifically, algorithmic discrimination based on collected and analysed data. One participant commented: “People, like the carers, the grandparents are the part of the family, but there could be visitors in the house with different relationships to the family. At least you would want to know that there is a device that is recording...”

**c. Negotiability**

The negotiability session revolved around a design fiction activity. The participants thought about the future of Smart Homes and how they see a utopian vision of the chosen use-case (e.g. Smart Toys) is going to look like in 2050. Participants came together to vote on the scenario they would like to discuss in the following role-playing activity. The participants assumed the roles of a lawyer/ a legal tech expert, a government, a designer, a technologist, or the end-user.

<b>Smart appliances</b>	<b>Home Security</b>	<b>Smart Health</b>	<b>Smart Toys</b>
A holographic figure accidentally saving a suicidal man	A future where you can leave your homes open without having to lock	<b>Using Aromachology to treat dementia patients and also mental health issues</b>	A retro IoT toy found in the garage in 2050, when re-connected to the internet, wreaks havoc leading to stolen identities
<b>A man struggling to adapt to the smart society after a 30-year coma</b>	Super smart homes run on algorithms has now decided to bring and impose their own rules on communities	Intuitive medical products that would reduce the contact time between health experts	A toy connecting to other devices without the owner’s knowledge and acts as a producer company’s space in another nation-state
Smart kitchens promoting the preparation of healthy food	<b>A future where a robot becomes a CEO and is held accountable for failing to comply with regulations on security systems</b>	A future where an intuitive digital twin exists for better health care services	A doll taken over by a cybercriminal used to manipulate a minor
An innocent grandpa arrested after being misidentified as a burglar by a smart speaker	A future where physical homes are redundant and virtual reality is all one need to live a better lifestyle		<b>A robot nanny that can track a child’s physical and emotional development and help parents by taking over certain tasks (e.g., reading a storybook).</b>

(Chosen story in bold)



	Smart Appliances	Home Security	Smart Health	Smart Toys
<b>Designer</b>	How the <b>public acceptance</b> of the technologies and <b>governmental oversight</b> would be crucial.	<b>Better communication and understanding</b> between designers and technologists. Better design to <b>personalise</b> the products.	<b>Better connectedness and interoperability</b>	The focus is on the tactile interface but not so much on the <b>data design</b> . This should change.
<b>Technologist</b>	Smart technologies designed to facilitate users may end up <b>burdening users</b> with the management of those technologies.	Playing devil's advocate: <b>users should be more vigilant</b> about the products and privacy <b>a user issue?</b>		Playing devil's advocate: We try to do our best. We add <b>lots of protections already</b> .
<b>User with privacy concerns</b>	How may <b>marginalised groups</b> suffer from the lack of support or options of "non-smart" technologies?	Using <b>co-design</b> to empower the users in the design process while holding the governments and regulations accountable.	The <b>accuracy</b> of the data shared and the possible decisions made from the 'inaccurate' data. What are the possible ways to overcome this?	As more and more <b>valuable data stored at home</b> , how will we be able to protect ourselves in the future
<b>User with fewer privacy concerns</b>	The possibility that certain technologies may become <b>mandatory for everyone</b> in the future.		The safety with <b>vulnerable user groups</b> (i.e. elderly) and ethical implications of the data collected and stored.	
<b>Lawyer/legal tech expert</b>		Giving <b>better transparency and understanding</b> to the user. Technologists have a responsibility to provide better information on the product.		Lawyers should <b>cooperate with designers</b> to ensure that they take into account legal considerations (data minimisation, data protection by default, consent)
<b>Government Regulator</b>	How the authority may show <b>apprehension</b> towards corporate powers possessed by tech giants but at the same time may be tempted to utilise such technologies to exert <b>control</b> ;	The need to bring <b>objective actors</b> into the decision-making process such as academics and think tanks "to provide a path to utopian future."	The governments' <b>responsibility</b> to make sure an inclusive approach is practised and everyone's voice is heard in the process	Concerns around the <b>global value chains</b> , who is controlling what, who is processing what. A <b>regulatory sandbox</b> for smart toys needed.



iv. **Discussion on Open Challenges**

This session was an opportunity to do some horizon scanning. Delegates formed small groups and were asked to identify what they thought were the main challenges. Each group then presented an elevator pitch on each of their identified key challenges to all workshop attendees.

One of the topics was “Unburdening users from the overload of information and consent”, intending to redesign communication in the IoT devices in a more responsible way. The group presented their idea through a metaphorical image of the ethical pendulum by potentially applying different levels of control by empowering the users. While the group identified personalisation as a potential solution, they argued there is “no one size fits all”. Another idea was expanding on a “regulatory sandbox” and brainstorming for its potential for crossing borders and general feasibility.

v. **End of the Workshop and Feedback**

The workshop participants all received a voucher for the time they have allocated to this 2-day workshop. A feedback form was shared with the participants. The responses from 10 participants (Appendix 7.c) show overall high satisfaction with the organisation, expert talks and use-cases.

Participants commented:

“I want to thank you for a wonderful and stimulating workshop which has given new insights into the field of IoT. It is definitely helpful, especially to include it in my PhD as I am a PhD Aspirant. Thank you indeed for your generosity in organising with tremendous efforts, team coordination and time with knowledge-full workshop, and also for the gift voucher.”

“I really enjoyed the workshop. It was conducted in an engaging way. There were many opportunities to learn and to meet other researchers. The activities were both fun and made you reflect on serious issues. I think that the workshop was very well organised. Miro was a useful tool, easy to use. My group’s moderator (smart toys) was great, listened and engaged with everyone’s ideas, was patient and provided useful information throughout the workshop as well as made interesting remarks herself.”

**6. Conclusions**

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.

One of the aims of THRIDI was to foster community discussion and collaboration among a multidisciplinary group of experts and early-career researchers in a design workshop. There was a strong sense of collegiality and lively discussions throughout the workshop, where interesting themes emerged for further research and exploration.

**Further Reading**

1. Chen, J., Edwards, L., Urquhart, L. and 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), pp.279-293.
2. McStay, A. (2019) Emotional AI and EdTech: Serving the Public Good, *Learning Media & Technology*, <https://www.tandfonline.com/doi/full/10.1080/17439884.2020.1686016>
3. Mortier, R, Haddadi, H, Henderson, T, McAuley, D & Crowcroft, J 2013, Challenges & Opportunities in Human-Data Interaction. in *Proceedings of DE2013: Open Digital - The Fourth Annual Digital Economy All Hands Meeting*.
4. Sengul, C., 2017. Privacy, consent and authorization in IoT. In: *20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*. IEEE, pp.319-321.
5. Urquhart, L. and Craigon, P., 2021. The Moral-IT Deck: a tool for ethics by design. *Journal of Responsible Innovation*, pp.1-33.
6. Victorelli, E., Dos Reis, J., Hornung, H. and Prado, A., 2020. Understanding human-data interaction: Literature review and recommendations for design. *International Journal of Human-Computer Studies*, 134, pp.13-32.



## Appendices

### a. Full participant listing

<b>Name</b>	<b>Institution</b>
Abigail Durrant	Newcastle University, UK
Lachlan Urquhart	University of Edinburgh, UK
Poonam Yadav	University of York, UK
Sameh Zakhary	University of Nottingham, UK
Nevena Balezdrova	Brunel University London, UK
Damla Kilic	University of Nottingham, UK
Israel Cedillo Lazcano	Universidad Las Americas Puebla, Mexico
Shruthi Venkat	Slow Studio, India
Stanislaw Piasecki	University of Nottingham, UK
Leigh Clark	Swansea University, UK
Guido Noto La Diega	University of Stirling, UK
Sarah Turner	University of Kent, UK
Nandita Pattnaik	University of Kent, UK
Gubing Wang	TU Delft, Netherlands
Luis Soares	University of Edinburgh, UK
Kuntal Shah	Oxford Brookes University, UK
Isabel Prochner	Syracuse University, USA
Cecilia Lee	Royal College of Art, UK
Sukanta Majumdar	School of Planning and Architecture, Bhopal, India
Farid Vayani	University of Nottingham, UK
Heekyoung Jung	University of Cincinnati, USA
Nils Ehrenberg	Aalto University, Finland
Tracy Ross	Loughborough University, UK
Yang Lu	University of Kent, UK



**b. Speaker Bios**

***Prof. Abigail Durrant***

I am an interaction design practitioner and researcher, predominantly working in the field of Human-Computer Interaction (HCI), at Open Lab, Newcastle University: <https://openlab.ncl.ac.uk/>.

My research addresses the significant design challenges that we face for managing identity in our everyday interactions with digital technologies and personal data. I have explored trusted data sharing and the digital representation of individuals and communities in different contexts, including the home and within family relationships, neighbourhoods, and local community settings. I have a longstanding interest in design research methods for interdisciplinary projects ([www.abigaildurrant.com/](http://www.abigaildurrant.com/)) and am a steering committee member for Research through Design (RTD) Conference: [www.researchthroughdesign.org](http://www.researchthroughdesign.org).

I am currently Principal Investigator for the EPSRC-funded project 'INTUIT: Interaction Design for Trusted Sharing of Personal Health Data to Live Well with HIV': <https://intuitproject.org/>. INTUIT explores issues of trust, identity and privacy that are experienced by people living with HIV when sharing self-generated data with clinicians, peers, and others, for the purposes of self-managing their condition. I am also a Co-Investigator of EPSRC Playing Out with IoT, exploring how the Internet of Things (IoT) technologies can be developed to support children under 9 years old to create free play outside in their neighbourhoods: <http://playingout.digital/>. I am Co-Director of the new EPSRC Centre for Digital Citizens launching Autumn 2020 ([EP/T022582/1](https://www.epsc.gov.uk/ep/t022582/1)).

***Dr Lachlan Urquhart***

Lachlan Urquhart is a Lecturer in Technology Law at the University of Edinburgh and Visiting Researcher at Horizon, University of Nottingham. He has a multidisciplinary background in computer science (PhD) and law (LL.B; LL.M). His main research interests are in human-computer interaction, ubiquitous computing, data protection and cybersecurity. He has won over £2m in grants from funding bodies, including EPSRC, ESRC, AHRC, Universitas 21, Impact Accelerator Funds, and Research Priority Funds. For recent publications and project activities, see here.

***Dr Poonam Yadav***

Dr Yadav is currently a Lecturer (~Assistant Professor) in the Computer Science Department at the University of York, UK, and a visiting research fellow at Computer Lab, Cambridge University. Her research is focused on making the Internet of Things (IoT) and edge computing-based distributed systems resilient, reliable, and robust. Dr Yadav is an active reviewer of many top-tier ACM/IEEE IoT and networking conferences and journals. Dr Yadav leads ACM-W UK professional chapter and is featured as "People of ACM Europe" and among the top ten N2Women Rising Star in Computer networking and communications in 2020.

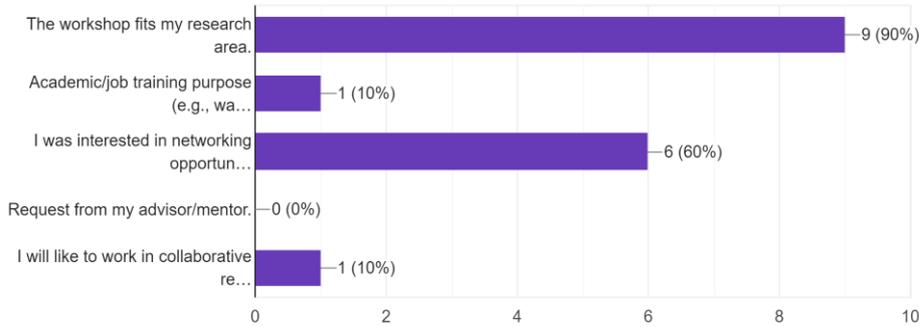


**c. Feedback**

Results of the [participant survey](#).

What caused you to come to the workshop?

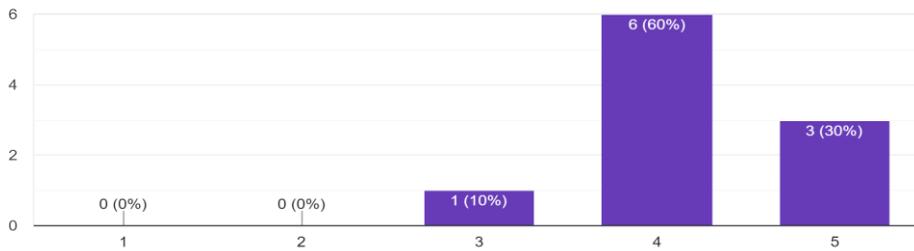
10 responses



Please rate each of the following area using the following scale (1=lowest 5=highest)

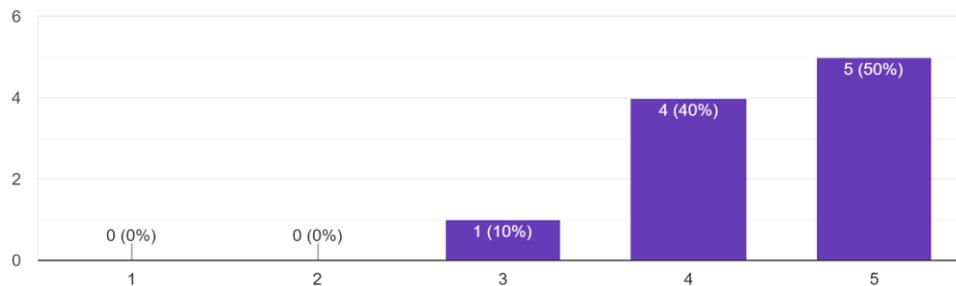
Expert talks and panel

10 responses



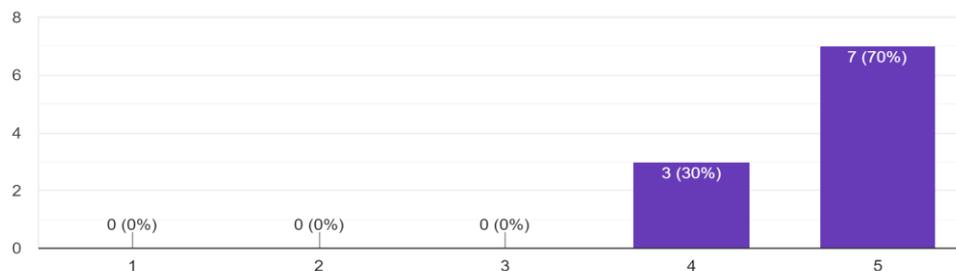
Use-case areas covered in the workshop

10 responses



Discussion opportunities in breakout rooms and activities

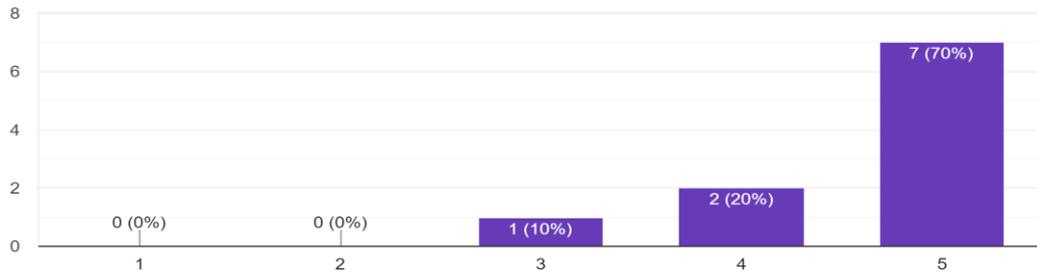
10 responses





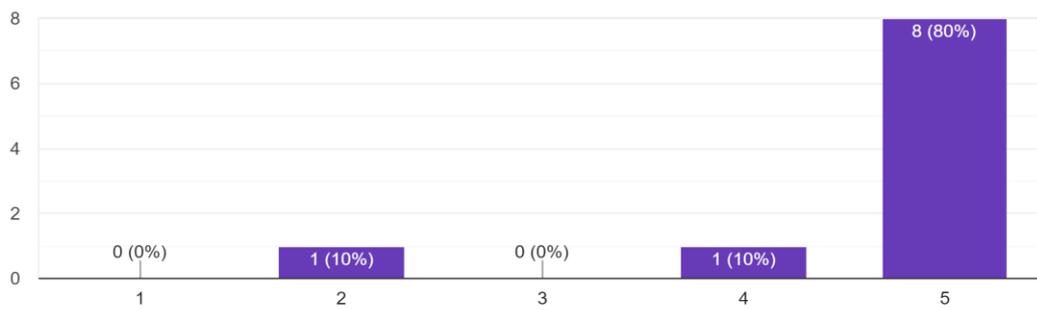
Format of the workshop

10 responses



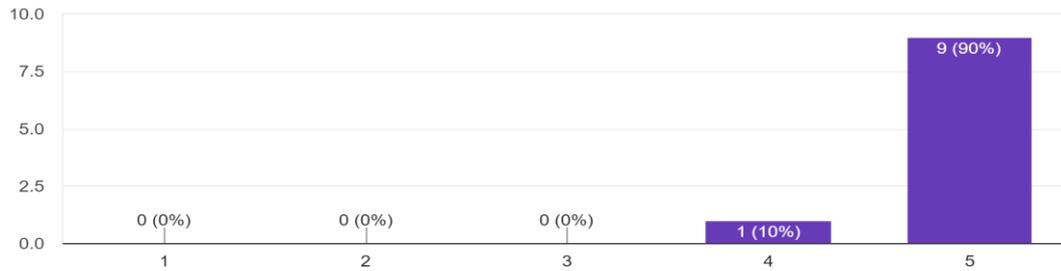
Tools used for online collaboration (e.g., Zoom, Miro)

10 responses



Moderators handling of virtual tables

10 responses



Participant engagement in breakout rooms and activities

10 responses

