Contents lists available at ScienceDirect

International Journal of Human - Computer Studies

journal homepage: www.elsevier.com/locate/ijhcs

Useful shortcuts: Using design heuristics for consent and permission in smart home devices

George Chalhoub [a,b,*], Martin J. Kraemer [b], Ivan Flechais [b]

[a] Department of Computer Science, University College London, London, WC1E 6BT, UK
[b] Department of Computer Science, University of Oxford, Oxford, OX1 3QD, UK

ARTICLE INFO

Keywords:
User experience
Design
Heuristics
Consent
Permissions
Privacy
Smart homes

ABSTRACT

Prior research in smart home privacy highlights significant issues with how users understand, permit, and consent to data use. Some of the underlying issues point to unclear data protection regulations, lack of design principles, and dark patterns. In this paper, we explore heuristics (also called "mental shortcuts" or "rules of thumb") as a means to address security and privacy design challenges in smart homes. First, we systematically analyze an existing body of data on smart homes to derive a set of heuristics for the design of consent and permission. Second, we apply these heuristics in four participatory co-design workshops (n = 14) and report on their use. Third, we analyze the use of the heuristics through thematic analysis highlighting heuristic application, purpose, and effectiveness in successful and unsuccessful design outcomes. We conclude with a discussion of the wider challenges, opportunities, and future work for improving design practices for consent in smart homes.

1. Introduction

The design of privacy in smart home technology is not simple: the convenience and efficiency offered by smart home products requires access to a plethora of data pertaining to users' homes and private lives (Yao, 2019; Yao et al., 2019a). However, public understanding of data use, awareness of key protective strategies, or responsible approaches to privacy and data protection in the smart home are not widely established yet (Ramokapane et al., 2022; Chalhoub et al., 2021). Most smart technology requires individual users to decide on data use and access control permissions on behalf of themselves, other users, and even bystanders in or near their home environment (Yao et al., 2019b; Choe et al., 2012; Wilson et al., 2017, 2015; Williams et al., 2017). This challenging task is complicated by the multitude of different manufacturers and service providers that each operate their own data usage models, and even further exacerbated by strong cultural and contextual influences on how privacy is perceived and managed across the world (Cobb et al., 2021; Apthorpe et al., 2018; Naeini et al., 2017; Abdi et al., 2019).

If we look past the perspectives of users and bystanders to the interests of businesses and regulators, privacy and data protection problems become yet more involved (Geneiatakis et al., 2017; Morgner et al., 2020; Morgner and Benenson, 2018; Gopavaram, 2019; Hadan et al., 2019). Data protection regulation has undergone significant changes over the past years and is still evolving in the face of new technical developments, advocacy efforts, and legal rulings (Gray et al., 2021; Mohan et al., 2019; Soe et al., 2020; Shao and Oinas-Kukkonen, 2019; Allegue et al., 2019; Chaudhuri, 2016). The aim of regulation is to provide greater protection and recognition for individual data rights, define how businesses and other organizations can handle information, and impose fines for breaches (Urquhart and Chen, 2020a; Bastos et al., 2018; Keane, 2018; Veil, 2018; Sobers, 2019; Schechner and Sam, 2019; Mohan et al., 2019).

General Data Protection Regulation (GDPR) in Europe requires organizations to obtain explicit, informed, and freely given consent before collecting and processing personal data. Organizations that fail to comply can be subject to significant fines (e.g., up to 4% of their worldwide annual revenue) – heightening the urgency of obtaining consent from the customer. However, many smart home devices fail to meet these data protection requirements (e.g., collecting personal data about users without their knowledge, not providing an effective way to opt-out of data collection, making it difficult for users to exercise their right to privacy).

Given the interconnection between business models for data use, data protection regulation, and user consent for data use, designing for smart homes is not straightforward (Zeng and Roesner, 2019; Apthorpe et al., 2017; Mare et al., 2019; Brush et al., 2011). Yet it is precisely this challenge that needs to be addressed to ensure responsible and appropriate data use from smart homes (Aldrich, 2003; Associates, 2019;

[*] Corresponding author at: Department of Computer Science, University College London, London, WC1E 6BT, UK.
E-mail address: g.chalhoub@ucl.ac.uk (G. Chalhoub).

https://doi.org/10.1016/j.ijhcs.2023.103177
Received 11 January 2023; Received in revised form 10 October 2023; Accepted 23 October 2023
Available online 27 October 2023

Apthorpe et al., 2017; Zheng et al., 2018). Thus, designers for privacy in smart homes face a plethora of challenges: withdrawing consent, revoking user permissions, bystander concerns, managing the access and control of other secondary users (Oh and Lee, 2015; Bergman et al., 2018; Shirehjini and Semsar, 2017; Atzori et al., 2010).

We propose and evaluate design heuristics – "*fast and practical ways to solve problems or make decisions*" including examples such as trial and error, a rule of thumb or an educated guess – as a means to addressing challenges specific to the design of consent and permission in smart homes (e.g., ensuring user control, creating transparency, establishing clear boundaries, offering opt-in/opt-out options, developing user-friendly privacy interfaces). Unlike desktop computing, smart home applications span inter-connected physical and digital devices (Thomas et al., 2016). Since smart home devices are often used in a variety of different contexts where functionality and interactions are distributed across more than one device, designing for smart devices is not straightforward (Follett, 2014). Hence, we explore design heuristics as a means of addressing security and privacy design challenges in smart homes.

We aim to address smart home designers' challenges by deriving, applying and evaluating a series of design heuristics grounded in User eXperience (UX) principles for consent in smart homes. Our research questions are (i) **RQ1:** How can we identify design heuristics related to consent and permission in smart homes? Based on this, (ii) **RQ2:** How can heuristics facilitate the design of consent interactions in smart homes?

Consent is defined as an agreement that is typically expressed through an affirmative action, for a user to provide their personal data to a company or a service provider (Regulation, 2018). Consent provides users with the opportunity to make informed decisions about how their data and devices are used, and to ensure that their rights are being respected (Friedman et al., 2000).

Designing for consent is challenging in smart homes because different stakeholders may have different needs and concerns (e.g., users could be concerned about utility whereas bystanders could be more concerned about social dynamics) (Yao et al., 2019b). We aim to address this challenge by synthesizing different modes of consent into our heuristics and hence factor the perspectives of users, bystanders, passive users, and other stakeholders (see Section 5).

We focus on consent user experiences as they have been widely studied in the literature and consist of a clearly designed encounter, the nuances of which encompass contextual, economic, compliance and strategic business priorities (Schaffer and Lahiri, 2013; Lallemand et al., 2015; Spartz and Weber, 2016; George Chalhoub and Ivan Flechais, 2022). We make the following contributions:

- We **analyzed** 125 previous studies for security, privacy and design in smart homes and derived a design heuristics framework consisting of 32 design heuristics and a description of smart home usage models.
- We **applied** our design heuristics framework in four participatory design workshops (n = 14) where participants addressed two challenges: (i) design for consent interactions, and (ii) design of permission interactions.
- We **evaluated** the usefulness and application of our design heuristics framework with thematic analysis based on the participant's (i) level of understanding, (ii) referencing count, (iii) reception, and (iv) goals.

We summarize our key findings below:

- Design heuristics *acted* as a bridge between the principles of privacy and data protection by design and the challenge of designing consent interactions in domestic environments.
- Design heuristics *facilitated* design communication through storytelling, anecdotes and also fostered wider communications between multicultural and diverse user stakeholder groups.
- Design heuristics *facilitated* the design of permission and administration models for domestic smart technology, and were useful in designing multi-user complex permission models.

2. Data protection and smart homes

In this paper, we exclusively focus on data protection in the context of consent and permission. Data protection regulation requires that individuals give their consent and permission before their data can be collected, stored, or used; which is necessary for organizations to comply with data protection regulation. We briefly summarize key challenges for the design of data protection interactions in smart homes.

2.1. Common challenges

A plethora of human-centered research studies has reported on the challenges of informational privacy and data protection in smart homes (Schaub et al., 2015). Data Protection in the context of design is defined as an approach which ensures that privacy and data protection issues are considered at the design phase of any system, service, product or process and then throughout the lifecycle (Information Commissioner Office, 2019).

Other research shows how issues of data protection are amplified in multi-user contexts. For example, household members expect to share access and distribute responsibilities around a shared home network or any smart device (Crabtree et al., 2012; Garg and Moreno, 2019). Sharing is influenced by different personal characteristics (attitude, aptitude, competence, and skill) that might limit possibilities to accommodate for individual and shared use of devices (Kraemer et al., 2019; Hargreaves et al., 2018). Questions of power and control arise where responsibilities are shared and access needs to be managed (Levy and Schneier, 2020), and can further complicate agreements on device use (Garg and Moreno, 2019). These agreements are not necessarily made explicit and established consensually. Devices can become part and parcel of relationship dynamics that lead to disagreement and tension (Geeng and Roesner, 2019), sometimes even coercive or abusive behaviors (McKay and Miller, 2021; Freed et al., 2019; Leitão, 2019). Across different kinds of relationships, the negotiation of preferences for data collection and use by third parties is not well catered for by design (Yao et al., 2019a,b). Previous research on the UX of data protection has shown that UX stakeholders experience difficulties in designing for consent and permission in smart homes (George Chalhoub and Ivan Flechais, 2022). Key issues that amplify the complexity of the UX for data protection in smart homes can be summarized with three questions: for whom should interactions be designed, how can control between users be balanced, and how can design cater for different preferences?

2.2. Legal provisions and design

Research on recent data protection legislation reflects these challenges for UX in the home. For example, Urquhart and Chen (2020b) question whether manufacturers ought to do more to support users as 'domestic data controllers' to satisfy the GDPR accountability principle. The challenge of obtaining consent has been researched extensively (Utz et al., 2019). In a non-exhaustive list, challenges for consent pertain to questions of awareness of the need to consent, understanding of what should be consented to (informed consent), and/or the ability to exercise consent. In particular, Speed and Luger (2019) raise questions on consent given by those not actively or implicitly involved in the set-up and configuration of devices, or for situations in which interactions are not deliberate and voluntary; and consent is dynamic in that people desire to grant, amend, and revoke consent at different points in time (Chalhoub et al., 2021).

Consent works well as long as it remains remarkable and seamless. Designers need to plan for the right moment and frequency to ask for consent carefully, because routinely required consent is perceived as overwhelming and disruptive (Hartzog, 2018; Barocas and Nissenbaum, 2009; Schwartz and Ward, 2004). Moreover, users require control and insight to establish preference of an informed consent decision. Building preferences is not always readily supported by technologies, particularly so where data trading happens unbeknownst to the user (Seymour et al., 2020). However, Chalhoub et al. (2021) point out, many smart home devices are far from reaching the threshold for overburdening consent and neither are they designed to respect users' data protection rights. While consent is rather difficult to implement correctly and the concept is not undisputed, researching and implementing consent is a worthwhile effort towards empowering users given the current legal and technical frameworks.

Researchers have found the problem is systematic, although principles and patterns exist to support designers. On the one hand, dark patterns are the anti-principle of good design. They play on users' feelings, recognizing how users' actions are guided by perceptions. They might suggest that data is protected and handled appropriately when it really is not (Bösch et al., 2016; Conti and Sobiesk, 2010; Gray et al., 2018; Mathur et al., 2019). They are systematically manipulative in making it more difficult for users to formulate preferences and to act on them (Luguri and Strahilevitz, 2021). On the other hand, principles of *apparency* (Schraefel et al., 2020), *seamfulness* (Chalmers and Galani, 2004), and *mindfulness* (Cox et al., 2016) provide better framing for user-friendly design efforts. Apparency portrays the use of data visibly and intuitively. Seamfulness acknowledges limitations of a system to a user, providing greater understanding of how the system works. Mindfulness encourages designing for deliberate and intentional behavior (Cox et al., 2016). Again, empirical studies do not suggest designers have taken these principles into account when designing the UX of data protection in smart homes (Chalhoub et al., 2021).

These shortcomings show designers' struggle to appropriately engage with legislation given the complexity of user-experience in the home. Designers are often challenged to serve a number of competing interests from different stakeholders, with the requirements of laws and regulations representing only a part of them. One particular challenge is the adherence to privacy-by-design principles, as failure to comply with these principles is common (e.g., Google Home failing to provide full functionality if users should not consent to sharing their data Chalhoub et al., 2021). A narrow interpretation of the legislation, one that is focused on compliance but fails to engage with the intent of the legislation, becomes apparent. To overcome this narrow interpretation, researchers have argued for designers "to be actively engaged in the regulatory frame" such that data protection might be "embedd[ed] in UX heuristics" (Luger et al., 2015). We share the sentiment by adding that particular challenges arise around actualizing privacy-by-design principles for the design of UX for data protection in smart homes.

2.3. Opportunities for UX design

UX designers have a large toolset of approaches, methods, and techniques at their fingertips (Kuniavsky, 2010). In research and design, UX techniques have evolved over the decades from human factors, cognitive approaches, social-constructionist and even post-modern orientations (Low, 2016). UX methods differ among a few key dimensions such as who does the design work for whom, who is involved in the design process, and which design goals are to be achieved (Hartson and Pyla, 2012). Such questions are particularly important where issues of power are at stake, such as the task to design for data protection in the home (Seymour et al., 2020).

There have been a multitude of contributions applying UX tools and methods to unpack, explore, and address particular issues of data protection and privacy (Chalhoub et al., 2020a). Researchers have advocated for designers to explore the strategies the UX toolset has to offer, advocating for privacy by design researchers to use participatory, value-centered, re-design, speculative and critical design orientations to advance the debate and get a new perspective on privacy and data protection (Wong and Mulligan, 2019). Outside research, practitioners are asked to invite designers to the table when aiming to solve complex socio-technical challenges (van Oorschot et al., 2022).

However, the reality outside academia often looks very different. Sometimes UX designers might just not be involved when engineers draw up requirements for compliance with data protection (Chalhoub et al., 2020b). UX designers might be involved, but have to balance competing goals to satisfy the requirements of different stakeholders (Chalhoub et al., 2020a). Data protection can become an afterthought where business interests dominate, UX design experience is low, and there is a pressure for time (George Chalhoub and Ivan Flechais, 2022). As a result, UX designers favor techniques that are efficient, offer means to align design efforts with business needs, and help to resolve design challenges (Chalhoub et al., 2020a).

Discount usability methods meet these requirements by providing early usability input and allowing designers to efficiently adapt their proposals (Nielsen, 2009). For example, designers can use think-aloud protocols, walkthroughs, or heuristic evaluation readily and easily compared to participatory design or even ethnographic approaches. Among these approaches, design heuristics have gained some popularity for being highly efficient to individual experts, expert groups, and as a vehicle for discussions with other stakeholders (Nielsen, 1994).

2.4. Design heuristics

Design heuristics are broad rules of thumb that are not specific but provide insights to an array of problems. The most popular examples are Jacob Nielsen's 10 usability heuristics, which withstood the test of time since 1994 (Nielsen, 1994). Nielsen's heuristics are widely applied by individual experts or in group settings, e.g., judging the degree to which users can recover from mistakes following the 'user control and freedom' heuristic.

Other authors have made proposals to extend these usability heuristics to UX, for example designing to 'respect the user' (Arhippainen, 2013). Such heuristics enable UX designers to reflect on users' needs during the design process in a principled way and thereby serve as 'boundary objects' (Huvila et al., 2014) for discussions with other stakeholders (e.g., data protection experts, engineers, or product owners) (Nielsen, 2009; Chalhoub et al., 2020a).

Design heuristics have also been proposed for evaluating UX design (Arhippainen, 2013), but heuristic evaluation remains niche among UX designers and is sometimes frowned upon by UX researchers (Lallemand et al., 2014). A potential challenge with expert evaluation is that the expert UX designers are not the users, leading to a disparity between issues identified by experts and problems reported by users (Lallemand et al., 2014). UX designers might not be able to adopt the perspective of the user without involving them, and maybe even more so from a UX than UI perspective. However, UX designers might be the only 'user experts' involved, and the time they are given to advocate for and evaluate design decisions against the needs of future users might be very limited (Wong and Mulligan, 2019; Nielsen, 2009).

2.5. Summary

Previous work in the UX of data protection for smart home devices highlights common smart home consent and permission problems. Designing for the UX of consent and permission (e.g., developing user-friendly privacy interfaces, creating transparency, ensuring user control) in smart homes remains a challenge. In practice, the way UX designers engage with challenges of consent and permission is often not driven by methodological rigor and scientific curiosity. The various demands of their job require compromising for the most feasible approach, such as using heuristics to design for consent and

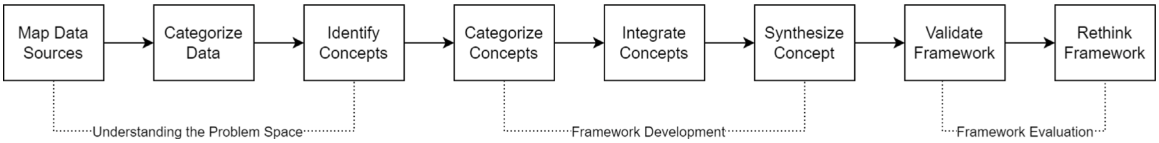


Fig. 1. Our analysis consisted of: (1) mapping the selected data sources; (2) extensive reading and categorizing of the selected data; (3) identifying and naming concepts; (4) deconstructing and categorizing the concepts; (5) integrating concepts; (6) synthesis, resynthesis, and making it all make sense; (7) validating the conceptual framework; and (8) rethinking the conceptual framework.

permission. To address this gap, we used a mixed-method approach and a substantial dataset to identify design heuristics for consent and permission in smart homes and explored how they can facilitate the design of consent interactions in smart homes.

3. Methodology

Taking into account insights from our prior work on UX and data protection in smart homes (Chalhoub and Flechais, 2020; Chalhoub et al., 2020b,a, 2021; Chalhoub, 2020; George Chalhoub and Ivan Flechais, 2022), we designed and conducted two studies to *explore design heuristics for improving on UX for data protection in smart homes*. The studies consisted of:

1. Constructing a design heuristics framework (32 heuristics and description of smart home models) using conceptual framework analysis (CFA) from 125 previous studies (see Section 4).
2. Engaging groups of UX designers, developers, security engineers, and users in four participatory design workshops (n = 14) to explore opportunities for the use of heuristics (see Section 6).
3. Analyzing the usefulness and the application of the workshop transcripts through a close-coding scheme in order to evaluate the use and application of the heuristics (See Section 8).

4. Study one: Design heuristics framework

4.1. Construction of design heuristics framework

We constructed our framework using the widely-used conceptual framework analysis (CFA) technique (Jabareen, 2009; Walker and Avant, 2005) which focuses on quantifying and tallying existing concepts (Carley, 1993). It is based on Grounded Theory (Corbin and Strauss, 2015) which is a systematic qualitative methodology that builds hypotheses and theories through collecting and analyzing data (Jabareen, 2009).

Using an eight-step procedure (see Fig. 1), we generated heuristics for the UX design of consent and permission in smart homes. We collected, read and analyzed 125 sources (see Sections 4.1.1 and 4.1.2) which included research papers, articles, books, interviews, guidelines, standards, and practices related to smart homes, design, security and privacy.

In accordance with Jabareen's CFA technique (Jabareen, 2009), we mapped data sources by identifying text types and other sources of data, such as existing empirical data and practices. We began with an extensive review of multidisciplinary texts, and consulted with practitioners, specialists, and scholars from various disciplines. We then read selected data and categorized it both by discipline and by a scale of importance. Further, we reread the selected data and discovered new concepts, resulting in a list of numerous competing concepts. We then deconstructed each concept, identified its main attributes, characteristics, assumptions, and role; and, subsequently, organized and categorized it according to its features. Moreover, we integrated and grouped concepts that have similarities before synthesizing them into a theoretical framework (the process was iterative and included repetitive synthesis/resynthesis). We provide more details about steps one (see Section 4.1.1), two (see Section 4.1.2) and three and four (see Section 4.1.3) of our analysis procedure below:

4.1.1. Map data sources

Following Morse and Mitcham (2002)'s "*fishing trip*" and "*scoping procedure*", we extracted data from previous studies, design workshops for heuristics, design heuristics, and best practices that have been developed targeting security and privacy in smart homes. We identified data sources by searching for many keywords such as "**smart homes**", "**design [guidelines, heuristics, principles, practice, ux]** ", "**consent [management, interaction, design]** ", "**security [authorization, authentication]** " and "**privacy [tracking, information]** " in Google Search and Scholar, and ACM and IEEE libraries. We collected more data by adding context-specific search terms to our original set e.g., "*dynamic consent*", "*data protection*"". We followed Morse, Janice and Richards' (Morse and Richards, 2002) data collection procedure which included holistic mapping to ensure complete data collection and validity. Data collection was an iterative process between two members of the research team, who recorded relevant search terms and frequently met to discuss data collection efforts. Our data collection process included data sources in a variety of contexts, beyond smart home contexts such as access control, websites, and software systems. To filter out our data, we used validated filters that have been tested against gold-standard sets (Jenkins, 2004). We also examined the full-texts of all data identified for inclusion from the searches. We specifically examined empirical studies for the quality of their design, and produced a narrative commentary to summarize both the included references and findings from the extracted data.

The process of gathering data and coding stopped once additional data stopped generating new insight (i.e., theoretical saturation). The resulting body of work included 125 sources which can be found in Appendix E.

4.1.2. Categorize data

To code the data sources, they focused on research questions, methodology (e.g., study design, research questions), and core contributions (e.g., study takeaways and implications) of each data source. Two research team members independently completed the initial coding of all sources: they familiarized themselves with the sources by reading them throughout, taking notes separately; then met multiple times to develop an initial codebook; then, they reviewed each others' work, discussing and resolving concerns. To verify the credibility of the codebook, a third team member cross-checked the codes against the sources. At the same time, a fourth team member reviewed the initial codes and supporting sources. All team members discussed any differences and generated a codebook of 91 codes. The team members handled cross-code analysis by looking for patterns and connections between different codes; and creating a matrix to compare and contrast the codes to identify common themes and relationships with our heuristics.

The researchers then grouped the codes into themes (axial coding) and categories (selective coding) and identified five themes: ux, design guidelines, security, privacy and home tech. After creating the final codebook, we tested for inter-rater reliability. The average Cohen's kappa coefficient (κ) was 0.82; values over 0.80 indicate almost perfect agreement (McHugh, 2012).

Table 1
Identified Concepts from Conceptual Framework Analysis.

Concept	Inquiry character	Selected sources of data
Communication	Ontological concept	Online communication studies, literature
Consent	Ontological concept	Data protection, consent management studies
Heuristics	Methodological concept	Heuristic creation, validation and evaluation studies
Knowledge	Ontological concept	Social epistemology, information science studies, literature
Privacy	Epistemological concept	Information privacy, privacy law studies
Security	Epistemological concept	Authorization, risk management, access controls studies
Permission	Ontological concept	Multi-user permission and family permission studies

4.1.3. Identify and categorize concepts

We followed Jabareen's (Jabareen, 2009) definition of 'concept' and used Corbin and Strauss (2015)'s procedure to identify, integrate, conceptualize, and theorize core concepts from designing security and privacy related technologies in smart homes. We identified seven distinct concepts by identifying their main attributes, characteristics, assumptions, and role; and, subsequently, organized and categorized them according to their ontological, epistemological, and methodological role. Table 1 summarizes the results of this phase. The concepts identified are different from the search keywords in Section 4.1.1.

The ontological inquiry challenges the nature of reality. It seeks to understand the form and nature of reality, what can be genuinely understood and accepted about it. Ontological assumptions relate to knowledge of the "way things are", "the nature of reality", "real" existence, and "real" action (Guba et al., 1994). Communication, consent and knowledge were mapped into because they relate to matters of "real" existence and "real" action.

The epistemological inquiry scrutinizes the relationship between the person seeking knowledge and what can actually be known. The established answer to the ontological inquiry limits the possible solutions to this inquiry (Guba et al., 1994). Security and privacy were mapped into epistemological assumptions because they relate to "how things really are" and "how things really work" in an assumed reality.

The methodological inquiry asks how an individual intending to acquire knowledge should proceed to determine whatever they believe can be known. Existing answers from the first two inquiries shape potential solutions to this question (Guba et al., 1994). Heuristics were mapped into the methodological inquiry because they relate to the process of building the conceptual framework and assessing what they can tell us about the "real" world.

We used these concepts to develop our framework: heuristics for communication, consent, and knowledge were derived to address security and privacy smart homes design challenges: design and permission.

5. Study one results: Design heuristics framework

In this section, we detail the results of the first study, describing the contents of our derived framework and the heuristics identified in the literature.

Our framework was aimed at participatory design environments and consisted of:

1. A description of lifestyles, process models, repurposing, reuse and usage models in smart homes.
2. A set of 32 heuristics for the design of security and privacy in smart home products.

The number of heuristics (e.g., 32) was structured in three categories: **Knowledge**, **Consent** and **Communication**. With ≈10 heuristics per category, the categories provided structure for participants to explore and understand the heuristics sufficiently. The heuristics were intended to apply specifically to the design of consent and permission interfaces in smart homes. A simplified version of our framework can be found in Fig. 2 and a detailed version in Fig. G.7.

Our framework represents interactions between devices and users. Our analysis (see Section 4.1.1) identified various modes of consent, which were synthesized into the framework. Additionally, our mapping data sources method uncovered different modes of concept during the analysis. These consent modes considered the perspectives of various stakeholders, including bystanders, non-expert household members, and passengers. These elements were synthesized and factored into our framework's construction and the modes of consent are implicit to the framework. Consequently, our framework can be used to contextualize these interactions and can be applied whenever there is a need for any user group's consent (e.g., admin/primary users, passive users, secondary users, bystanders, guests). Irrespective of whether there is a need to design for any specific user group (e.g., primary user or bystander), the framework can be effectively utilized in the same manner.

6. Study two: Participatory design workshops

6.1. Applying the framework in PD workshops

We applied our design heuristics framework in four participatory design (PD) workshops (n = 14). We gave participants two design tasks: design for (i) consent and (ii) permissions. We conducted the workshops online through Miro, a visual collaborative platform. We collected notes, pictures of any sketches (context and design solutions), and audio-recordings. Audio was shared between participants using Microsoft Teams.

6.1.1. Participatory design

Following calls from previous work addressing privacy and design challenges (Mulligan and King, 2011; Wong and Mulligan, 2019), we adopted a PD approach to evaluate our design heuristics framework. Known as the "*third space in HCI*" (Muller, 2003), PD reinforces the role of end users as stakeholders in the design process and can be instrumental in understanding their values and expertise (Muller, 2003; Wong and Mulligan, 2019). Thereby, PD invites interpretation by users and focuses more on collectivism than individualism, with a heterogeneity of perspectives becoming the norm (Muller, 2003). In electing to use PD, we intended to allow the interpersonal character of data protection in shared spaces to take center stage in our investigations, more fully exploring its contextual nature. Exploring data protection "*through the eyes of stakeholders*" (Wong and Mulligan, 2019) enables the investigation of how stakeholders absorb heuristics and apply them in design tasks.

6.1.2. Workshop procedure

We first presented our framework and heuristics to participant groups and asked them to read, understand and examine the heuristics and the framework given to them. Second, we proposed the problem scenarios to the participants and monitored how they self-organized and addressed the problem. As part of our problem scenarios, we asked participants to (i) design for consent interactions and (ii) design for permission interactions in which users would be asked to consent. Participants were asked to look into permission design as a means of trying to understand how consent should be dealt with.

In addition, we explicitly instructed our participants to use all three components of our design heuristics which included: knowledge, consent and communication. We ensured that participants understood the

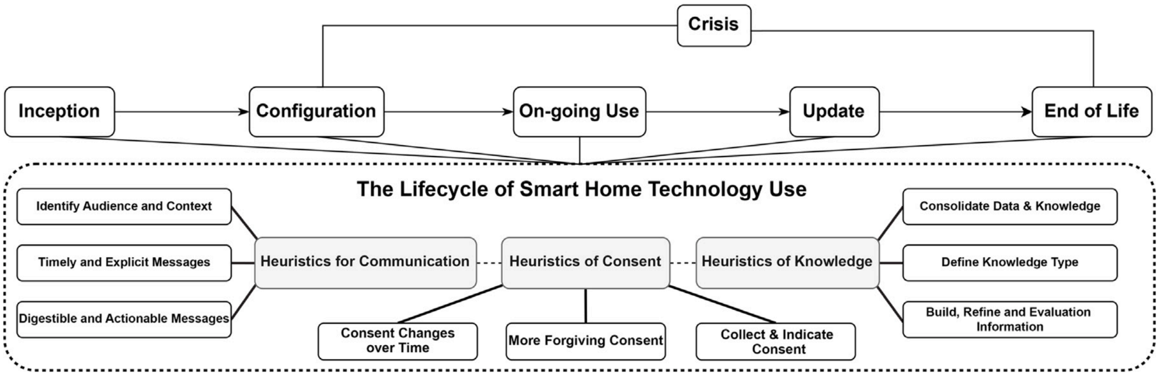

Crisis
Inception
Configuration
On-going Use
Update
End of Life
The Lifecycle of Smart Home Technology Use
Identify Audience and Context
Timely and Explicit Messages
Digestible and Actionable Messages
Heuristics for Communication
Heuristics of Consent
Heuristics of Knowledge
Consent Changes over Time
More Forgiving Consent
Collect & Indicate Consent
Consolidate Data & Knowledge
Define Knowledge Type
Build, Refine and Evaluation Information

Fig. 2. Simplified version of our Framework of Design Heuristics. The full version with heuristics can be found in Fig. G.7.

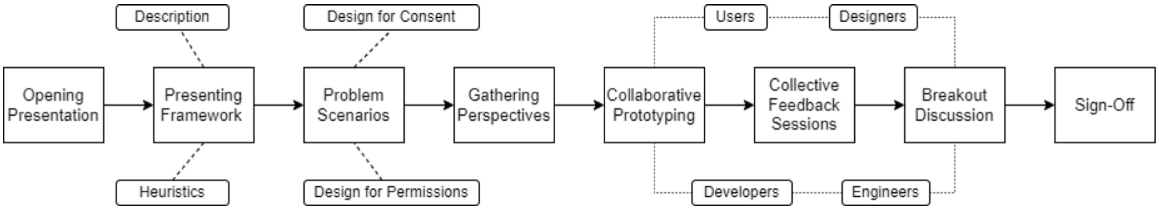


Fig. 3. Participatory Design Workshop Procedure.

Table 2
Participatory design workshop detailed procedure.

Activity	Description
Opening presentation	We briefed our participants about our workshop and procedures.
Presenting framework	We presented and explained our framework of design heuristics.
Problem scenarios	We presented one problem scenario for every participant group.
Gathering perspectives	Participants generated ideas for solutions to the problem scenario.
Collaborative prototyping	Participants brainstormed, and prototyped potential solutions.
Collecting feedback sessions	Participants reflected on the utility of the presented framework.
Breakout discussion	Participants discussed and resolved any conflicts or disagreements.
Sign-Off	We concluded our workshop and we addressed any questions.

value of and equally focused on all components during the workshop procedure.

We tightly controlled the discussion to ensure that workshop participants were accentuating the identity assigned to them. For instance, participants with the role of ‘mobile developer’ were focused on deriving mobile application prototypes whereas participants with the role of ‘security engineer’ were analyzing security problems that could have occurred.

We started gathering design ideas from participants addressing these design problems, and asked their feedback about the heuristics given to them, noting down what worked well and what did not. Third, we conducted collective feedback sessions with the participants where we collected general feedback about the workshop, focusing on the utility and the use of heuristics.

Two workshops groups were asked to (i) design for consent interactions and two were asked to (ii) design for permission interactions in which users would be asked to consent. The prompts were derived from our conceptual framework analysis which highlighted these prompts as an on-going design challenge. The authors’ understanding of the research question was informed by the feedback that they received from the participants in each session.

The heuristics were initially presented to participants using a presentation based on Collins’ recommendations for communicating effectively (Collins, 2004). The presentation included: a detailed explanation of our framework and heuristics, overview of what heuristics are and how they are used in design. Participants also had the opportunity to ask questions. Our workshop procedure is found in Fig. 3 and Table 2.

6.1.3. *Pilot study*

We conducted a pilot study of our workshop to make sure that the questions for all stakeholders could be understood and to identify any potential problems in the script (e.g., cost, time, adverse events) in advance, so that the methodology could be fine-tuned before launching into the main study. We used the common practice of convenience sampling by selecting four members of our organization to conduct a workshop for the pilot. No considerable changes were made.

6.1.4. *Participant recruitment*

To recruit our participants, we advertised our study on Twitter, Reddit, LinkedIn and Blogs. We posted flyers around University of Oxford’s buildings and emailed university staff members. We asked interested participants to complete an online pre-screening questionnaire, which 50 completed.

We aimed to recruit demographically-diverse participants who owned and used smart homes devices and were technically competent (Davidoff et al., 2006). We also wanted to ensure that participants had job roles that would be similar to their workshop role (e.g., UX designers, developers, and security experts). Hence, demographic questions about gender, age, educational level, employment status, job title and description were included. Additionally, participants were asked to describe their existing knowledge of smart products, and their interest behind wanting to participate.

All participants had technical experience with smart homes. Different levels of technical competence were defined (Novice, Competent, Expert) using a simplified Dreyfus model of skill acquisition (Dreyfus and Dreyfus, 1980). Dreyfus’ model has been widely used to define

Table 3
Demographics of our workshop participants (n = 14)

G#	P#	Age (Gender)	Race	Job role (Degree)	Workshop role	Competency
G01	P1	25–34 (M)	Asian	UX Consultant (BSc.)	UX Designer	Expert
	P2	35–44 (F)	Hispanic	Academic Admin (BSc.)	Ordinary User	Competent
	P3	18–24 (M)	White	iOS Developer (BSc.)	Mobile Developer	Expert
	P4	25–34 (F)	White	Security Analyst (BSc.)	Security Engineer	Expert
G02	P5	25–34 (M)	Afro-Arab	Hotel Receptionist (B.S.)	Ordinary User	Novice
	P6	35–44 (M)	Asian	Product Designer (B.A.)	UX Designer	Competent
	P7	25–34 (F)	White	Security Architect (B.Eng.)	Security Engineer	Expert
G03	P8	25–34 (M)	White	Marketing Coordinator (BSc.)	Ordinary User	Competent
	P9	25–34 (M)	White	Security Consultant (BSc.)	Security Engineer	Competent
	P10	35–44 (M)	Asian	Senior UX Designer (BSc.)	UX Designer	Expert
	P11	18–24 (M)	Black	Store Assistant (BSc.)	Ordinary User	Novice
G04	P12	18–24 (M)	Hispanic	Finance Assistant (BSc.)	Ordinary User	Expert
	P13	35–44 (F)	Indian	UX Director (B.A.)	UX Designer	Competent
	P14	25–34 (M)	White	iOS Engineer (BSc.)	Mobile Developer	Expert

levels for assessing one's competence (based on skill development through instruction and experience). Participants were asked to report their own skill level using the recruitment questionnaire.

Participants were later allocated workshop roles that were similar to their job description (e.g., technical, security, design background). Participants that did not have a matching job description with a workshop role were given the role of ordinary users (e.g., administrative, hospitality background).

We ensured that participants recruited for the ordinary user role had personal lived experienced smart homes (e.g., using smart cameras or doorbells at home) and participants recruited for non-ordinary user roles (e.g., UX designer, mobile developer) had professional experiences in smart homes (e.g., designing or developing smart home products).

Table 3 summarizes the demographics of our sample (n = 14). Our sample consisted of 10 male and 4 female participants. Ages ranged from 18 to 44. Ten participants had a college degree. We divided our participants (n = 14) into four workshop groups. We also categorized participants based on their workshop role: UX Designer (n = 4), Ordinary User (n = 5), Security Engineer (n = 3) and Mobile Developer (n = 2). Seven participants were experts, five were competent and two were novice.

6.1.5. Data collection and analysis

One leading team member conducted all participatory design workshops with the help of the second and third team members. The team members collected included participants' notes, pictures of any sketches (context and design solutions), and audio-recording of the workshop itself. At the beginning of each workshop session, the lead team member presented the same induction to all participants summarizing the heuristics and their use. After every session, the researchers came together to reflect on the session and adapt the approach as required. Audio recordings were transcribed verbatim by a transcription service and proof-read by the first author. Participants and groups are assigned unique identifiers, shown in Table 3 that are used throughout the paper.

The first and the third team member then inductively and thematically analyzed the transcribed recordings in accordance with Braun and Clark's thematic analysis (Braun and Clarke, 2006). An open coding approach was applied to allow themes to emerge from the data. The thematic analysis also included participants notes and any produced sketches. The themes observed from our analysis were: design perspectives in different contexts, how design goals motivated heuristics choices, how heuristics were used to address design problems and the effectiveness of heuristics to design solutions.

We triangulated between these data as presented in the results section. Some discussions and design features were driven by information we introduced deliberately. We observed data saturation (Seale, 1999; Corbin and Strauss, 2014; Guest et al., 2006) during the fourth workshop, and, hence, we stopped conducting workshops. In total, the study material analyzed consisted of 4 recorded workshops (≈1 h and 11 min per workshop), 14 participant notes, and four sketches.

6.2. Research ethics

Our study was thoroughly reviewed and approved by the University of Oxford's Central University Research Ethics Committee (CS_C1 A_021_037). Before each interview, we asked participants to read an information sheet that explained the high-level purpose of the study and outlined our data-protection practices. Participants were thanked for their time with GBP50 in electronic store vouchers. In addition, participants were reimbursed for out-of-pocket expenses related to participation, including travel, meals, accommodation, and childcare.

We also asked participants to sign a consent form that presented all the information required in Article 14 of the EU General Data Protection Regulation (GDPR). We emphasized that all data collected was treated as strictly confidential and handled in accordance with the provisions of the UK Data Protection Act 1998 (registration no.: Z6364106/2015/08/61).

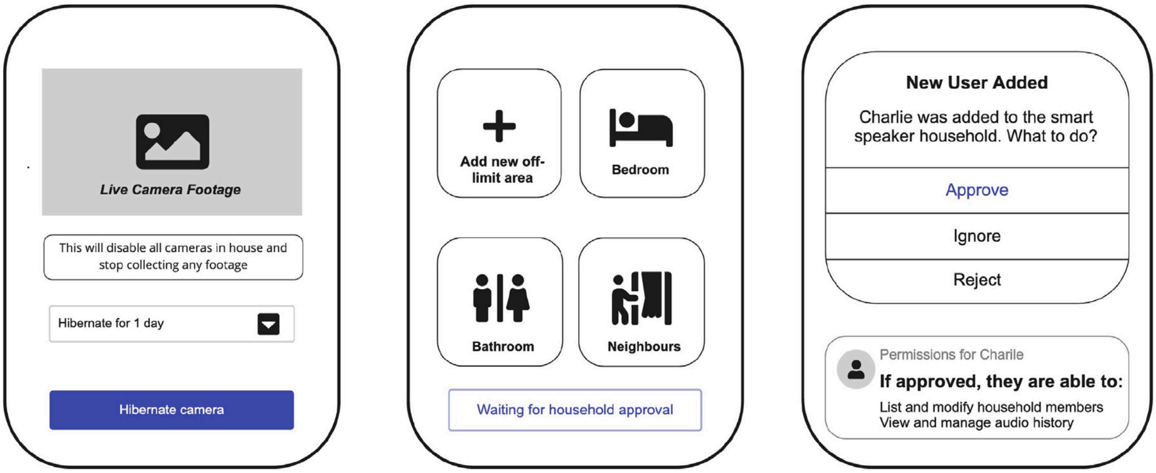
6.3. Limitations

First, the workshops uncovered useful insights into security and privacy design in smart home products, but the number of exploratory workshops (n = 4) we conducted was limited. Following recommendations from prior work, we stopped conducting workshops after observing data saturation (see Section 6.1.5).

Furthermore, our sample consisted (n = 14) solely of UK residents, but we made efforts to ensure diversity by utilizing different recruitment channels. However, the sample size was sufficient for our initial evaluation. One can argue that this limits the generalizability of our results. However, we have clearly documented our methodology and provided the data sources used for the study, as well as the protocols and procedures used for data collection; meaning that our study can be replicated with participants in different cultural contexts.

Second, given the way we presented our framework, we could not evaluate whether the description of lifecycle and reuse of our design framework were particularly helpful because the PD workshops were articulated around heuristics. To address this limitation, we performed a detailed evaluation of the heuristics which allowed us to give recommendations for future design improvements. Specifically, we used a combination of analytical modeling, empirical analysis, and user testing to assess the strengths and weaknesses of each heuristic. We then identified areas for improvement, such as making the heuristics more intuitive and easier to apply, and developed insights to guide their use.

Third, our workshop study does not have a control group, e.g., we do not provide our design exercises to a participant who does not receive our framework of design heuristics. Control groups are expected to show what happens in the absence of the framework of design heuristics. As a result, it is impossible to know whether the positive observed behaviors were really caused by the heuristics as opposed to a



This will disable all cameras in house and stop collecting any footage

Charlie was added to the smart speaker household. What to do?

If approved, they are able to:

List and modify household members
View and manage audio history

Fig. 4. Consent and permission smart homes features designed by participants using heuristics: (a) hibernate feature for smart cameras that temporarily stops cameras from collecting footage; (b) off-limits feature for smart cameras that restricts areas in the home from being recorded; and (c) permissions feature for smart speakers that requires household approval to add new members.

good workshop construction. Future work evaluating design heuristics for smart homes should consider including a control group.

Fourth, we demonstrated and evaluated a framework based on given scenarios. We also do not have data showing what users would do without the framework given the same scenarios. Nonetheless, the purpose of this study was not comparing our framework against a benchmark, but seeing how it gets used. Hence, we cannot claim that this study is better than other user centered design approaches (user testing, card sorting, personas, usability testing, focus groups, expert interviews). This is because our study only looked at a single type of user interface (our results may not apply to other types of user interfaces). In addition, our study only involved a small number of users.

However, due to our mixed-method approach and the use of a substantial dataset, we can use the results of this study to suggest that the framework of design heuristics is fit for purpose (e.g., suitable or appropriate for its intended use). Specifically, the design heuristic framework was (i) easy to use and understand, (ii) suitable for designing for consent and permissions in smart homes and (iii) effective in addressing design challenges. Another limitation of our workshop study is that we are shaping the problem according to how it fits the proposed solution, rather than having a problem in investigating solutions.

Fifth, roughly 32 heuristics were provided to participants, which is a large number for participants to read through, recall, and use within a short time-frame (compared to Nielson's 10 heuristics). It is possible that fatigue set in during the experiment: participants could have become tired of the experiment resulting in deterioration of the quality of data (e.g., perfunctory answers). To address this, we prompted participants to give comprehensive answers and balanced between collecting accurate and sufficient information and conducting a well-structured not-too-long experiment.

Sixth, a major limitation of our study is that our workshop participants are mostly from younger generations (e.g., between 18 and 44). As such, our sample is biased. Future work should evaluate and test our heuristics with a more representative and diverse sample.

7. Study two results: Design workshops

We detail the results of the second study in this section, presenting the outcomes of our workshops and the ways in which the participants used heuristics. This is followed by an evaluation of the heuristics in the next section (see Section 8).

7.1. Case studies

7.1.1. Problem scenario 1: Design for consent as an on-going relationship

Using the framework and the heuristics given to participants, we asked them to design for consent as an on-going relationship over time for smart speakers. We collected design ideas from participant groups addressing the problem space.

7.1.1.1. Group 1. Tasked with designing for consent as an on-going relationship over time, group 1 used our framework and design heuristics to derive, prototype and iterate new ideas (e.g., selecting relevant heuristics based on their own understanding and experiences). During the workshop, participants designed two additional consent features for smart speakers. First, they designed audio interactions where the smart speaker assistant asked users to revisit their audio recordings every Sunday. Second, they designed a two-step feature for mobile application of smart speakers where the smart speaker assistant added an extra validation option to ask for contact details and voice recordings, as well as providing an undo button. The framework and accompanying heuristics strongly helped participants in deriving new design ideas for the problem posted. Most importantly, it helped engagement and facilitated discussion from diverse and different backgrounds.

7.1.1.2. Group 2. Faced with the same design challenge given to the previous group, group 2 used our framework and design heuristics to derive, prototype and iterate new ideas (e.g., selecting relevant heuristics based on their own understanding and experiences). During the workshop, participants designed one feature for smart speakers, and suggested improvement of other features. First, they created a privacy feature for sharing smart speaker accounts among households. The feature added an automated setting where all users heard notifications from linked accounts once a new account is added to the mobile application of the smart speaker. The setting also allowed users to deny and control consent permissions when new users are added (see Fig. 4c). Second, they suggested that more effective communication should be provided over the physical mute buttons in smart speakers. Especially since it was not clear to participants whether the mute button in smart speakers physically disconnects to the device.

7.1.2. Problem scenario 2: Design family-friendly permission models

Using the framework and the heuristics given to participants, we asked them to design for family-friendly permission models for external and internal smart cameras. We collected design ideas from participant groups addressing the problem space.

7.1.2.1. Group 3. Tasked with designing for family-friendly permission models for smart home cameras, group 1 used our framework and design heuristics to derive, prototype and iterate new ideas (e.g., selecting relevant heuristics based on their own understanding and experiences). During the workshop, participants designed two additional permission features for smart cameras. First, they designed a communal privacy zone feature for families where all family members specify an area within the smart home camera's field-of-view which can be defined as an off-limits area (see Fig. 4b). The feature broadcasted to all households that anything in the area will not be video recorded. Second, they designed a communal privacy permissions feature in smart cameras that allowed all families in a household to control when and what the device recorded in the home. The framework and accompanying heuristics strongly helped participants in deriving new design ideas for the problem posted. Most importantly, it demonstrated value in the design communications among stakeholders.

7.1.2.2. Group 4. Faced with the same design challenge given to group 3, group 4 used our framework and design heuristics to derive, prototype and iterate new ideas (e.g., selecting relevant heuristics based on their own understandings and experiences). During the workshop, participants designed one feature for smart cameras, and suggested the development of offline smart cameras. First, they designed a hibernate mode feature for households using a smart camera that could be triggered by anyone in the household (see Fig. 4a). This would allow households to not only protect their privacy, but also to be used in situations where household members experience domestic or external abuse. Second, the households proposed that offline smart cameras should be developed to be used solely for the purpose of security monitoring. As such, the workshop participants argued that while offline smart cameras would not benefit from advanced features (e.g., cloud storage, phone alerts), it would nearly eliminate privacy and safety risks that come from connected security cameras.

7.2. Heuristics evaluation

Based on our analysis of the workshops, we present how the heuristics were used during the workshop; how heuristics were helpful in facilitating communication and discussion of different design perspectives; what the underlying goals were behind the use of the heuristics; and how effective the heuristics were according to the design outcomes.

7.2.1. The use of heuristics

7.2.1.1. Heuristics used alongside other heuristics. Participant groups (n = 4) combined multiple heuristics (often from different themes) to derive design solutions for the design challenges posed. Participants naturally were able to combine multiple heuristics to solve solutions. For example, group G1 combined three heuristics to design an audio interaction feature where the smart assistant asked users to revisit their settings regularly. They used the *"consider how you might want to retrospectively undo a mistaken consent decision"* heuristic, the *"provide messages through notifications detailing how data can be misused"* heuristic, and the *"periodically revisit granted consent choices"* heuristic to design the feature. Similarly, group G3 combined the *"consider usage triggers that might prompt consent revision"* and the *"research communal spaces where data may affect bystanders and other users"* heuristics to design an automated setting that notifies all households once a new member is added.

7.2.1.2. Heuristics used as a guide for do's and don'ts. Participant groups (n = 2) used heuristics as a guide for do's and don'ts of a particular situation, and used them as an advice on what they should or should not design in particular situations. For example, the heuristic *"ensure that consent collected is valid, informed, and genuine"* was used as a rule and a custom when designing interactions for collecting consent by group G1 and G3. UX Design P10 referred to the heuristic when Ordinary User P11 proposed a new feature that did not explicitly collect consent from the user. UX Designer P10 said: "*You can't do that because if you look at the fourth point under Collect & Indicate consent, it says that consent collected should be informed.*"

7.2.1.3. Heuristics used to directly justify an opinion. To convince other workshop participants, participant groups (n = 3) used heuristics as an acceptable and logical reason or to justify and defend their opinion in a design setting. In G4, Ordinary User P12 was arguing that smart home manufacturers should consider more than the legitimate interest and consent for the legal basis of processing consent, they should consider whether their practices impact human rights or individual values. However, Mobile Developer P14 disagreed with P12 saying that this is the role of regulations. To defend his opinion, P14 cited the "*develop knowledge of the additional uses and negative consequences of smart homes*" heuristic. P14 said: "*As you see in the figure, developers should develop knowledge of additional uses and negative consequences of smart home usage.*"

7.2.1.4. Storytelling was used in the context of heuristics. Participants groups (n = 4) used heuristics to think about important experiences in their real life and used heuristics to derive personal anecdotes and tell stories based on their personal experiences. Participants used anecdotes in two different contexts:

7.2.1.4.1. Using anecdotes to expand and contextualize the heuristic Participants groups (n = 4) used anecdotal evidence to justify an opinion or to provide greater information about a particular problem. It was trying to expand the heuristic, apply it and demonstrate it. For example, Ordinary User P5 recalled a personal anecdote that closely aligns with the heuristic "*consider how you might retrospectively undo a mistaken consent decision*". P5 said: "*I remember adding a friend to my Alexa by mistake, and I couldn't figure out how to undo that. It would be very useful if we can add a two-step validation for these kinds of interactions.*"

7.2.1.4.2. Using anecdotes was used to support and backup the heuristic Participants groups (n = 2) used anecdotes to provide evidence, backup or justify heuristic. For example, UX Designer P10 used vicarious and fictitious storytelling imagined in the eyes of ordinary users to back up the heuristic "*periodically (and make it easy to) revisit granted consent choices.*" P10 said: "*I'd imagine many users are unaware that Google Homes are tracking them in many ways like analyzing their audio recordings. Revisiting their choices and reminding them of what is being collected is crucial.*"

7.2.2. Design discussion context

Heuristics helped participants talk about different design perspectives and problem spaces in different contexts.

7.2.2.1. Heuristics used in a privacy design interaction context. Participant groups (n = 3) used heuristics when solving design problems in the context of user interaction design. Most notably, UX Designers in participant groups G1, G2 and G3 in our workshops discussed heuristics in the context of UX and usability guidelines, focusing on user needs and interests. For example, UX Designer P1 argued that heuristics related to consent should never be overwhelming to the user and should try to be as simple as possible. Similarly, UX Designer P6 said that heuristics concerning misuse of personal data could scare users and should be done very carefully.

7.2.2.2. Heuristics used in a regulatory and data protection context. Participant groups (n = 4) used heuristics when solving design problems in the context of regulation and data protection. Participants focused mostly on the data protection rights of users in the workshops such as providing and withdrawing consent. For example, Participants P7 and P13 aligned some of our consent-related heuristics with data protection regulation when addressing our design challenges. P7 contrasted the "*consider how you might want to retrospectively undo a mistaken consent decision*" heuristic with the right to withdraw consent. Similarly, P13 contrasted the "*ensure that consent collected is valid, informed, and genuine*" heuristic with informed consent principles in medical ethics.

7.2.2.3. Heuristics used in a technical privacy context. Participant groups (n = 3) used heuristics when solving design problems in a technical context. Participants focused on improving design problems such as designing privacy controls by addressing technical aspects of smart home products (e.g., designing better permissions and technical physical privacy control). For example, Security Engineer P4 used the "*be aware that physical privacy properties are more trusted than software settings or indicated lights*" heuristic to discuss the technical difficulties designing physical privacy indicators. Similarly, Mobile Developer P3 used the "*aim for transparency (e.g., provide information showing how personal data has been used over time)*" to tackle the challenge of controlling or knowing what personal data is collected by third party services.

7.2.2.4. Heuristics used outside of privacy design discussions. Participant groups (n = 2) also used heuristics outside of privacy design discussions mostly focusing on the lifecycle of systems and use, and the reuse and proposing of smart home devices. For example, UX designer P13 used the "*develop knowledge of the additional uses and negative consequences of smart homes*" heuristic to discuss how the repurposing of smart home products can be more efficient and useful for smart home users. Moreover, UX Designer P6 used our smart home lifecycle map (e.g., Inception, Configuration, On-going, Update) to suggest more user-friendly smart home lifecycle experiences. This finding shows that our heuristics were also useful outside of a data protection or privacy perspective.

7.2.3. The goals of heuristics

7.2.3.1. Problem understanding. Participants groups (n = 4) used the heuristics (n = 12) to understand the design problem given to them. The heuristics helped participants take a step back and make sure they understood the design task that was given to them. For example, in Group 4, Mobile Developer P14 used heuristics from the '*Define Knowledge Type*' box to understand the problem space before designing a hibernate mode for smart cameras that protects households from privacy breaches, misuse, or abuse. UX designer P13 argued it is important to understand the imbalances, and tensions in the home that can cause conflict. Ordinary User P12 added that it is also important to understand how smart home technologies can be misused or abused.

7.2.3.2. Problem resolution. Participants groups (n = 4) used heuristics to resolve the design problem given to them. The heuristics helped participants determine essential challenges in design problems, identify, prioritize or select alternatives for a solution. For instance, participants in group G2 used three heuristics to address the problem of multi-sharing in smart speakers. The group discussed ways of designing an interface that would be intuitive and easy to use (e.g., having a simple menu of options and allowing multiple users) in addition ensuring the privacy of users (e.g., discussed ways of preventing data from being shared without the user's permission). UX Designer P6 added that researching communal spaces affecting bystanders and non-users in the home is crucial for solving the problems. Security Engineer P7 added that it is critical to be able to understand what kind of users can be added to a household. Ordinary User P5 said they would be more comfortable if they had full control over who can be added to their device (e.g., Amazon Household). These participants designed an automated notification setting that gets triggered when a new account is added to a smart speaker.

7.2.3.3. Problem-solving discussion. Participants groups (n = 4) used problem-solving discussion to resolve the design problem given to them. The heuristics helped participants discuss unsatisfactory situations, design goals, and obstacles that must be surmounted to address the design challenge. For example, participants in group G1 had different opinions about the "*be aware that physical privacy properties are more trusted than software settings or indicated lights*" heuristic which has been used for addressing the design challenge of privacy controls around smart speakers. Security engineer P4 argued that the mute button in smart speakers such as Amazon Echo is a hardware button (physical switch) according to various sources, and as a result, there is no need for design changes. In return, Ordinary User P2 said that despite what P4 has mentioned, they still cannot trust that the device will protect their privacy. The group resolved the problem by recommending more effective communication over the physical muting button of smart speakers.

7.2.4. The effectiveness of heuristics

To define satisfactory and unsatisfactory design outcomes, we adopted Swan and Combs's definition (Swan and Combs, 1976) of customer satisfaction as involving (1) instrumental performance that meets or exceeds expectations, and (2) expressive performance that meets or exceeds expectation.

7.2.4.1. Successful design outcomes. We define satisfactory design outcomes as a situation where the understanding, solution and discussion of the result lead to a clear resolution that satisfies all parties who were present in the workshop. Most design outcomes (n = 8) that were tackled in the workshop by the participants were successful. In Groups 1 and 2, participant groups successfully used the heuristics to design outcomes to address the challenge of consent in smart speakers. They designed a two-step feature for providing consent, a consent revisiting feature and a privacy sharing feature. Similarly, in groups 3 and 4, participant groups successfully used the heuristics to design outcomes to address the challenge of permissions in smart cameras. They designed a communal privacy zone feature, a permission alerting feature, and a hibernate safety mode feature.

7.2.4.2. Unsatisfactory design outcomes. We define unsatisfactory design outcomes as a situation that arises when problem understanding, and problem discussion do not result in a clear resolution that satisfies all parties who were present in a workshop. While most design outcomes were successful, some design outcomes (n = 2) were unsuccessful. In Group 2, participants disagreed over how privacy features in smart speakers can be effective, mostly whether changing the privacy features (e.g., physical mute button) can improve the privacy assurance. While the participants could not use the heuristics to come up with a design solution, they were able to use them to facilitate a discussion around more effective commutation concerning the privacy features of smart speakers.

8. Heuristics evaluation

To evaluate the usefulness and the application of the heuristics, we looked at the heuristics, the models, and descriptions of reuse and lifecycle. However, during our open-ended qualitative analysis, we could not identify significant quality fact evidence from how the framework was articulated (due to the nature of our PD workshops), so we focused exclusively on evaluating the security and privacy design heuristics individually rather than the framework holistically.

The purpose of our evaluation and analysis was to identify how heuristics are used in design workshops and hence how they can be useful to designers of consent interactions and inform privacy by design. Furthermore, since this was a co-design space, every participant brought their own background and previous experiences. We chose to analyze the design discussions that explicitly mention our heuristics to rule out factors related only to the participants.

To evaluate the design heuristics framework, we conducted a qualitative exploration focusing on enhancing our understanding and putting results into a more meaningful context. Two team members analyzed the design workshops with thematic analysis. Evaluation of the heuristics was based on (i) whether the heuristics were understood or not, (ii) the number of times the heuristics were referenced, (iii) the reception (i.e., sentiment) of participants' responses for heuristics according to a simple closed-coding scheme: positive, neutral, negative,

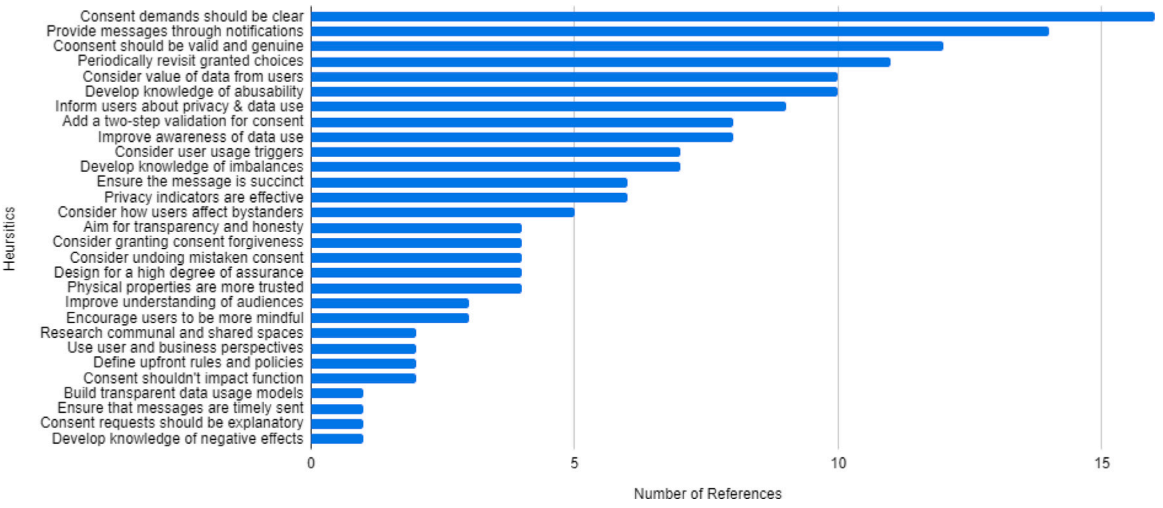
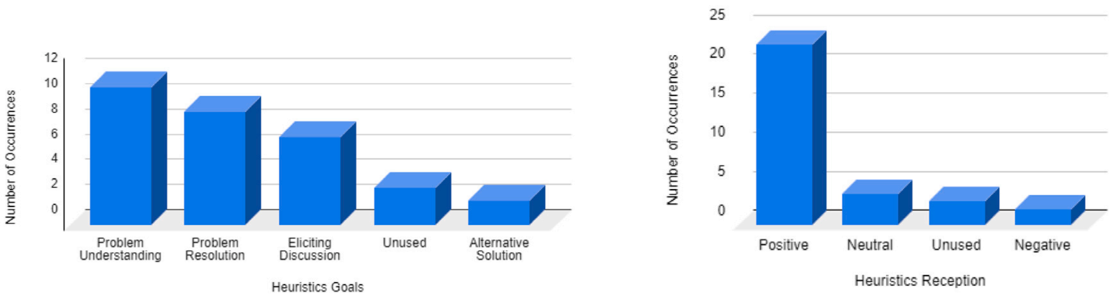


Fig. 5. Most referenced heuristics (from most to least referenced). Three heuristics were not used and omitted from the figure. The text of heuristics was shortened in order to construct this figure. The full list of heuristics can be found in Table F.5 in Appendix F.



(a) Goals of the heuristics (b) Reception of the heuristics

Fig. 6. (a) Heuristics were used for Problem Understanding (n = 11), Problem Resolution (n = 9), Eliciting Discussion (n = 7) and Alternative Solution (n = 2). (b) 72% of heuristics were positively received, 12% were neutral, 9% were unused and 6% were negatively perceived.

or indeterminable (iv) the goals of the participants when trying to use the heuristics.

The first and third team members independently completed an initial coding of all transcripts, identifying relevant participant utterances and assigning them to codes. The second team member then cross-checked the codes against the transcripts, asking for clarifications and additional context from the first and third team member, who annotated the study data to note ambiguities and disagreements. The initial coding had an agreement of 0.68 (average Cohen's kappa coefficient (κ) for all codes). All team members negotiated each disagreement, resulting in the re-coding of participant utterances, addition, deletion of merging codes. After cross-reviewing coding decisions, clarifying coding rules, and independently re-coding the utterances, inter-rater reliability increased to an acceptable level (average Cohen's κ was 0.85) (McHugh, 2012).

Figs. 5 and 6 illustrate our evaluation results: Fig. 5 displays the heuristics used from highest to lowest, while Fig. 5 displays the goals and reception of the heuristics. These results may not be representative of the wider usefulness of heuristics or their applicability in different scenarios.

9. Discussion

9.1. Prominent heuristics

We highlight and summarize the design heuristics that had the biggest influence:

9.1.1. Ensure that demands for consent are explanatory and make sense to the user

This heuristic prompted workshop participants to consider more user-friendly consent experiences that go beyond the minimum legal requirements and ensure that consent requests are fully understandable and clear to the user. For instance, this heuristic was used by Groups 1, 2 and 3 to go beyond what is being required by data protection regulation when designing privacy and security features for smart home products.

9.1.2. Providing messages through notifications detailing how data can be misused

This heuristic prompted workshop participants to improve the transparency of smart home interactions by looking at innovative areas such as conversational interfaces. For example, this heuristic was used by Group 1 when designing a two-step validation feature that is used when users are providing consent for their personal data use. Workshop participants used the heuristic to add include messages (e.g., risks of consenting to personal data) when two-step validation interactions are triggered.

9.1.3. Periodically (and make it easy to) revisiting granted consent choices

This heuristic prompted workshop participants to design for consent as an-going relationship that can change over time and require updates. For instance, this heuristic was used by Group 2 to examine frequent situations where users might need to revisit their consent preferences and design for appropriate interactions. For example, workshop participants designed a feature that helped users easily revisit their consent permissions once a new user is added to the environment of a smart home application. The heuristic was also used by Group 1 to design a smart speaker assistant feature that makes it easy for them to control their privacy choices through audio interactions.

9.1.4. Considering the value of data to users, the company, attackers, bystanders and other users

This heuristic prompted workshop participants to relate to the perceptions of value of personal data from all various stakeholders, instead of having narrow views of the dimensions and the value of personal data. For instance, this heuristic was used by Group 2 to improve the UX of privacy controls of smart speakers (e.g., physical mute buttons). Workshop participants considered the value of smart speaker audio recordings from the perspective of users (e.g., ability of users to fully control their audio recordings) and business leaders (e.g., ability of the manufacturer to improve the voice recognition service).

9.1.5. Developing knowledge of the abusability, and repurposing of smart homes

This heuristic prompted workshop participants to consider all discoverability features of smart homes that improve security and privacy of the devices but also can be exploited and misused by adversaries. For example, this heuristic was used by Group 4 to design a hibernate mode for smart cameras that can instantly turn off smart cameras in situations of suspected misuse and by Group 3 to design a privacy feature that allows household members to restrict sensitive areas of the home from being recorded (e.g., bedrooms).

9.2. The interplay between consent and permissions

Heuristics as described in our framework focused broadly on consent, however it is interesting to note the relationship between consent interactions and permission design. For smart home interactions which are consensual or egalitarian, participants used the consent heuristics to help design permissions models that were well suited to that domestic environment. This would suggest a wider benefit in applying principles of responsible consent management to help design, configure, and manage the permissions for data use in unregulated domestic spaces. More work is needed to fully explore this, however we believe that this is a promising approach for embedding the principle of responsibility into how smart devices are designed and used in communal domestic settings.

9.3. Problems of designing for permissions

The model underpinning smart home permissions tends to concentrate on authority, and does not tackle the problem of decision-making (e.g. helping users decide on appropriate data use for themselves, other users, or bystanders) or help evaluate the implications of those design decisions. In the absence of permission and administration models that are more consensual or more democratic, our results show that consent heuristics can be helpful in exploring this space.

Furthermore, participants brought many of their own values into the participatory design workshops such as fairness, equality, and agency. Our design heuristics also brought some other values (such as transparency and accountability). While the values of the participants and those embodied in the heuristics were well aligned, we can anticipate that this may not hold for all situations and all cultural contexts. While it is beyond the scope of this paper to explore this in more detail, this points to a wider problem in the design of technology that aims to operate in less regulated spaces, where different contextual norms and values may conflict with those that are embodied in its design.

9.4. Why are heuristics useful

9.4.1. Heuristics demonstrated value in communicating design

Participant groups (n = 2) used heuristics to communicate design compellingly. Heuristics gave participants the ability to articulate design decisions which helped signal to other stakeholders they can be trusted. They also allowed them to prove purpose, validating that they have thought about their solutions and that there is logic to their approach.

9.4.2. Heuristics fostered engagement and discussions

In addition, heuristics elicited and fostered discussions through storytelling and by facilitating communication of specific issues. Heuristics helped participant groups (n = 4) in fostering participatory engagement and discussion within different stakeholders, enabling conversation and active skills.

9.4.3. Heuristics helped avoid profound analysis needed for complex problems

Participants groups (n = 3) found heuristics to be an effective method for identifying, defining, and potentially solving complex design problems that involved ambiguity, had a lot of unknowns and ill-defined boundaries. They helped to resolve a problem without further analysis.

9.5. Why are heuristics unuseful

Our results also show that there are more contentious heuristics that were unsuitable for stakeholders and were not used. This may be due to a smaller sample of design workshops and participants, a lack of clarity in the heuristic, disagreement with the intent or values embodied by the heuristic, or due to how the workshops were designed. Overall, we believe that these heuristics are best used to enrich the understanding of designers and to facilitate the communication between the stakeholders rather than providing a solution.

9.6. Study implications

Our Framework of Design Heuristics in Section shows that responsible innovation (Stilgoe et al., 2020; Owen et al., 2013; von Schomberg, 2013; Koops, 2015) is implicitly tied to our design heuristics. The user-centricity of the heuristics enabled designers to better understand the context and the values of the users as well as their needs and limitations. As a result, they helped tackle responsibility in innovation and promote responsible thinking. For example, many of our heuristics for consent and communication are focused on improving the UX of smart home products, making them more user-centric, which is inherently more value sensitive, hence leading to more responsibility (e.g., consider how users interact with personal data that is specific to only one user).

Furthermore, our Framework of Design Heuristics also showed that heuristics helped designers act more responsibly in tackling security, privacy and ethical challenges (e.g., UX designers in the workshop considered ethical and human right issues to design panic features). Explicitly taking user values into account and designing for them would achieve responsible behavior and responsible decisions from all stakeholders. This is evidenced in prior research where user experience is regarded as a shared responsibility among all stakeholders (e.g., users, designers and business leaders) who contribute to the development of a smart home product (Chalhoub et al., 2020a; Chalhoub, 2020; Kuniavsky, 2003).

Since UX is useful for tackling user-centricity of smart home products, our research tackled two aspects of responsible innovation: the ethical and social implications. It also tackled the legal aspects of responsible innovation through data protection regulation. Future work should strongly consider their environmental impacts (e.g., explore how data security and privacy practices of smart homes could be less harmful for the environment while achieving their function).

In addition, more work needs to be done to identify and explore responsible perspectives from our framework of design heuristics. In particular, future work should explore in more detail how to (i) identify more heuristics that tie to responsibility and (ii) identify existing heuristics for which there is a responsibility perspective. For instance, future work can categorize heuristics that seem to tie to responsibility from those that do not at all. In addition, future work can explore what constitutes a responsible design recommendation and develop frameworks or methods that can evaluate design recommendations for their responsibility.

Moreover, to facilitate the process of responsible innovation, we argue that smart home designers, researchers, business leaders, regulators and decision makers should continuously exercise the moral imagination to consider the socio-technical implications of smart home technologies. Since moral imagination takes time to build, we propose that designers, business leaders and companies should invest in developing tools, framework and methods that can facilitate moral imagination. For example, researchers at Microsoft have introduced a Responsible Innovation Practices Toolkit to help facilitate responsible innovation practices (Lane, 2020). While these are not guaranteed to address all the challenges, they represent a good direction towards designing responsible smart home technologies with better intention.

10. Conclusion

The design for privacy in smart home devices faces a plethora of challenges in addressing user, business and regulatory needs. Despite their awareness to balance such competing interests, designers may lack the means to explore and communicate essential requirements and possible solutions with different stakeholders. This results in bad design outcomes that are particularly worrying with regards to the UX of privacy and data protection in smart homes.

This paper proposed and evaluated design heuristics as "*fast and practical ways to solve problems and make decisions*" during the design process. We presented a framework of heuristics for smart home consent interactions based on a conceptual framework analysis of data collected from researching smart homes and the UX design literature. We demonstrated its application through a series of four workshops exploring how consent interactions could be designed and how consent principles influence the design of permissions models in smart homes. Based on a detailed analysis of the workshop transcripts, we evaluated the heuristics and identified how these are used in the design setting, and can be used to foster innovative thinking around consent in smart home devices.

We conclude that design heuristics can be instrumental in improving the UX of privacy in smart homes. Our heuristics allowed designers to effectively demonstrate to stakeholders how their design decisions were positioned against the backdrop of regulatory requirements, user demands, and business interests. The heuristics proved particularly useful in allowing designers to apply techniques of storytelling and participatory engagement when approaching design problems with ambiguity and ill-defined boundaries.

We encourage future work to pursue design heuristics for the UX of privacy in smart homes. Future work should further explore the scope for design heuristics in privacy UX design. Future iterations with participatory formats should refine our set of heuristics and apply them in real world settings. Overall, we believe that design heuristics have the potential to help build bridges between user, business and regulatory interests.

CRediT authorship contribution statement

George Chalhoub: Conceptualization, Methodology, Software, Data curation, Validation, Writing – review & editing. **Martin J. Kraemer:** Writing – original draft. **Ivan Flechais:** Visualization, Supervision, Investigation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Appendix A. Design heuristics

We list the design heuristics from our framework (see Appendix G) which were derived from our conceptual framework analysis procedure (see Section 4.1).

- Research communal spaces where data may affect bystanders and other users
- Improve understanding of audiences and contextual uses of smart home products
- Consider how the actions of one user can affect other bystander users
- Build data usage models that represent transparent and ethical data usage practices
- Encourage users to learn the value of their data and make more mindful decisions
- Provide messages through notifications detailing how data can be misused
- Design and provide educational material to users of smart home products at crisis times
- Ensure that message are sent at the right time and the relevant stage of the life cycle
- Use user and business perspectives to communicate value of personal information
- Make sure the message is clear and succinct, and test it against sample users.
- Define upfront rules, heuristics and policies for deciding whether an event requires new notification.
- Periodically (and make it easy to) revisit granted consent choices
- Aim for transparency (e.g., provide information showing how personal data has been used over time)
- Consider usage triggers (changes to bystanders or users) that might prompt consent revisions
- Consider in which phases of the system life cycle would it be appropriate to revisit consent
- Consider how much forgiveness can you grant, and the implications of revoking mistakenly given consent.
- Consider how you might want to retrospectively undo a mistaken consent decision.
- Add a two-step validation for consent decisions to ensure genuine choices
- Collecting consent should not impact an unrelated function
- If functionality requires consent, it should be explicit, and truthful
- Ensure that demands for consent are explanatory and make sense to the user
- Ensure that consent collected is valid, informed, and genuine.
- Consider how users can improve their awareness of data use from the company and other users.
- Consider how users interact with personal data that is specific to only one user.
- Consider what information you provide to users about personal data use.
- Consider the value of data to users, the company, attackers, bystanders and other users.
- Develop knowledge of imbalances, interests, and tensions which might cause conflict

- Develop knowledge of the additional uses and negative consequences of smart homes
- Develop knowledge of the abusability, and repurposing of smart home technologies
- Aim to design for the highest degree of assurance based on sensitive various functions
- Be aware that physical privacy properties are more trusted than software settings or indicated lights
- Consolidate information related to the effectiveness of privacy settings indicators

Appendix B. Conceptual framework analysis codebook

user experience

usability
utility
product
learnability
flexibility
robustness
branding
design
usability
function
accessibility
utility
credibility
human factors
design
marketing
HCI
user research

design guidelines

guidelines
heuristics
principles
practices
standards
rules
abstract rules
shortcuts
rules of thumb
guides
recommendations
general applications
low authority
limited applications
high authority
specific design rules
abstract design rules
high generalizability

user security

authentication
authorization
account management
password management
security updates
security tools
security design
security vulnerabilities
security concerns
security breaches
security behaviors
usable security
unauthorized access
data theft
access control
secure by design
security threats
security updates

user privacy

privacy by design
privacy design
consent management
data protection
tracking
privacy tools
privacy management
privacy control
privacy perceptions
privacy challenges
privacy attacks
privacy preferences
privacy concerns
privacy threats
privacy behaviors
transparency
privacy countermeasures
trust

home tech

smart speakers
smart cameras
smart plugs
smart bulbs
smart kitchen
smart thermostats
smart phones
smart alarms
smart doorbells
smart hubs
smart door locks
smart ecosystem
home cameras
motion sensors
microphones
smart home assistants
smart heaters
smart displays
smart watches

Appendix C. Code definitions

User Experience:

- Usability: The ease with which users can learn to use a product and how efficient they are able to use it.
- Utility: The usefulness of a product in meeting the user's needs.
- Product: A tangible or intangible object that is created to meet the needs of a user.
- Learnability: The ease with which users can learn how to use a product.
- Flexibility: The ability of a product to be adapted to the needs of different users.
- Robustness: The ability of a product to withstand the demands of use.
- Branding: The process of creating a unique identity for a product or service.
- Design: The process of creating a product or service that is both functional and appealing.
- Function: The purpose or intended use of a product or service.
- Valuable: Worthy of being valued or esteemed.
- Accessibility: The ability of people with disabilities to use a product or service.
- Utility: The usefulness of a product or service.
- Credibility: The quality of being believable or trustworthy.
- Human factors: The study of the interaction between humans and machines.
- Design: The process of creating a product or service that is both functional and appealing.
- Marketing: The process of promoting and selling a product or service.
- System performance: The ability of a system to meet the demands placed on it.
- Ergonomics: The study of the design of objects and environments for human use.
- HCI: Human–computer interaction, the study of the interaction between humans and computers.
- User research: The process of gathering information about users' needs and preferences in order to improve the design of a product or service.

Design Guidelines:

- Guidelines: A set of rules or principles that are used to guide the design of a product or service.
- Heuristics: General rules of thumb that are used to evaluate the usability of a product or service.
- Principles: Fundamental truths or beliefs that guide the design of a product or service.
- Practices: Specific ways of doing things that are used in the design of a product or service.
- Standards: Formal specifications that define the requirements for a product or service.
- Rules: Explicit instructions that must be followed in order to achieve a desired outcome.
- Abstract rules: Rules that are not specific to any particular product or service.
- Shortcuts: Rules that allow users to complete tasks more quickly.
- Rules of thumb: General rules that are used to guide decision-making.
- Guides: Documents that provide information and guidance on the design of a product or service.
- Recommendations: Suggestions that are made based on expert knowledge.
- General applications: Guidelines that can be applied to a wide range of products and services.
- Low authority: Guidelines that are not binding and can be ignored at the discretion of the designer.
- Limited applications: Guidelines that are only applicable to a specific type of product or service.
- High authority: Guidelines that are binding and must be followed by the designer.

Table E.4
Conceptual Framework Analysis Papers.

	ux	design	user security	user privacy	home tech
More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. Noura Abdi, Kopo M. Ramokapane, and Jose M. Such.	✓		✓	✓	✓
A Review of Smart Homes—Past, Present, and Future. Muhammad Raisul Alam, Mamun Bin Ibne Reaz, and Mohd Alauddin Mohd Ali.					✓
Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2017. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic.				✓	✓
Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering smart home internet of things privacy norms using contextual integrity.				✓	✓
Gaurav Bansal, Fatemeh ‘Mariam’ Zahedi, and David Gefen. 2015. The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern.	✓			✓	
Genevieve Bell and Paul Dourish. 2007. Yesterday’s tomorrows: notes on ubiquitous computing’s dominant vision.					✓
Victoria Bellotti and Abigail Sellen. 1993. Design for privacy in ubiquitous computing environments.			✓		
Asa Blomquist and Mattias Arvola. 2002. Personas in action: ethnography in an interaction design team.	✓	✓			
A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. 2011. Home automation in the wild: challenges and opportunities.	✓				✓
Marshini Chetty, Richard Banks, Richard Harper, Tim Regan, Abigail Sellen, Christos Gkantsidis, Thomas Karagiannis, and Peter Key. 2010. Who’s hogging the bandwidth: the consequences of revealing the invisible in the home.				✓	✓
Nielsen, J., and Molich, R. (1990). Heuristic evaluation of user interfaces.	✓	✓			
Experience, World Leaders in Research-Based User. "Heuristic Evaluation: How-To: Article by Jakob Nielsen".	✓	✓			
Molich, R., and Nielsen, J. (1990). Improving a human–computer dialogue.	✓	✓			
Nielsen, J. (1994). Heuristic evaluation. In Nielsen, J., and Mack, R.L. (Eds.).	✓	✓			
Nielsen, Jakob (1994). Usability Engineering.	✓	✓			
Gerhardt-Powals, Jill (1996). "Cognitive engineering principles for enhancing human – computer performance".	✓	✓			
Heuristic Evaluation – Usability Methods – What is a heuristic evaluation?	✓	✓			
Shneiderman (1998, p. 75); as cited in: “Eight Golden Rules of Interface Design”	✓	✓			
Malviya, Kartik (20 November 2020). “8 Golden Rules of Interface Design”	✓	✓			
Weinschenk, S and Barker,D. (2000) Designing Effective Speech Interfaces. Wiley.	✓	✓			
Jeff Sauro. "What’s the difference between a Heuristic Evaluation and a Cognitive Walkthrough?"	✓	✓			
Nizamani, Sehrish; Khoumbati, Khalil; Nizamani, Sarwat; Memon, Shahzad; Nizamani, Saad; Laghari, Gulsher A methodology for domain and culture-oriented heuristics creation and validation".	✓	✓			
Nizamani, Sehrish; Nizamani, Saad; Basir, Nazish; Memon, Muhammad; Nizamani, Sarwat; Memon, Shahzad (5 April 2021). "Domain and culture-specific heuristic evaluation of the websites of universities of Pakistan".	✓	✓			
Marshini Chetty, Ja-Young Sung, and Rebecca E. Grinter. 2007. How Smart Homes Learn: The Evolution of the Networked Home and Household.					✓
Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, and Julie A. Kientz. 2011. Living in a glass house: a survey of private moments in the home.				✓	✓
Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. 2012. Investigating receptiveness to sensing and inference in the home using sensor proxies.			✓	✓	✓
K. L. Courtney. 2008. Privacy and Senior Willingness to Adopt Smart Home Information Technology in Residential Care Facilities.				✓	✓
Scott Davidof, Min Kyung Lee, Charles Yiu, John Zimmerman, and Anind K. Dey. 2006. Principles of Smart Home Control.				✓	✓
George Demiris and Brian K. Hensel. 2008. Technologies for an aging society: a systematic review of “smart home” applications.					✓
Paul Dourish, Rebecca E. Grinter, Jessica Delgado De La Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem.			✓		✓
Serge Egelman, Raghudeep Kannavara, and Richard Chow. 2015. Is This Thing On? Crowdsourcing Privacy Indicators for Ubiquitous Sensing Platforms.				✓	✓

(*continued on next page*)

Table E.4 (*continued*).

Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior.	✓		✓	✓	✓
Christine Geeng and Franziska Roesner. 2019. Who's In Control?: Interactions In Multi-User Smart Homes.	✓		✓	✓	✓
Esther Goernemann and Sarah Spiekermann. 2020. Moments of Truth with Conversational Agents: An Exploratory Quest for the Relevant Experiences of Alexa Users.	✓				✓
Manu Gupta, Stephen S. Intille, and Kent Larson. 2009. Adding GPS-Control to Traditional Thermostats: An Exploration of Potential Energy Savings and Design Challenges.		✓	✓		✓
Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking access control and authentication for the home internet of things (IoT).			✓		✓
Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras.				✓	✓
Information Commissioner's Ofce. 2020. When is consent appropriate?				✓	
Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. 2017. The Catch(es) with Smart Home: Experiences of a Living Lab Field Study.	✓				✓
Timo Jakobi, Gunnar Stevens, Nico Castelli, Corinna Ogonowski, Florian Schaub, Nils Vindice, Dave Randall, Peter Tolmie, and Volker Wulf. 2018. Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility.	✓		✓		✓
Roxanne Leitão. 2019. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse.			✓	✓	✓
Brian Y. Lim, Anind K. Dey, and Daniel Avrahami. 2009. Why and why not explanations improve the intelligibility of context-aware intelligent systems.	✓				✓
Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users.	✓			✓	✓
Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. "What Can't Data Be Used For?":				✓	✓
Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. 2019. Consumer Smart Homes: Where WeAre and Where WeNeed toGo.					✓
Michelle L. Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger, and Michael K. Reiter. 2010. Access Control for Home Data Sharing: Attitudes, Needs and Practices.			✓		✓
Michelle L. Mazurek, Peter F. Klemperer, Richard Shay, Hassan Takabi, Lujo Bauer, and Lorrie Faith Cranor. 2011. Exploring reactive access control.			✓		
Sarah Mennicken and Elaine M. Huang. 2012. Hacking the Natural Habitat: An In the-Wild Study of Smart Homes, Their Development, and the People Who Live in Them.	✓				✓
Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world.				✓	✓
David H. Nguyen, Alfred Kobsa, and Gillian R. Hayes. 2008. An empirical investigation of concerns of everyday tracking and recording technologies.				✓	✓
Norbert Nthala and Ivan Flechais. 2018. Informal support networks: an investigation into home data security practices.			✓		✓
Norbert Nthala and Emilee Rader. 2020. Towards a Conceptual Model for Provoking Privacy Speculation.				✓	
Antti Oulasvirta, Aurora Pihlajamaa, Jukka Perkìo, Debarshi Ray, Taneli V́ahäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. 2012. Long-term efects of ubiquitous surveillance in the home.				✓	✓
Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world.				✓	✓
Erika Shehan Poole, Marshini Chetty, Rebecca E. Grinter, and W. Keith Edwards. 2008. More than meets the eye: transforming the user experience of home network management.	✓				✓
Dave Randall. 2003. Living Inside a Smart Home: A Case Study. In Inside the Smart Home, Richard Harper (Ed.).	✓				✓
Erika Shehan and W. Keith Edwards. 2007. Home networking and HCI: what hath god wrought?	✓				✓
Peter Tolmie, Andy Crabtree, Tom Rodden, Chris Greenhalgh, and Steve Benford. 2007. Making the home network at home: Digital housekeeping.					✓
Daphne Townsend, Frank Knoefel, and Rafk Goubran. 2011. Privacy versus autonomy: A tradeof model for smart home monitoring technologies.	✓				✓

(*continued on next page*)

Table E.4 (*continued*).

Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2013. The current state of access control for smart devices in homes.			✓		✓
Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance.				✓	✓
Meredydd Williams, Jason RC Nurse, and Sadie Creese. 2017. Privacy is the boring bit: user perceptions and behaviour in the Internet-of-Things.	✓			✓	✓
Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2015. Smart homes and their users: a systematic analysis and key challenges.	✓				✓
Charlie Wilson, Tom Hargreaves, and Richard HauxwellBaldwin. Benefits and Risks of Smart Home Technologies.			✓	✓	✓
Jong-bum Woo and Youn-kyung Lim. 2015. User experience in do-it-yourselfstyle smart homes.	✓				✓
Allison Woodruf, Sally Augustin, and Brooke Foucault. 2007. Sabbath day home automation: "it's like mixing technology and religion".	✓				✓
Rayoung Yang and Mark W. Newman. 2013. Learning from a learning thermostat: lessons for intelligent systems for the home.	✓				✓
Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes.	✓		✓	✓	✓
Eric Zeng and Franziska Roesner. 2019. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study.	✓		✓	✓	✓
Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy.	✓			✓	✓
Ivan Flechais, M. Angela Sasse, and Stephen M. V. Hailes. Bringing Security Home: A Process for Developing Secure and Usable Systems.	✓	✓	✓		
Mary Ellen Zurko. User-Centered Security: Stepping Up to the Grand Challenge.	✓	✓	✓		
Lee A. Bygrave. Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements.		✓		✓	
Kambiz Ghazinour and Emil Shirima. Privacy for Security Monitoring Systems.				✓	✓
Rosa Yáñez Gómez, Daniel Cascado Caballero, and José-Luis Sevillano. Heuristic Evaluation on Mobile Interfaces: A New Checklist.		✓			
Timo Jokela. Assessments of Usability Engineering Processes: Experiences from Experiments.	✓				
Michael Onuoha Thomas, Beverly Amunga Onyimbo, and Rajasvaran Logeswaran. Usability Evaluation Criteria for Internet of Things.	✓	✓			
Claire Rowland. UX and Service Design for Connected Products.	✓				✓
Tyler W. Thomas, Madiha Tabassum, Bill Chu, and Heather Lipford. Security During Application Development: An Application Security Expert Perspective.	✓		✓		
Tayyaba Nafees, Natalie Coull, Ian Ferguson, and Adam Sampson. Vulnerability Anti-patterns: A Timeless Way to Capture Poor Software Practices (Vulnerabilities).			✓		
Hala Assal and Sonia Chiasson. Security in the Software Development Lifecycle.			✓		
Johanna Bergman and Isabelle Johansson. The User Experience Perspective of Internet of Things Development.	✓				✓
Noura Aleisa and Karen Renaud. Privacy of the Internet of Things.				✓	✓
Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User Perceptions of Smart Home IoT Privacy.	✓			✓	✓
Panagiotis Zagouras, Christos Kalloniatis, and Stefanos Gritzalis. Managing User Experience: Usability and Security in a New Era of Software Supremacy.	✓		✓		
Niels Raabjerg Mathiasen and Susanne Bødker. Threats or Threads - From Usable Security to Secure Experience?	✓		✓		
Fungai Bhunu Shava and Darelle Van Greunen. Factors Affecting User Experience with Security Features: A Case Study of an Academic Institution in Namibia.	✓		✓		
Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. Understanding the Experience-Centeredness of Privacy and Security Technologies.	✓		✓	✓	
Julia Bernd, Alisa Frik, Maritza L. Johnson, and Nathan Malkin. Smart Home Bystanders: Further Complexifying a Complex Context.			✓	✓	✓
Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. Privacy Perceptions and Designs of Bystanders in Smart Homes.	✓			✓	✓
Jeungmin Oh and Uichin Lee. Exploring UX Issues in Quantified Self Technologies.	✓				✓

(*continued on next page*)

Table E.4 (*continued*).

Johanna Bergman, Thomas Olsson, Isabelle Johansson, and Kirsten Rassmus-Gröhn. An Exploratory Study on How Internet of Things Developing Companies Handle User Experience Requirements.	✓				✓
Ali Dorri, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home.			✓	✓	✓
Andreas Jacobsson and Paul Davidsson. Towards a Model of Privacy and Security for Smart Homes.			✓	✓	✓
Claire Rowland, Elizabeth Goodman, Martin Charlier, Ann Light, and Alfred Lui. Designing Connected Products : UX for the Consumer Internet of Things.	✓				✓
Marc Hassenzahl and Noam Tractinsky. User experience — a research agenda.	✓				
Jingjing Ren, Daniel J. Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach.			✓	✓	✓
Junia Valente, Matthew A. Wyn, and Alvaro A. Cardenas. Stealing, Spying, and Abusing: Consequences of Attacks on Internet of Things Devices. IEEE Security			✓	✓	✓
Sarah Spiekermann and Lorrie Faith Cranor. “Engineering Privacy”.				✓	
Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. “A Design Space for Eective Privacy Notices”.		✓		✓	
Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. “Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online”.	✓			✓	
Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. “Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes”.				✓	✓
Ewa Luger, Lachlan Urquhart, Tom Rodden, and Michael Golembewski. “Playing the legal card: Using ideation cards to raise data protection issues within the design process”.	✓	✓		✓	✓
Helen J. Richardson. “A ’smart house’ is not a home: The domestication of ICTs”.					✓
Jon O’Brien, Tom Rodden, Mark Rounceeld, and John Hughes. “At Home with the Technology : An Ethnographic Study of a Set-Top-Box Trial”.	✓				✓
Sarah Mennicken, Jo Vermeulen, and Elaine M Huang. “From Today ’ s Augmented Houses to Tomorrow ’ s Smart Homes : New Directions for Home Automation Research”.					✓
Peter Tolmie, James Pycock, Tim Diggins, Allan MacLean, and Alain Karsenty. “Towards the Unremarkable Computer: Making Technology at Home in Domestic Routine”.	✓				✓
Peter Tolmie, Andy Crabtree, Tom Rodden, Chris Greenhalgh, and Steven Benford. “Making the Home Network at Home: Digital Housekeeping”.	✓				✓
Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. “I don’t own the data": End User Perceptions of Smart Home Device Data Practices and Risks”.	✓			✓	✓
Sarah Mennicken and Elaine M Huang. “Hacking the natural habitat: An in-the-wild study of smart homes, their development, and the people who live in them”.					✓
Ssara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. ““She’ll Just Grab Any Device That’s Closer”: A Study of Everyday Device & Account Sharing in Households”.	✓		✓		✓
Roxanne Leitão. “Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse”.			✓	✓	
Yolande Strengers, Jenny Kennedy, Paula Arcari, Larissa Nicholls, and Melissa Gregg. “Protection, Productivity and Pleasure in the Smart Home”.	✓				✓
Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. “I’m All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios”.	✓			✓	✓
Andy Crabtree, Richard Mortier, Toni Robertson, and Ina Wagner. “Human Data Interaction: Historical Lessons from Social Studies and CSCW”.	✓				
Karola Marky, Alexandra Voit, Alina St̀over, Kai Kunze, Svenja Schŕoder, and Max M̀uhlh́auser. ““I Don’t Know How to Protect Myself”: Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments”.	✓			✓	✓
Vinay Koshy, Joon Sung Park, Ti-Chung Cheng, and Karrie Karahalios. ““We Just Use What They Give Us”: Understanding Passenger User Perspectives in Smart Homes”.	✓				✓
Liam J. Bannon. “From Human Factors to Human Actors: The Role of Psychology and Human-Computer Interaction Studies in System Design”.	✓	✓			
Lian J Bannon. “Perspectives on CSCW: From HCI and CMC to CSCW”.	✓				
Paul M. Aoki and Allison Woodru. “Making space for stories: ambiguity in the design of personal communication systems”.	✓				

Table F.5
Heuristic evaluation details.

Design Heuristics	Used	Understood	Ref	Reception	Goals
Research communal spaces where data may affect bystanders and other users	✓	Yes	2	Positive	Problem Understanding
Improve understanding of audiences and contextual uses of smart home products	✓	Yes	3	Positive	Problem Understanding
Consider how the actions of one user can affect other bystander users	✓	Yes	5	Positive	Problem Understanding
Build data usage models that represent transparent and ethical data usage practices	✓	Yes	1	Neutral	Alternative Solution
Encourage users to learn the value of their data and make more mindful decisions	✓	Yes	3	Positive	Problem Resolution
Provide messages through notifications detailing how data can be misused	✓	Yes	14	Positive	Problem Resolution
Design and provide educational material to users of smart home products at crisis times		N/A	N/A	N/A	N/A
Ensure that message are sent at the right time and the relevant stage of the life cycle	✓	No	1	Negative	Eliciting Discussion
Use user and business perspectives to communicate value of personal information	✓	Yes	2	Positive	Problem Understanding
Make sure the message is clear and succinct, and test it against sample users.	✓	Yes	6	Positive	Problem Resolution
Define upfront rules, heuristics and policies for deciding whether an event requires new notification.	✓	Yes	2	Neutral	Alternative Solution
Periodically (and make it easy to) revisit granted consent choices	✓	Yes	11	Positive	Problem Resolution
Aim for transparency (e.g., provide information showing how personal data has been used over time)	✓	Yes	4	Positive	Eliciting Discussion
Consider usage triggers (changes to bystanders or users) that might prompt consent revisions	✓	Yes	7	Positive	Problem Understanding
Consider in which phases of the system life cycle would it be appropriate to revisit consent		N/A	N/A	N/A	N/A
Consider how much forgiveness can you grant, and the implications of revoking mistakenly given consent.	✓	Yes	4	Positive	Problem Understanding
Consider how you might want to retrospectively undo a mistaken consent decision.	✓	Yes	4	Positive	Problem Understanding
Add a two-step validation for consent decisions to ensure genuine choices	✓	Yes	8	Positive	Problem Resolution
Collecting consent should not impact an unrelated function	✓	No	2	Negative	Eliciting Discussion
If functionality requires consent, it should be explicit, and truthful	✓	Yes	1	Positive	Eliciting Discussion
Ensure that demands for consent are explanatory and make sense to the user	✓	Yes	16	Positive	Problem Resolution
Ensure that consent collected is valid, informed, and genuine.	✓	Yes	12	Positive	Problem Resolution
Consider how users can improve their awareness of data use from the company and other users.	✓	Yes	8	Positive	Problem Understanding
Consider how users interact with personal data that is specific to only one user.		N/A	N/A	N/A	N/A
Consider what information you provide to users about personal data use.	✓	Yes	9	Positive	Problem Understanding
Consider the value of data to users, the company, attackers, bystanders and other users.	✓	Yes	10	Positive	Problem Resolution
Develop knowledge of imbalances, interests, and tensions which might cause conflict	✓	Yes	7	Positive	Problem Understanding
Develop knowledge of the additional uses and negative consequences of smart homes	✓	Yes	1	Positive	Problem Understanding
Develop knowledge of the abusability, and repurposing of smart home technologies	✓	Yes	10	Positive	Problem Resolution
Aim to design for the highest degree of assurance based on sensitive various functions	✓	Yes	4	Positive	Eliciting Discussion
Be aware that physical privacy properties are more trusted than software settings or indicated lights	✓	Yes	4	Neutral	Eliciting Discussion
Consolidate information related to the effectiveness of privacy settings indicators	✓	Yes	6	Neutral	Eliciting Discussion

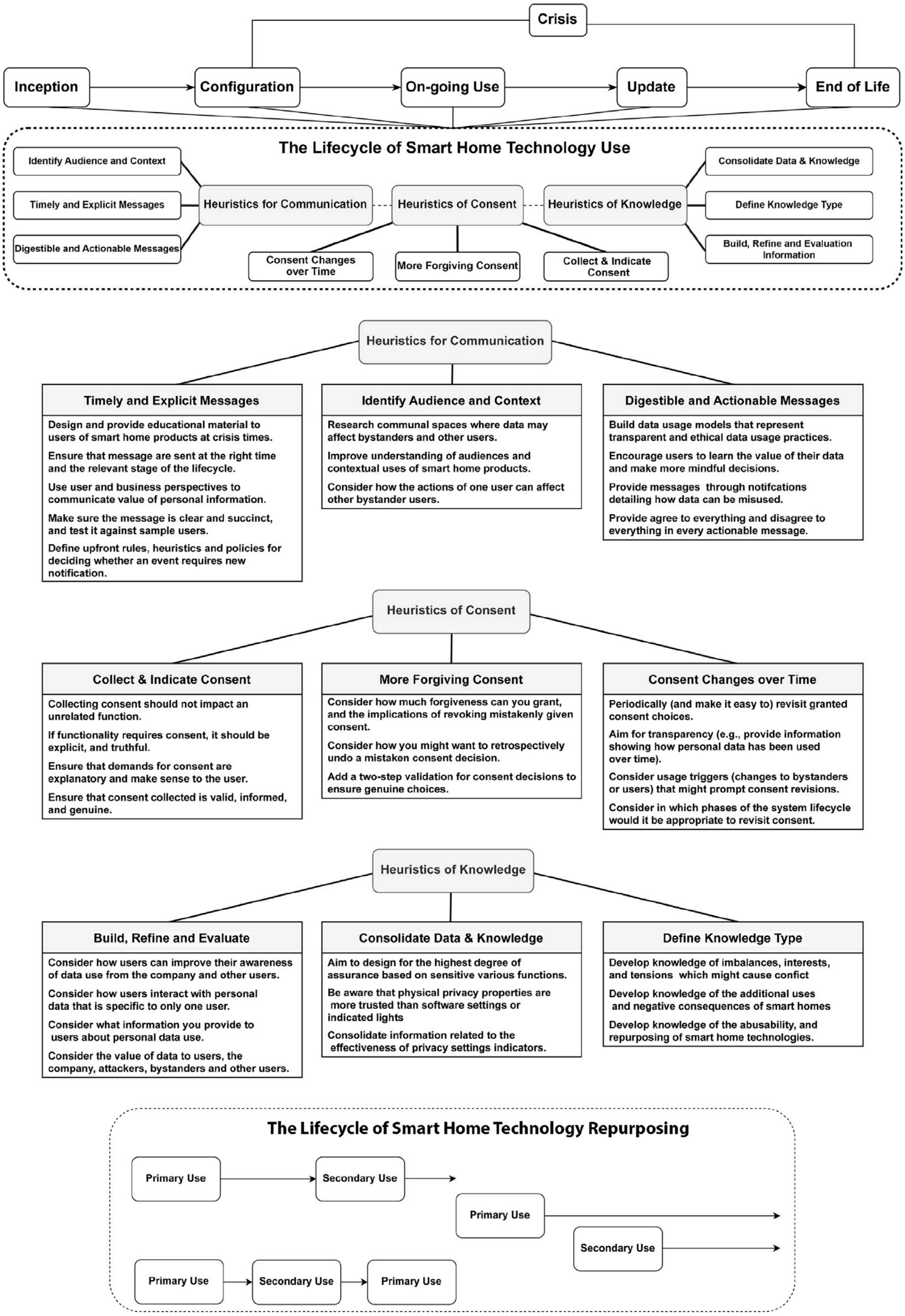
- Specific design rules: Guidelines that are specific to a particular product or service.
- Abstract design rules: Guidelines that are not specific to any particular product or service.
- High generalizability: Guidelines that can be applied to a wide range of products and services.

User Security:

- Authentication: The process of verifying the identity of a user.
- Authorization: The process of granting or denying access to a resource.
- Account management: The process of creating, managing, and closing user accounts.
- Password management: The process of creating, storing, and using strong passwords.
- Security updates: Updates that are released to fix security vulnerabilities.
- Security tools: Tools that are used to improve the security of a system.
- Security design: The process of designing a system that is secure.
- Security vulnerabilities: Weaknesses in a system that can be exploited by attackers.
- Security concerns: Issues that are related to the security of a system.
- Security breaches: Incidents in which unauthorized access is gained to a system.
- Security behaviors: The ways in which users interact with a system that can impact its security.
- Usable security: Security that is easy for users to understand and use.
- Unauthorized access: Access to a system that is gained by someone who is not authorized to have access.
- Data theft: The unauthorized copying or transfer of data.
- Access control: The process of controlling who has access to a system or resource.
- Secure by design: A security approach that involves designing a system with security in mind from the start.
- Security threats: Any action that can potentially cause harm to a system or its users.
- Security updates: Updates that are released to fix security vulnerabilities.

User Privacy:

- Privacy by design: An approach to developing information technology systems that protects privacy from the outset.
- Privacy design: The process of incorporating privacy protections into information technology systems.
- Consent management: The process of obtaining and managing consent from individuals for the collection, use, and sharing of their personal information.
- Data protection: The collection, use, and storage of personal information in a way that protects the privacy of individuals.
- Tracking: The collection of data about individuals' online activities, such as websites visited, pages viewed, and links clicked.
- Privacy tools: Tools that help individuals protect their privacy, such as privacy settings on social media platforms and encryption software.
- Privacy management: The process of individuals taking steps to control their personal information, such as choosing what information to share and with whom.
- Privacy control: The ability of individuals to control how their personal information is collected, used, and shared.
- Privacy perceptions: Individuals' beliefs and attitudes about privacy.
- Privacy challenges: The challenges of protecting privacy in the digital age, such as the increasing collection and use of personal data.


Crisis
Inception
Configuration
On-going Use
Update
End of Life
The Lifecycle of Smart Home Technology Use
Identify Audience and Context
Timely and Explicit Messages
Digestible and Actionable Messages
Heuristics for Communication
Heuristics of Consent
Heuristics of Knowledge
Consolidate Data & Knowledge
Define Knowledge Type
Build, Refine and Evaluation Information
Consent Changes over Time
More Forgiving Consent
Collect & Indicate Consent
Heuristics for Communication
Heuristics of Consent
Heuristics of Knowledge
The Lifecycle of Smart Home Technology Repurposing
Primary Use
Secondary Use
Primary Use
Secondary Use
Primary Use
Secondary Use
Primary Use

Timely and Explicit Messages

Design and provide educational material to users of smart home products at crisis times.

Ensure that message are sent at the right time and the relevant stage of the lifecycle.

Use user and business perspectives to communicate value of personal information.

Make sure the message is clear and succinct, and test it against sample users.

Define upfront rules, heuristics and policies for deciding whether an event requires new notification.

Identify Audience and Context

Research communal spaces where data may affect bystanders and other users.

Improve understanding of audiences and contextual uses of smart home products.

Consider how the actions of one user can affect other bystander users.

Digestible and Actionable Messages

Build data usage models that represent transparent and ethical data usage practices.

Encourage users to learn the value of their data and make more mindful decisions.

Provide messages through notifcations detailing how data can be misused.

Provide agree to everything and disagree to everything in every actionable message.

Collect & Indicate Consent

Collecting consent should not impact an unrelated function.

If functionality requires consent, it should be explicit, and truthful.

Ensure that demands for consent are explanatory and make sense to the user.

Ensure that consent collected is valid, informed, and genuine.

More Forgiving Consent

Consider how much forgiveness can you grant, and the implications of revoking mistakenly given consent.

Consider how you might want to retrospectively undo a mistaken consent decision.

Add a two-step validation for consent decisions to ensure genuine choices.

Consent Changes over Time

Periodically (and make it easy to) revisit granted consent choices.

Aim for transparency (e.g., provide information showing how personal data has been used over time).

Consider usage triggers (changes to bystanders or users) that might prompt consent revisions.

Consider in which phases of the system lifecycle would it be appropriate to revisit consent.

Build, Refine and Evaluate

Consider how users can improve their awareness of data use from the company and other users.

Consider how users interact with personal data that is specific to only one user.

Consider what information you provide to users about personal data use.

Consider the value of data to users, the company, attackers, bystanders and other users.

Consolidate Data & Knowledge

Aim to design for the highest degree of assurance based on sensitive various functions.

Be aware that physical privacy properties are more trusted than software settings or indicated lights

Consolidate information related to the effectiveness of privacy settings indicators.

Define Knowledge Type

Develop knowledge of imbalances, interests, and tensions which might cause confict

Develop knowledge of the additional uses and negative consequences of smart homes

Develop knowledge of the abusability, and repurposing of smart home technologies.

Fig. G.7. Detailed Version of the Design Heuristics Framework.

- Privacy attacks: Attempts to gain unauthorized access to or use of personal information.
- Privacy preferences: Individuals' preferences about how their personal information is collected, used, and shared.
- Privacy concerns: Individuals' worries about the privacy of their personal information.
- Privacy threats: Anything that could harm an individual's privacy, such as data breaches, identity theft, and government surveillance.
- Privacy behaviors: The ways in which individuals interact with the digital world in ways that affect their privacy, such as sharing personal information online or using privacy settings.

- Transparency: The openness and accountability of organizations that collect and use personal information.
- Privacy countermeasures: Measures that organizations can take to protect the privacy of individuals, such as implementing security measures and conducting privacy impact assessments.
- Trust: The belief that an organization will respect individuals' privacy.

Home Tech:

- Smart speakers: Voice-activated devices that can play music, answer questions, control smart home devices, and more.
- Smart cameras: Security cameras that can be connected to the internet and monitored remotely.
- Smart plugs: Electrical outlets that can be controlled by a smartphone or other device.
- Smart bulbs: Light bulbs that can be controlled by a smartphone or other device.
- Smart kitchen: A kitchen that is equipped with smart appliances and devices.
- Smart thermostats: Thermostats that can be controlled by a smartphone or other device.
- Smartphones: Mobile phones that are equipped with a variety of features, such as a camera, internet access, and a GPS.
- Smart alarms: Alarms that can be controlled by a smartphone or other device.
- Smart doorbells: Doorbells that have a camera and can be used to see who is at the door without having to get up.
- Smart hubs: Devices that connect to other smart home devices and allow them to be controlled together.
- Smart door locks: Locks that can be locked and unlocked by a smartphone or other device.
- Smart ecosystem: A group of smart home devices that are all compatible with each other and can be controlled together.
- Home cameras: Security cameras that are installed in the home.
- Motion sensors: Sensors that detect movement and can be used to trigger smart home devices, such as lights or alarms.
- Microphones: Devices that can be used to record sound.
- Smart home assistants: Voice-activated assistants that can be used to control smart home devices and answer questions.
- Smart heaters: Heaters that can be controlled by a smartphone or other device.
- Smart displays: Devices that have a screen and can be used to control smart home devices, view security footage, and more.
- Smart watches: Wearable devices that can be used to track fitness, receive notifications, and more.

Appendix D. Concept definitions

- Heuristics: The concept refers to mental shortcuts or strategies that individuals use to solve problems or make judgments quickly, often relying on past experiences or general rules of thumb.
- Communication: This concept refers to the exchange of information or ideas between individuals or groups through various channels such as speech, writing, or non-verbal cues.
- Permission: This concept refers to the act of obtaining consent or authorization from individuals or entities before engaging in certain activities such as accessing personal information, using data, or sharing content.
- Consent: This concept refers to the voluntary agreement or permission given by an individual to participate in a specific activity or to have their personal information used for a particular purpose.
- Security: This concept refers to the practice of safeguarding internet-connected systems including hardware, software, and data from digital attacks, damage, or unauthorized access.
- Privacy: This concept refers to an individual's right to control the collection, use, and dissemination of their personal data or information.
- Knowledge: This concept refers to the range of understanding or awareness a person has acquired through experience or education. It encompasses facts, information, skills, and concepts understood by an individual or community.

Appendix E. Conceptual framework analysis papers

In this appendix section, we present the papers used in our Conceptual Framework Analysis. Each paper was categorized in one or more categories from: user experience, design guidelines, user security, user privacy and home tech.

We used the term "user privacy" to encompass the privacy of users in a broader sense. As a result, the term factors broader stakeholders such as primary users (e.g., passengers, operators) and secondary users (e.g., other vessels, bystanders) (see Table E.4).

Appendix F. Heuristics evaluation

We present the evaluation of our heuristics below.

Appendix G. Framework of design heuristics

See Fig. G.7.

References

Abdi, N., Ramokapane, K.M., Such, J.M., 2019. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In: Fifteenth Symposium on Usable Privacy and Security. SOUPS 2019.

Aldrich, F.K., 2003. Smart homes: Past, present and future. In: Harper, R. (Ed.), Inside the Smart Home. Springer, London, pp. 17–39.

Allegue, S., Rhahla, M., Abdellatif, T., 2019. Toward gdpr compliance in iot systems. In: International Conference on Service-Oriented Computing. Springer, pp. 130–141.

Apthorpe, N., Reisman, D., Feamster, N., 2017. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. arXiv preprint arXiv:1705.06805.

Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., Feamster, N., 2018. Discovering smart home internet of things privacy norms using contextual integrity. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2 (2), 59.

Arhippainen, L., 2013. A tutorial of ten user experience heuristics. In: Proceedings of International Conference on Making Sense of Converging Media. pp. 336–337.

Associates, P., 2019. Parks associates: Privacy concerns increasing among smart home device owners. GlobeNewswire News Room.

Atzori, L., Iera, A., Morabito, G., 2010. The internet of things: A survey. Comput. Netw. 54 (15), 2787–2805.

Barocas, S., Nissenbaum, H., 2009. On notice: The trouble with notice and consent. In: Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information.

Bastos, D., Giubilo, F., Shackleton, M., El-Moussa, F., 2018. GDPR privacy implications for the Internet of Things.

Bergman, J., Olsson, T., Johansson, I., Rassmus-Gröhn, K., 2018. An exploratory study on how Internet of Things developing companies handle user experience requirements. In: International Working Conference on Requirements Engineering: Foundation for Software Quality. Springer, pp. 20–36.

Bösch, C., Erb, B., Kargl, F., Kopp, H., Pfattheicher, S., 2016. Tales from the dark side: Privacy dark strategies and privacy dark patterns. Proc. Priv. Enhanc. Technol. 2016 (4), 237–254.

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qual. Res. Psychol. 3 (2), 77–101. http://dx.doi.org/10.1191/1478088706qp063oa, Publisher: Routledge _eprint: https://www.tandfonline.com/doi/pdf/10.1191/1478088706qp063oa, URL https://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa.

Brush, A.B., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S., Dixon, C., 2011. Home automation in the wild: challenges and opportunities. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '11, Association for Computing Machinery, Vancouver, BC, Canada, pp. 2115–2124. http://dx.doi.org/10.1145/1978942.1979249.

Carley, K., 1993. Coding choices for textual analysis: A comparison of content analysis and map analysis. Sociol. Methodol. 23, 75–126. http://dx.doi.org/10.2307/271007, URL https://www.jstor.org/stable/271007.

Chalhoub, G., 2020. The UX of things: Exploring UX principles to inform security and privacy design in the smart home. In: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems. In: CHI EA '20, Association for Computing Machinery, New York, NY, USA, pp. 1–6. http://dx.doi.org/10.1145/3334480.3381436.

Chalhoub, G., Flechais, I., 2020. "Alexa, are you spying on me?": Exploring the effect of user experience on the security and privacy of smart speaker users. In: Moallem, A. (Ed.), HCI for Cybersecurity, Privacy and Trust. In: Lecture Notes in Computer Science, Springer International Publishing, Cham, pp. 305–325.

Chalhoub, G., Flechais, I., Nthala, N., Abu-Salma, R., 2020a. Innovation inaction or in action? The role of user experience in the security and privacy design of smart home cameras. In: Sixteenth Symposium on Usable Privacy and Security. SOUPS 2020, USENIX Association, pp. 185–204.

Chalhoub, G., Flechais, I., Nthala, N., Abu-Salma, R., Tom, E., 2020b. Factoring user experience into the security and privacy design of smart home devices: A case study. In: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems. In: CHI EA '20, Association for Computing Machinery, New York, NY, USA, pp. 1–9. http://dx.doi.org/10.1145/3334480.3382850.

Chalhoub, G., Kraemer, M.J., Nthala, N., Flechais, I., 2021. 'It did not give me an option to decline': A longitudinal analysis of the user experience of security and privacy in smart home products. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. CHI '21, Association for Computing Machinery, New York, NY, USA, pp. 1–16. http://dx.doi.org/10.1145/3411764.3445691.

Chalmers, M., Galani, A., 2004. Seamful interweaving: Heterogeneity in the theory and design of interactive systems. In: Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques. DIS '04, Association for Computing Machinery, New York, NY, USA, pp. 243–252. http://dx.doi.org/10.1145/1013115.1013149.

Chaudhuri, A., 2016. Internet of things data protection and privacy in the era of the general data protection regulation. J. Data Prot. Priv. 1 (1), 64–75.

Choe, E.K., Consolvo, S., Jung, J., Harrison, B., Patel, S.N., Kientz, J.A., 2012. Investigating receptiveness to sensing and inference in the home using sensor proxies. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing. UbiComp '12, Association for Computing Machinery, Pittsburgh, Pennsylvania, pp. 61–70. http://dx.doi.org/10.1145/2370216.2370226.

Cobb, C., Bhagavatula, S., Garrett, K.A., Hoffman, A., Rao, V., Bauer, L., 2021. "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. Proc. Priv. Enhanc. Technol. 2021 (4), 54–75. http://dx.doi.org/10.2478/popets-2021-0060, URL https://www.sciendo.com/article/10.2478/popets-2021-0060.

Collins, J., 2004. Education techniques for lifelong learning: giving a PowerPoint presentation: the art of communicating effectively. Radiographics 24 (4), 1185–1192.

Conti, G., Sobiesk, E., 2010. Malicious interface design: exploiting the user. In: Proceedings of the 19th International Conference on World Wide Web. WWW '10, Association for Computing Machinery, New York, NY, USA, pp. 271–280. http://dx.doi.org/10.1145/1772690.1772719.

Corbin, J., Strauss, A., 2014. Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Sage publications.

Corbin, J., Strauss, A., 2015. Basics of Qualitative Research. SAGE, Google-Books-ID: Dc45DQAAQBAJ.

Cox, A.L., Gould, S.J., Cecchinato, M.E., Iacovides, I., Renfree, I., 2016. Design frictions for mindful interactions: The case for microboundaries. In: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems. In: CHI EA '16, Association for Computing Machinery, New York, NY, USA, pp. 1389–1397. http://dx.doi.org/10.1145/2851581.2892410.

Crabtree, A., Mortier, R., Rodden, T., Tolmie, P., 2012. Unremarkable networking: the home network as a part of everyday life. In: Proceedings of the Designing Interactive Systems Conference. ACM.. pp. 554–563. http://dx.doi.org/10.1145/2317956.2318039, URL http://dl.acm.org/citation.cfm?id=2318039.

Davidoff, S., Lee, M.K., Yiu, C., Zimmerman, J., Dey, A.K., 2006. Principles of smart home control. In: Dourish, P., Friday, A. (Eds.), UbiComp 2006: Ubiquitous Computing. In: Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, pp. 19–34.

Dreyfus, S.E., Dreyfus, H.L., 1980. A Five-Stage Model of the Mental Activities Involved in Directed Skill Acquisition. Tech. Rep., California Univ Berkeley Operations Research Center.

Follett, J., 2014. Designing for Emerging Technologies: UX for Genomics, Robotics, and the Internet of Things. O'Reilly Media, Inc.

Freed, D., Havron, S., Tseng, E., Gallardo, A., Chatterjee, R., Ristenpart, T., Dell, N., 2019. "Is my phone hacked?" analyzing clinical computer security interventions with survivors of intimate partner violence. Proc. ACM Hum.-Comput. Interact. 3 (CSCW), 1–24. http://dx.doi.org/10.1145/3359304.

Friedman, B., Felten, E., Millett, L.I., 2000. Informed Consent Online: A Conceptual Model and Design Principles. University of Washington Computer Science & Engineering Technical Report 00–12–2, Vol. 8.

Garg, R., Moreno, C., 2019. Understanding motivators , constraints , and practices of sharing internet of things. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 3 (2), 1–21. http://dx.doi.org/10.1145/3328915.

Geeng, C., Roesner, F., 2019. Who's in control? Interactions in multi-user smart homes. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. CHI '19, Association for Computing Machinery, New York, NY, USA, http://dx.doi.org/10.1145/3290605.3300498

Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., Baldini, G., 2017. Security and privacy issues for an IoT based smart home. In: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics. MIPRO, pp. 1292–1297. http://dx.doi.org/10.23919/MIPRO.2017.7973622.

George Chalhoub, Ivan Flechais, 2022. Data protection at a discount: Investigating the UX of data protection from user, designer, and business leader perspectives. In: The 25th ACM Conference on Computer-Supported Cooperative Work and Social Computing. CSCW 2022.

Gopavaram, S., 2019. IoTMarketplace : Informing purchase decisions with risk communication.

Gray, C.M., Kou, Y., Battles, B., Hoggatt, J., Toombs, A.L., 2018. The dark (patterns) side of UX design. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. CHI '18, Association for Computing Machinery, New York, NY, USA, pp. 1–14. http://dx.doi.org/10.1145/3173574.3174108.

Gray, C.M., Santos, C., Bielova, N., Toth, M., Clifford, D., 2021. Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. CHI '21, Association for Computing Machinery, New York, NY, USA, pp. 1–18. http://dx.doi.org/10.1145/3411764.3445779.

Guba, E.G., Lincoln, Y.S., et al., 1994. Competing paradigms in qualitative research. Handb. Qual. Res. 2 (163–194), 105.

Guest, G., Bunce, A., Johnson, L., 2006. How many interviews are enough? An experiment with data saturation and variability. Field methods 18 (1), 59–82.

Hadan, H., Serrano, N., Das, S., Camp, L.J., 2019. Making IoT Worthy of Human Trust. SSRN Scholarly Paper ID 3426871, Social Science Research Network, Rochester, NY, URL https://papers.ssrn.com/abstract=3426871.

Hargreaves, T., Wilson, C., Hauxwell-Baldwin, R., 2018. Learning to live in a smart home. Build. Res. Inf. 46, 127–139. http://dx.doi.org/10.1080/09613218.2017.1286882.

Hartson, R., Pyla, P., 2012. The UX Book: Process and Guidelines for Ensuring a Quality User Experience. Elsevier Science, URL https://books.google.co.uk/books?id=w4I3Y64SWLoC.

Hartzog, W., 2018. Privacy's Blueprint: The Battle to Control the Design of New Technologies. Harvard University Press, URL https://books.google.de/books?id=YERMDwAAQBAJ.

Huvila, I., Anderson, T.D., Jansen, E.H., McKenzie, P., Westbrook, L., Worrall, A., 2014. Boundary objects in information science research: An approach for explicating connections between collections, cultures and communities. Proc. Am. Soc. Inf. Sci. Technol. 51 (1), 1–4. http://dx.doi.org/10.1002/meet.2014.14505101003, arXiv:https://asistdl.onlinelibrary.wiley.com/doi/pdf/10.1002/meet.2014.14505101003.

Information Commissioner Office, 2019. Data protection by design and default. ICO, URL https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/.

Jabareen, Y., 2009. Building a conceptual framework: Philosophy, definitions, and procedure. Int. J. Qual. Methods 8 (4), 49–62. http://dx.doi.org/10.1177/160940690900800406.

Jenkins, M., 2004. Evaluation of methodological search filters—a review. Health Inf. Libr. J. 21 (3), 148–163. http://dx.doi.org/10.1111/j.1471-1842.2004.00511.x.

Keane, E., 2018. The GDPR and employee's privacy: Much ado but nothing new. King's Law J. 29 (3), 354–363, Publisher: Taylor & Francis.

Koops, B.-J., 2015. The concepts, approaches, and applications of responsible innovation. In: Koops, B.-J., Oosterlaken, I., Romijn, H., Swierstra, T., van den Hoven, J. (Eds.), Responsible Innovation 2: Concepts, Approaches, and Applications. Springer International Publishing, Cham, pp. 1–15.

Kraemer, M.J., Flechais, I., Webb, H., 2019. Exploring communal technology use in the home. In: Proceedings of the Halfway To the Future Symposium 2019. In: HTTF 2019, ACM, New York, NY, USA, http://dx.doi.org/10.1145/3363384.3363389.

Kuniavsky, M., 2003. Observing the User Experience: A Practitioner's Guide to User Research. In: Interactive Technologies, Elsevier Science, URL https://books.google.co.uk/books?id=1tE4Skp9pI8C.

Kuniavsky, M., 2010. Smart Things: Ubiquitous Computing User Experience Design. Elsevier Science, URL https://books.google.co.uk/books?id=-WLyUCBBUVAC.

Lallemand, C., Gronier, G., Koenig, V., 2015. User experience: A concept without consensus? Exploring practitioners' perspectives through an international survey. Comput. Hum. Behav. 43, 35–48. http://dx.doi.org/10.1016/j.chb.2014.10.048.

Lallemand, C., Koenig, V., Gronier, G., 2014. How relevant is an expert evaluation of user experience based on a psychological needs-driven approach? In: Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational. NordiCHI '14, Association for Computing Machinery, New York, NY, USA, pp. 11–20. http://dx.doi.org/10.1145/2639189.2639214.

Lane, M., 2020. Responsible innovation: The next wave of design thinking. Microsoft Design, URL https://medium.com/microsoft-design/responsible-innovation-the-next-wave-of-design-thinking-86bc9e9a8ae8.

Leitão, R., 2019. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In: Proceedings of the 2019 on Designing Interactive Systems Conference. ACM, http://dx.doi.org/10.1145/3322276.3322366.

Levy, K., Schneier, B., 2020. Privacy threats in intimate relationships. J. Cybersecur. 6 (1), tyaa006.

Low, S., 2016. Spatializing Culture: The Ethnography of Space and Place. Taylor & Francis, URL https://books.google.co.uk/books?id=KCQlDwAAQBAJ.

Luger, E., Urquhart, L., Rodden, T., Golembewski, M., 2015. Playing the legal card: Using ideation cards to raise data protection issues within the design process. Conf. Hum. Factors Comput. Syst. - Proc. 2015-April, 457–466. http://dx.doi.org/10.1145/2702123.2702142.

Luguri, J., Strahilevitz, L.J., 2021. Shining a light on dark patterns. J. Leg. Anal. 13 (1), 43–109. http://dx.doi.org/10.1093/jla/laaa006, arXiv:https://academic.oup.com/jla/article-pdf/13/1/43/36669915/laaa006.pdf.

Mare, S., Girvin, L., Roesner, F., Kohno, T., 2019. Consumer smart homes: Where we are and where we need to go. In: Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications. HotMobile '19, Association for Computing Machinery, Santa Cruz, CA, USA, pp. 117–122. http://dx.doi.org/10.1145/3301293.3302371.

Mathur, A., Acar, G., Friedman, M.J., Lucherini, E., Mayer, J., Chetty, M., Narayanan, A., 2019. Dark patterns at scale: Findings from a crawl of 11k shopping websites. Proc. ACM Hum.-Comput. Interact. 3 (CSCW), 1–32.

McHugh, M.L., 2012. Interrater reliability: the kappa statistic. Biochem. Med. 22 (3), 276–282, Publisher: Medicinska naklada.

McKay, D., Miller, C., 2021. Standing in the way of control: A call to action to prevent abuse through better design of smart home technologies. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. ACM

Mohan, J., Wasserman, M., Chidambaram, V., 2019. Analyzing GDPR compliance through the lens of privacy policy. In: Gadepally, V., Mattson, T., Stonebraker, M., Wang, F., Luo, G., Laing, Y., Dubovitskaya, A. (Eds.), Heterogeneous Data Management, Polystores, and Analytics for Healthcare. In: Lecture Notes in Computer Science, Springer International Publishing, Cham, pp. 82–95.

Morgner, P., Benenson, Z., 2018. Exploring security economics in IoT standardization efforts. arXiv preprint arXiv:1810.12035.

Morgner, P., Mai, C., Koschate-Fischer, N., Freiling, F., Benenson, Z., 2020. Security update labels: Establishing economic incentives for security patching of IoT consumer products. In: 2020 IEEE Symposium on Security and Privacy. SP, (ISSN: 2375-1207) pp. 429–446. http://dx.doi.org/10.1109/SP40000.2020.00021.

Morse, J.M., Mitcham, C., 2002. Exploring qualitatively-derived concepts: Inductive—Deductive pitfalls. Int. J. Qual. Methods 1 (4), 28–35. http://dx.doi.org/10.1177/160940690200100404.

Morse, J.M., Richards, L., 2002. Readme First for a User's Guide to Qualitative Methods. SAGE Publications, Incorporated.

Muller, M., 2003. Participatory design: The third space in HCI. Hum.-Comput. Inter. Handb. 4235 (January 2002), 1051–1068. http://dx.doi.org/10.1145/153571.255960.

Mulligan, D.K., King, J., 2011. Bridging the gap between privacy and design. U. Pa. J. Const. L. 14, 989–1034.

Naeini, P.E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L.F., Sadeh, N., 2017. Privacy expectations and preferences in an IoT world. In: Thirteenth Symposium on Usable Privacy and Security. ${$SOUPS$}$ 2017, pp. 399–412.

Nielsen, J., 1994. Usability inspection methods. In: Conference Companion on Human Factors in Computing Systems. pp. 413–414.

Nielsen, J., 2009. Discount usability: 20 years. Jakob Nielsen's Alertbox Available at http://www.useit.com/alertbox/discount-usability.html. (Accessed 23 January 2012).

Oh, J., Lee, U., 2015. Exploring UX issues in quantified self technologies. In: 2015 Eighth International Conference on Mobile Computing and Ubiquitous Networking. ICMU, pp. 53–59. http://dx.doi.org/10.1109/ICMU.2015.7061028.

Owen, R., Stilgoe, J., Macnaghten, P., Gorman, M., Fisher, E., Guston, D., 2013. A framework for responsible innovation. In: Responsible Innovation. John Wiley & Sons, Ltd, pp. 27–50. http://dx.doi.org/10.1002/9781118551424.ch2, section: 2 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118551424.ch2, URL https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118551424.ch2.

Ramokapane, K.M., Bird, C., Rashid, A., Chitchyan, R., 2022. Privacy design strategies for home energy management systems (HEMS). In: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. CHI '22, Association for Computing Machinery, New York, NY, USA, pp. 1–15. http://dx.doi.org/10.1145/3491102.3517515.

Regulation, G.D.P., 2018. General data protection regulation (GDPR). Intersoft Consult. 24 (1), Accessed in October.

Schaffer, E., Lahiri, A., 2013. Institutionalization of UX: A Step-By-Step Guide to a User Experience Practice. Addison-Wesley, Google-Books-ID: XIpTAgAAQBAJ.

Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F., 2015. A design space for effective privacy notices. In: Eleventh Symposium on Usable Privacy and Security. ${$SOUPS$}$ 2015, pp. 1–17.

Schechner, N.K., Sam, 2019. GDPR has been a boon for google and facebook. Wall Street J.

Schraefel, M., Gomer, R., Gerding, E., Maple, C., 2020. Rethinking transparency for the internet of things. In: Life and the Law in the Era of Data-Driven Agency. Edward Elgar Publishing, Cheltenham, UK.

Schwartz, B., Ward, A., 2004. Doing better but feeling worse: The paradox of choice. Posit. Psychol. Pract. 86, 104.

Seale, C., 1999. Quality in qualitative research. Qual. Inq. 5 (4), 465–478.

Seymour, W., Kraemer, M.J., Binns, R., Van Kleek, M., 2020. Informing the design of privacy-empowering tools for the connected home. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. CHI '20, Association for Computing Machinery, New York, NY, USA, pp. 1–14. http://dx.doi.org/10.1145/3313831.3376264.

Shao, X., Oinas-Kukkonen, H., 2019. How does GDPR (general data protection regulation) affect persuasive system design: Design requirements and cost implications. In: Oinas-Kukkonen, H., Win, K.T., Karapanos, E., Karppinen, P., Kyza, E. (Eds.), Persuasive Technology: Development of Persuasive and Behavior Change Support Systems. In: Lecture Notes in Computer Science, Springer International Publishing, Cham, pp. 168–173.

Shirehjini, A.A.N., Semsar, A., 2017. Human interaction with IoT-based smart environments. Multimedia Tools Appl. 76 (11), 13343–13365.

Sobers, R., 2019. GDPR's impact so far: Must-know stats and takeaways - Varonis. Inside Out Secur. Section: Compliance & Regulation, URL https://www.varonis.com/blog/gdpr-effect-review/.

Soe, T.H., Nordberg, O.E., Guribye, F., Slavkovik, M., 2020. Circumvention by design - dark patterns in cookie consent for online news outlets. In: Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society. NordiCHI '20, Association for Computing Machinery, New York, NY, USA, pp. 1–12. http://dx.doi.org/10.1145/3419249.3420132.

Spartz, J.M., Weber, R.P., 2016. User experience as a driver of entrepreneurial innovation. In: 2016 IEEE International Professional Communication Conference. IPCC, pp. 1–7. http://dx.doi.org/10.1109/IPCC.2016.7740486.

Speed, C., Luger, E., 2019. Sensing data in the home. In: Schnädelbach, H., Kirk, D. (Eds.), People, Personal Data and the Built Environment. Springer International Publishing, Cham, pp. 123–142.

Stilgoe, J., Owen, R., Macnaghten, P., 2020. Developing a Framework for Responsible Innovation*. Routledge, pp. 347–359. http://dx.doi.org/10.4324/9781003075028-22, Publication Title: The Ethics of Nanotechnology, Geoengineering, and Clean Energy, URL https://www.taylorfrancis.com/chapters/edit/10.4324/9781003075028-22/developing-framework-responsible-innovation-jack-stilgoe-richard-owen-phil-macnaghten.

Swan, J.E., Combs, L.J., 1976. Product performance and consumer satisfaction: A new concept: An empirical study examines the influence of physical and psychological dimensions of product performance on consumer satisfaction. J. Mark. 40 (2), 25–33. http://dx.doi.org/10.1177/002224297604000206.

Thomas, M.O., Onyimbo, B.A., Logeswaran, R., 2016. Usability evaluation criteria for internet of things. Int. J. Inf. Technol. Comput. Sci. 8, 10–18.

Urquhart, L., Chen, J., 2020a. On the Principle of Accountability: Challenges for Smart Homes & Cybersecurity. SSRN Scholarly Paper ID 3629119, Social Science Research Network, Rochester, NY, URL https://papers.ssrn.com/abstract=3629119.

Urquhart, L., Chen, J., 2020b. Stuck in the middle with U (sers): Domestic data controllers & demonstrations of accountability in smart homes. In: ETHICOMP 2020. p. 211.

Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T., 2019. (Un)informed consent: Studying GDPR consent notices in the field. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. CCS '19, Association for Computing Machinery, New York, NY, USA, pp. 973–990. http://dx.doi.org/10.1145/3319535.3354212.

van Oorschot, R., Snelders, D., Kleinsmann, M., Buur, J., 2022. Participation in design research. Des. Stud. 78, 101073. http://dx.doi.org/10.1016/j.destud.2021.101073, URL https://www.sciencedirect.com/science/article/pii/S0142694X21000843.

Veil, W., 2018. The GDPR: The Emperor's New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law. SSRN Scholarly Paper ID 3305056, Social Science Research Network, Rochester, NY, URL https://papers.ssrn.com/abstract=3305056.

von Schomberg, R., 2013. A vision of responsible research and innovation. In: Responsible Innovation. John Wiley & Sons, Ltd, pp. 51–74. http://dx.doi.org/10.1002/9781118551424.ch3, section: 3 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118551424.ch3, URL https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118551424.ch3.

Walker, L.O., Avant, K.C., 2005. Strategies for Theory Construction in Nursing, Vol. 4. Pearson/Prentice Hall Upper Saddle River, NJ.

Williams, M., Nurse, J.R., Creese, S., 2017. Privacy is the boring bit: user perceptions and behaviour in the internet-of-things. In: 2017 15th Annual Conference on Privacy, Security and Trust. PST, IEEE, pp. 181–18109.

Wilson, C., Hargreaves, T., Hauxwell-Baldwin, R., 2015. Smart homes and their users: a systematic analysis and key challenges. Pers. Ubiquitous Comput. 19 (2), 463–476.

Wilson, C., Hargreaves, T., Hauxwell-Baldwin, R., 2017. Benefits and risks of smart home technologies. Energy Policy 103, 72–83.

Wong, R.Y., Mulligan, D.K., 2019. Bringing design to the privacy table: Broadening "design" in "privacy by design" through the lens of HCI. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. CHI '19, Association for Computing Machinery, New York, NY, USA, http://dx.doi.org/10.1145/3290605.3300492.

Yao, Y., 2019. Designing for better privacy awareness in smart homes. In: Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing. CSCW '19, Association for Computing Machinery, New York, NY, USA, pp. 98–101. http://dx.doi.org/10.1145/3311957.3361863.

Yao, Y., Basdeo, J.R., Kaushik, S., Wang, Y., 2019a. Defending my castle: A co-design study of privacy mechanisms for smart homes. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 1–12, URL DOI:10.1145/3290605.3300428.

Yao, Y., Basdeo, J.R., Mcdonough, O.R., Wang, Y., 2019b. Privacy perceptions and designs of bystanders in smart. Proc. ACM Hum.-Comput. Interact. 3 (CSCW), 1–24. http://dx.doi.org/10.1145/3359161.

Zeng, E., Roesner, F., 2019. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In: 28th USENIX Security Symposium. USENIX Security 19, pp. 159–176.

Zheng, S., Apthorpe, N., Chetty, M., Feamster, N., 2018. User perceptions of smart home IoT privacy. Proc. ACM Hum.-Comput. Interact. 2 (CSCW), 200.