Data Protection at a Discount: Investigating the UX of Data Protection from User, Designer, and Business Leader Perspectives

GEORGE CHALHOUB, University of Oxford, UK
IVAN FLECHAIS, University of Oxford, UK

Smart homes are dangerous – a sentiment arising from prior research exploring the user experience (UX) of data protection for smart home devices. While this research has explored data protection shortcomings for users, UX is a designed encounter reconciling development, economic, compliance and strategic business priorities. And so, in addition to studying user perspectives, there is a gap in understanding how designers and business leaders influence the UX of data protection. To address this gap, we study smart home users, designers and business leaders, exploring how they experience data protection interactions, regulation, and processes. Our findings confirm that users have poor data protection interactions (e.g., consent and data access requests). We also find that business leaders and designers experience difficulties in identifying, applying, and tailoring suitable processes and practices for data protection for which some have developed "discount data protection": shortcuts, heuristics, and common sense practices to overcome these challenges.

CCS Concepts: • **Security and privacy** → **Privacy protections**; Usability in security and privacy; • **Human-centered computing** → *Empirical studies in HCI*.

Additional Key Words and Phrases: smart home, user experience, data protection, consent

ACM Reference Format:
George Chalhoub and Ivan Flechais. 2022. Data Protection at a Discount: Investigating the UX of Data Protection from User, Designer, and Business Leader Perspectives. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 436 (November 2022), 36 pages. https://doi.org/10.1145/3555537

1 INTRODUCTION

The allure of the smart home is powerful: simple voice commands can raise window shades, change home temperatures, and turn on the coffee maker. Smart homes can save time, increase personal productivity, and provide a level of convenience for households. And yet the convenience comes at a cost: more data pertaining to private home spaces is created, processed, and shared outside the home [187].

To ensure the privacy and protection of this data, regulations (e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA)) have been introduced and refined. In spite of the aims of such regulation, its introduction has resulted in a number of negative experiences: e.g., the introduction of GDPR in 2018 resulted in the malfunction or even discontinuation of thousands of smart home products [37]. Yeelight, a prominent light bulb manufacturer sent a notice to its EU customers saying: "*According to GDPR, we will not be able to continue to provide this service*

Authors' addresses: George Chalhoub, george.chalhoub@cs.ox.ac.uk, University of Oxford, Department of Computer Science, Wolfson Building, Parks Road, Oxford, UK, OX1 3QD; Ivan Flechais, ivan.flechais@cs.ox.ac.uk, University of Oxford, Department of Computer Science, Wolfson Building, Parks Road, Oxford, UK, OX1 3QD.

2573-0142/2022/11-ART436 $15.00
https://doi.org/10.1145/3555537

to you." [123]. Moreover, the proliferation of persuasive practices such as dark patterns aimed at gaining consent over data usage has further made the experience of data protection a confusing and unpleasant affair [85, 141, 166, 169]. Dark patterns subversively steer users into consenting to data collection, making it harder to reject consent by hiding away privacy-friendly options and pre-ticking boxes [3, 40, 49, 51, 84, 129]. Previous CHI research found dark patterns in 88% of the top 10,000 websites in the UK [148].

Previous studies have emphasized the need for research to improve the User eXperience (UX) of data protection in smart home products. The international standard of human-system interaction (ISO 9241-210) defines UX [65] as "*a person's perceptions and responses that result from the use or anticipated use of a product, system or service.*" Smart homes products collect real-time, contextual and increasingly detailed data about the lives of home users [16, 53, 154, 187]. Commercial smart products such as security cameras and baby monitors use consumer data for their own purposes and disclose sensitive data (e.g., location data, health data, voice recordings) to third parties [38, 78, 156]. Smart homes often have constrained interactions because they often lack interfaces. As a result, designing user-friendly data protection interactions in smart homes is challenging [48, 116].

There has been an increased focus on data protection user experiences (e.g., consent interactions) for users [14, 40, 49, 61, 84, 127, 129, 179], however this largely overlooks the importance of both design challenges and business perspectives in the whole data protection experience. The UX of data protection is a designed encounter which encompasses contextual, economic, compliance and strategic business priorities [114, 160, 170]. Despite that, there has been little research into the UX of data protection for the designer's perspectives [43], and even less research exploring how business leaders experience the practicalities and challenges of data protection [127]. This has created the need to explore bridges between user needs and business goals [137, 170].

To gain a wider understanding into data protection, our research aims to explore data protection experiences (e.g., consent interactions) for users, designers and business leaders in the context of smart homes in the UK. Our overarching research question is: **RQ:** How can we understand and support the UX of data protection in smart homes from the perspective of users, designers, and business leaders? We break this down into three further questions: (i) **RQ1:** How do smart home users experience and perceive data protection interactions (e.g., consent) in smart homes? (ii) **RQ2:** What are the challenges and practices of data protection compliance of smart home designers and business leaders? Based on this, (iii) **RQ3:** How can we identify and improve data protection practices that fit the needs of smart home business leaders and designers, and provide better solutions for users?

In order to answer these questions, we conducted qualitative semi-structured in-depth interviews with smart home users (n=7), business leaders (n=6) and designers (n=6). We analyzed the interviews using Grounded Theory (GT) and provided a detailed account of (i) users experiencing consent interactions and exercising their legal rights, (ii) business leaders navigating data protection requirements and, (iii) designers addressing data protection during design stages. We summarize our key findings about each user group below:

- Smart home *users* experienced dark patterns when providing consent and exercising their legal rights. They didn't know how their data was collected and used, experienced imbalances in the data-value exchange process and perceived smart home data protection interactions to be manipulative and meaningless (see Section 4.1).
- Smart home *business leaders* perceived data protection costs to be unfair to smaller businesses due to lacking necessary resources and facing unrecognized smart home compliance costs. As a result, they took '*necessary shortcuts*' to comply with data protection and outsourced some of their duties to third parties (see Section 4.2).

- Smart home *designers* faced obstacles to aligning UX efforts (e.g., advocating user needs) with business goals, and pressure from rapid smart home development needs. As such, they used heuristics (e.g., rules of thumb), best practices and tried-and-tested solutions to navigate data protection design requirements (see Section 4.3).

The rest of the paper is organized as follows: we discuss related work in Section 2; we describe the methodology followed in this study in Section 3; in Section 4, we present the findings of our study; we discuss the findings in Section 5; we conclude the paper and distill design recommendations in Section 6.

2 LITERATURE REVIEW

2.1 User Studies in Data Protection

Before GDPR was implemented, studies of privacy policies and seeking user consent to data processing have been ongoing for nearly two decades [161]. A substantial body of research has explored the experiences of privacy policies and notices (e.g., [18, 54, 72, 99]), novel privacy notification tools (e.g., [55, 105, 106]), and technical means to support privacy notice interfaces (e.g., [2, 117]). The increasing adoption of wearable devices and smart home products has resulted in interactions that are constrained (e.g., lack of interfaces). As such, finding user-friendly privacy notices for wearable and smart home products is difficult [48, 116].

Research suggests that consent interactions and privacy notices generally don't function well: users tend to ignore impactful privacy notices [87, 183], perceive them as a privacy threat [111] and are accustomed to "clicking away" consent interactions [39]. To improve consent interactions, researchers looked into improving mobile application notification permission requests. They found that nearly half of permission requests can be automated which resulted in decreased user attention [70]. Machuletz and Böhme [127] suggested that GDPR-compliant consent permissions requests can similarly be automated. However, research into automating GDPR privacy notices is under-explored.

Since GDPR came into effect, many studies have investigated its impact on smart home users and devices [13, 21, 45, 57, 59, 73, 81, 94, 97, 103, 121, 177, 178]. More research emerged into facilitating GDPR-compliant consent notices. Ulbricht and Pallas [176] presented a privacy preference language, called YaPP, which complies with GDPR consent requirements in smart homes. Utz et al. [179] explored GDPR consent notices and found that 'nudging' practices were widespread and strongly influenced user choices. They recommended that data protection regulation should explicitly state (e.g., clearer requirements and guidance) how consent has to be obtained. Mangini [128] conducted a survey study with users and organizations on the impact of GDPR's right to erasure ('right to be forgotten') on privacy. They reported that companies found GDPR costly and difficult to implement while users strongly mistrusted the companies.

Other research has addressed the impact of GDPR on web interfaces. Anderson and von Seek [14] found that after GDPR, websites were collecting fewer cookies and users had the ability to inform themselves about data processing. However, GDPR did not result in more web transparency because policies were too long and complex. Machuletz and Bohme conducted an experiment with 150 university students in two countries and found that consent decisions were highly affected by highlighted buttons and the number of options offered [127]. Degeling et al. [61] measured the 500 most popular websites in the EU and found that websites were more transparent after GDPR, but there was a lack of user-centric tools to support users in consenting or denying access to their data.

Moreover, dark patterns used to steer or nudge users into consenting to data collection have been recently explored [179]. A dark pattern is defined as a "*user interface that has been carefully crafted with an understanding of human psychology to trick users into doing things they did not intend to.*"

Dark patterns for privacy notices have been previously reported in the literature [40, 49, 84, 129], protection organizations [51], whitepapers [3], and press articles [167]. For instance, Nouwens et al. [148] analyzed the most 10,000 websites visited in the UK and found that only 12% of the websites were free of dark patterns.

Dark patterns techniques reported in the literature include hiding away privacy-friendly choices, hiding advanced settings, preselecting checkboxes, requiring more effort to reject consent, and take-it-or-leave-it choices [51, 129]. The infamy of dark patterns has led California to outlaw them under the CCPA [184] and EU data protection officers to explicitly cite dark patterns examples in their advisory documents [148].

2.2 User Experience of Smart Home Security and Privacy

Smart homes presented new opportunities for manufacturers and businesses to collect real-time, contextual and increasingly detailed data about the habits, lives, and activities of smart home users [16, 53, 154, 187]. As such, many commercial smart home products (e.g., thermostats, baby monitors, and security cameras) use consumer data for their own purposes and disclose sensitive data (e.g., location data, health data, voice recordings) to third parties [38, 78, 156]. As a result, there has been an increased focus on user-centered smart home security and privacy [7, 15, 20, 77, 91, 92, 149, 190–194, 196], however there has been little research into the wider aspects of UX of security and privacy for smart home devices, and little work exploring how designers factor the UX of security and privacy for these smart home devices [11, 195]. Shortfalls have been identified in UX design of security and privacy in smart cameras [43].

The UX of smart home products extends beyond the use of day-to-day services into the experience of security and privacy. Research has uncovered a number of negative security and privacy experiences: powerlessness, confusion, frustration, disappointment and annoyance [194]. Prior research on the UX of smart home technology has been conducted in laboratories [95, 109], or with prototypes in experimental settings [89, 120]. Smart home security and privacy interactions have been studied using surveys (e.g., [140]), in-situ design evaluation (e.g., [194]), focus groups and interviews (e.g., [52, 193]). More recent work researched 'in the wild' security and privacy user experiences in contextual real-life home settings (e.g., [98, 133]).

The literature suggests that security and privacy design may pose UX challenges for smart home product teams. Oh and Lee [151] analyzed reviews of quantified self applications and found that privacy was a key problem affecting both UX and security and privacy design processes. This was later confirmed by Bergman et al. [31], where they explored how 11 smart home companies captured UX requirements and found that security and privacy posed a UX challenge for designers. Rowland et al. [158] found that designers often faced tensions between UX and security in smart homes.

2.3 Economics of Personal Data

Personal data has been consistently described as the new "oil" of the internet [152, 180]. Bauer et al. describe personal data as "*one of the world's most valuable commodities*" [22]. Tech giants such as Facebook and Google have based their business models on collecting and analyzing user data (e.g., Google [68]). While large companies were capitalizing on consumer data and demands for privacy, personal data markets (e.g., PFP (Paying For Privacy) and PDE (personal data economy) [68]) have been growing. Studies investigating and anticipating personal data markets [62, 102, 118, 163, 180] date back to the 1990s. Personal data markets refer to an online destination where customers were compensated for their use of their data [122]. Personal data markets are often regarded as GDPR-compliant as they allow users to completely prevent their personal data from being used (compared to the "right to erasure"). However, since personal data use is highly regulated, existing

personal data markets must navigate gray areas of law or operate within regulatory restrictions (e.g., enforcement gaps, cross-jurisdiction arbitrage) [171].

Moreover, legislators and researchers have strongly advocated for enforcing property right (data ownership) regimes for personal data [157, 172] where data is treated as property. However, researchers argue that data property rights would not be effective in protecting user privacy. Data property rights would reduce privacy to a commodity, rely heavily on consumer choice, and are notoriously difficult to implement [126]. Furthermore, the current notice-and-choice models (e.g., users clicking past privacy notices) system are already failing because users are unable to understand the potential uses of data, how it will be used, and the accompanying privacy risks [10]. Data property rights would face the same challenges of existing consent models because they rely entirely on individual control [107]. Other researchers argue that data property rights may result in scarcity of personal data and make business models entirely obsolete (e.g., [82]) which might hinder an economy's potential to innovate (e.g., disruption to businesses, hardware supply chains and software development) [171].

Furthermore, measuring and estimating the monetary value of personal data has been a key focus to many researchers; different approaches include: examining market capitalization, examining revenues or net income per user, assessing the cost of data breaches and running economic experiments and surveys [150]. However, estimating the value of personal data has been previously reported to be difficult because personal data is highly context-dependent and lacks harmonization and measurable impacts over time [9, 10, 33, 150]. Previous studies that have attempted to explore price tags for personal data [86, 100, 119] were unsuccessful because user privacy choices were affected by heuristics and biases (e.g., users' own valuations of their personal data) [8, 9]. Furthermore, the monetary values of personal data cannot cover the full economic and social benefits [150].

Lastly, studies exploring privacy interactions from the perspectives of users and designers rarely consider the economic interests of product manufacturers or business leaders [127]. To our knowledge, previous smart home studies have not explored how the strategic interests of the business leaders conflict with the personal interests of the users. To address this gap, we systematically study the combined data protection experiences of users, designers and business leaders in one study.

2.4 Summary

Data protection user experiences (e.g., consent interactions) have been widely studied in the literature. However, the user experience of data protection is a designed encounter, the modalities of which arise out of a process that encompasses contextual, economic, compliance and strategic business priorities. As a result, our research aims to expand the consideration of data protection user experience to encompass the perspectives of designers and business leaders to gain a wider understanding of the complexities and nuances. To understand and address the challenges of data protection compliance, our research qualitatively investigates smart home experiences by bridging the perspectives of smart home users (n=7), designers (n=6) and business leaders (n=6).

3 METHODS

We designed and conducted a qualitative user study of smart home users, designers and business leaders following similar approaches used in previous qualitative studies [36, 134, 135]. We interviewed 19 participants in the United Kingdom, focusing on understanding smart home data protection experiences and practices from the perspectives of users (n=7), designers (n=6), and business leaders (n=6). We concentrated on smart home products because they (i) have a growing adoption rate [142] and (ii) are seen as particularly invasive by end-users [75, 79].

A trained researcher conducted qualitative semi-structured interviews in the UK in English between October 2020 and June 2021. Our institution's ethics committee approved this study.

3.1 Recruitment

3.1.1 Recruitment of Users. To recruit our user participants, we posted flyers and distributed leaflets in the UK, and advertised the study on online platforms (e.g., Twitter, LinkedIn). We asked interested participants to complete an online screening questionnaire, which about 30 completed. We aimed to recruit a demographically-diverse sample of participants. Hence, we included a number of demographic questions about gender, age, educational level, occupation and work field. In addition, we asked participants to specify the smart home devices they use and whether they share them with other users. We aimed to recruit smart home users that (i) were in favor of technology adoption [60], (ii) had previous experiences in data protection (e.g., consent or right of access), and (iii) were technically competent. We defined different levels of technical competence (novice, competence, proficiency, expertise, and mastery) using Dreyfus' model of skill acquisition [66]. Dreyfus' model has been widely used to define levels for assessing one's competence.

3.1.2 Recruitment of Designers and Business Leaders. To recruit designers and business leaders, we also advertised the study in the UK. However, we experienced difficulties finding designers and business leaders willing to share their experiences with data protection. Data protection in many organizations is considered a strictly confidential [30, 104, 175], sensitive and/or 'taboo' topic [181]. In addition, many potential participants could not participate due to being bound by non-disclosure and confidentiality obligations.

To address this limitation, we used the snowball sampling method [83], which is commonly used when investigating hard-to-reach groups [17, 69, 159]. We also recruited a smart home consultant advisor who had wider access to smart home designers and business leaders working in a professional capacity in the United Kingdom. The consultant facilitated referrals to around 25 smart home designers and 25 smart home business leaders contacts. We reached out to all referred participants by email to arrange interviews, and interested participants were asked to fill a screening questionnaire.

All designers and business leaders were working at different companies, and were not connected to each other in any way. In total, we recruited six designers and six business leaders that represented twelve different companies.

3.2 Participant Demographics

The demographics of our user participants (see Table 1) consisted of seven participants from seven households. Participants were composed of five male and two female participants. Two reported having an undergraduate degree, and five a graduate degree. Three were expert smart home users and four were proficient. As for business leaders (see Table 2), all were male (n=6) and leading small and medium-sized enterprises (SMEs). Four came from a technical background while two came from an arts and communication background. Their SMEs sold a wide range of smart home products such as smart locks, smart doorbells and smart vacuum cleaners. Our designer participants (see Table 3) consisted of three male and three female participants, all working in different companies. Four worked as UX designers and two as UX consultants. Three participants worked in a flexible team structure, two worked in cross-functional teams, and one in a centralized team.

3.3 Interview Procedure

3.3.1 Interview Process. To address our research questions, we conducted semi-structured interviews with 19 smart home participants: users (n=7), designers (n=6) and business leaders (n=6)

Table 1. Demographics of Users

P#	Gender	Age (Degree)	Field	Occupation	Competence	Sharing Devices	Devices Used
U01	Male	35-49 (M.Sc.)	Commercial Insurance	Commercial Finance Analyst	Expert	Multiple Users	Amazon Echo Dot, Hue Smart Light
U02	Male	25-34 (B.Eng.)	Railway Transport	Senior Mechanical Engineer	Expert	Single User	Google Home, Nest Audio, Nest Hub
U03	Female	35-49 (M.Sc.)	Information Technology	Senior Engineering Manager	Proficient	Single User	Google Home Mini, Echo Show 5
U04	Male	25-34 (M.Sc.)	Information Technology	Database Administrator	Proficient	Multiple Users	Google Home Hub, Hue Smart Light
U05	Male	18-24 (P.h.D)	Computer Security	Doctoral Researcher	Expert	Multiple Users	Amazon Echo, Google Home
U06	Male	35-49 (B.Sc.)	Education Leadership	Academic Administrator	Proficient	Single User	Nest Thermostat, Nest Hub Max
U07	Female	35-49 (M.Sc.)	Professional Services	Chief Financial Officer	Proficient	Multiple Users	Ring Doorbell, Nest Thermostat

Table 2. Demographics of Business Leaders

P#	Gender	Age (Degree)	Background	Executive Role	Team Size	Company Type	Devices Sold
B01	Male	25-34 (B.A.)	Graphic and Media Design	CTO & Founder	18	SME	smart baby monitors, smart alarms, smart trackers
B02	Male	45-54 (M.Sc.)	Computer Science & Digital Electronics	Technology Lead	5	SME	smart cups, smart food containers, smart mugs
B03	Male	35-44 (B.Sc.)	Mechanical Engineering	CTO & Founder	3	SME	smart robots, smart vacuum cleaners, smart mops
B04	Male	35-44 (P.h.D)	Electrical & Electronic Engineering	Co-Founder	25	SME	smart adult toys, smart vibrators, remote vibrators
B05	Male	45-54 (M.A.)	Virtual Communication	CEO & Founder	11	SME	smart doorbells, smart door chimes, smart cameras
B06	Male	45-54 (M.Sc.)	Electronic & Hardware Security	CEO & Founder	7	SME	smart locks, smart digital door locks, smart padlocks

Table 3. Demographics of Designers

P#	Gender	Age (Degree)	Team Structure	Occupation	Experience	Company Size	Devices Worked On
D01	Female	35-44 (B.Sc.)	Flexible	UX Consultant	7 years	50-100	activity trackers, smart cameras, smart speakers
D02	Female	45-54 (B.Des.)	Centralized	UX Designer	5 years	01-50	smart thermometer, smart grill thermometer
D03	Male	25-34 (M.Des.)	Cross-Functional (Embedded)	UX Designer	4 years	100-500	smart locks, smart security sensors, smart alarms
D04	Male	45-54 (M.Sc.)	Flexible	UX Consultant	6 years	50-100	smart speakers, smart displays, baby monitors
D05	Female	35-44 (M.Arch.)	Flexible	UX Designer	8 years	100-500	smart intelligent sensors, smart home automation,
D06	Male	45-54 (M.Sc.)	Cross-Functional (Embedded)	UX Designer	10 years	500-1000	smart indoor/outdoor cameras, smart doorbells,

between October 2020 and June 2021. We conducted all our interviews remotely using Skype, Zoom and Microsoft Teams. We also audio-recorded the interviews and took notes to document noticeable events. No participant was compensated for the interviews.

We allowed participants to elaborate, share their thoughts, and ask any clarification questions. We also asked follow-up questions and probed participants when appropriate. This is a common practice in semi-structured interviews, in which the interviewer primarily uses a list of questions, but has the discretion to ask follow-ups or skip questions that have already been covered. The value

of conducting qualitative research lies in providing a holistic understanding of the phenomenon under inquiry using predominantly subjective qualitative data, which can be supplemented by observational and other quantitative data [112].

We refer to 'users' as end-users who ultimately use or intend to ultimately use a smart home product (e.g., device purchaser, device administrator, and device user in the house). We refer to 'designers' as people who create tangible or intangible smart home objects, products, processes, services or experiences (e.g., UX designer, UX consultant). We refer to 'business leaders' as corporate leaders and executives in charge of managing a smart home product company or organization (e.g., CEO, CTO).

3.3.2 User Interviews. We started with general questions asking users to describe the smart home devices they own, how they use them, and what apps or automation they have installed. We also asked them to describe any previous experiences dealing with or understanding data protection regulation (e.g., exercising their online rights, experiencing consent interactions). In addition, we asked participants to describe their understanding of their data use by smart home companies. To avoid participant response bias [23, 63], we began by querying more general questions that could elicit security or privacy concerns but did not explicitly mention them.

3.3.3 Designer Interviews. We started with general questions characterizing the designers' role at the company (e.g., responsibilities, duration of employment), the type of products they designed or developed, and their experiences with UX and data protection regulation. We then asked questions related to requirements gathering and specification in the design phase, as well as questions about how UX was factored into the design process (e.g., data protection design decisions, UX design methods, techniques, and artifacts). Our designer participants referred to different groups of people (e.g., device purchaser, device administrator, and device user in the house) as 'users' without distinction.

3.3.4 Business Leader Interviews. With business leaders, we started asking general questions regarding their executive role, their leadership approach, and how they attain business goals and objectives. We also asked them about the products they sold and marketed, their plans for expansion, their customer base, their markets, and innovative industry developments and standards. In addition, we asked business leaders about their experience with GDPR data protection compliance, which included questions regarding their role in implementing a data protection strategy or program, strategic experience in guiding the organization through a process of continuous compliance, and their internal organizational challenges and mismatches with data protection law.

3.4 Pilot Study

We conducted a pilot study of three semi-structured interviews to check that the questions for all stakeholders could be understood and 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 [32] by selecting three employees (with a background relevant to each user group) in our organization for the pilot study. In addition to the three sessions, we asked two researchers to review the study. No considerable changes were made to the study.

3.5 Data Analysis

We professionally transcribed and then analyzed all 19 semi-structured interviews using Grounded Theory, following Strauss and Corbin's procedure [174]. We chose Grounded Theory over other approaches (e.g., thematic analysis) because we wanted to (i) develop a substantive theory, (ii)

explore data protection interactions and processes in depth, and (iii) derive recommendations grounded in the problem domain [43]. Grounded Theory enables the examination of topics and situations from many different angles, leading to comprehensive and deep explanations. It can uncover beliefs and meanings behind behaviors and events, through examining both rational and irrational aspects of behaviors [173].

Four researchers in total analyzed the transcripts. Author 1 (the primary researcher who conducted all the interviews) and author 2 (the principal investigator of the study) independently completed the initial coding of all interview transcripts. Throughout the coding process, author 2 was able to ask for clarifications and additional insights while author 1 annotated the study data to provide additional context. To verify the credibility of the initial codes, a third researcher cross-checked the codes against the interview transcripts. At the same time, a fourth researcher (external to the study) reviewed the initial codes and supporting quotes. Any differences and/or issues arising from the initial coding were discussed and resolved among the four researchers. A codebook consisting of 210 codes emerged from the initial coding (see Table 4). These codes were then applied across other interviews through constant comparison, while new codes were added as they emerged and were deemed necessary. The researchers then grouped the codes into themes (axial coding) and categories (selective coding), based on the properties and dimensions of each theme. These codes were applied across other interviews through constant comparison. Axial coding allowed us to group different perspectives and experiences from all of our user groups: users, designers, and business leaders. Regular coding meetings were held to discuss any emerging codes and to group the codes into families.

To make our consolidated analysis feasible, we derived a core set of questions linking all interviews together. However, we observed data saturation separately for all our three participant groups. We observed data saturation [50, 88, 164] between the 6^{th} and the 7^{th} interview for users, the 5^{th} and the 6^{th} interview for business leaders , and the 5^{th} and the 6^{th} interview for designers. Data saturation has attained widespread acceptance as a methodological principle in qualitative research. It is commonly taken to indicate, on the basis of the data that has been collected and analyzed, that further data collection and analysis are unnecessary.

After creating the final codebook, we tested for inter-rater reliability for each user group. The average Cohen's kappa coefficient (κ) is 0.86 for users, 0.80 for business leaders, and 0.83 for designers. Cohen's kappa values over 0.80 indicate almost perfect agreement [132].

In total, the analyzed material interviews consisted of 10 hours and 28 minutes for users (average of 1 hour and 29 minutes per interview), 10 hours and 18 minutes for business leaders (average of 1 hour and 43 minutes per interview) and 8 hours and 19 minutes (average of 1 hour and 23 minutes per interview) for designers.

3.6 Research Ethics

Our study was thoroughly reviewed and approved by our organization's ethics committee. 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. 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).

Due to the sensitivity of our interviews (e.g., privacy, security, compliance), we asked participants not to name specific people or sites so that the interviews will already be anonymous to some degree. All interviews were AES 256 encrypted and stored in a physical safe in our organization. Participants had the option to withdraw at any point during the study without providing an

explanation. We explained to them that in such a case, none of their data would be used in the analysis. No participant withdrew.

3.7 Limitations

Our study has a number of limitations common to all qualitative research studies. First, research quality depends on the researchers' individual skills and might be influenced by their personal biases. Inexperienced interviewers may not be able to ask prompt questions or probe into situations that would result in missing gathering relevant data [110]. For instance, the depth of data collected is dependent on the interviewer's skill [101] and the quality of the questions asked [34]. To address this limitation, one researcher, who was trained to conduct the interviews consistently and ask questions in an open and neutral way in order not to influence participants, conducted all 19 interviews.

Second, self-reporting bias is common in interview studies [1]. Some participants might have not responded accurately to our questions because they did not remember specific details. Other participants could have been concerned about the interviewer's perception of them and, therefore could have changed their answers in line with how they like to be perceived. For instance, social factors such as ethnicity may influence the answers that different social groups are willing to give [41]. To maximize validity and minimize self-reporting bias, we avoided leading questions and relied on open-ended questions, inviting participants to provide in-depth answers in their own words. Some of our participant answers were less detailed, however, we prompted participants to give full answers to all questions.

Third, as we note in our recruitment section, finding designers and business leaders willing to share their experiences in data protection (e.g., GDPR) is challenging due to legal matters being sensitive and confidential. As a result, despite numerous efforts, we were unable to recruit any business leaders from large companies. As such, our qualitative work is limited by the size and diversity of our sample. Following recommendations from prior work to interview between 12 and 20 participants [44], we interviewed users, designers and business leaders until new codes stopped emerging.

Fourth, security, privacy, and regulatory matters are sensitive issues in organizations. Our participants' corporate responsibilities, as well as their company's reputation, might have biased their responses. Some participants (e.g., business leaders) were not able to share sensitive and confidential information, and could have stripped essential and valuable research data. To mitigate this, we briefed our participants about our security and privacy measures, focusing on how we will encrypt their data and process it in accordance with the General Data Protection Regulation (GDPR).

Fifth, we note that ours is a qualitative study. We do not attempt to quantify our findings or draw conclusions or generalizable findings about a larger or a wider population of users, business leaders and designers. The focus of our qualitative work is about the richness of understanding rather than the generalizability to a population. Since our methodology was qualitative and exploratory in nature, the hypotheses we formulated based on our findings, emerging themes and discussion coming from the grounded-theoretic analysis, would need to be tested in a follow-up confirmatory study to assess their broader applicability and generalizability.

4 RESULTS

In this section, we present our findings. We discuss our key themes: the experience of users (Section 4.1), the experience of business leaders (Section 4.2) and the experience of UX designers (Section 4.3).

4.1 Experience of Users

Users experienced dark patterns when consenting to personal data processing (e.g., tracking) or giving access to device permissions (e.g., location services). In addition, they experienced dark patterns when exercising their data protection rights (e.g., right of data access). As a result, they perceived the data-value exchange with smart home companies to be imbalanced, confusing, and untrustworthy.

4.1.1 Dark Patterns when Providing Consent. Smart home users (n=4) reported experiencing dark patterns when consenting to providing access to their audio recordings, web cookies and device permissions. They experienced four categories of dark patterns: intrusive privacy defaults, difficulty rejecting consent, unexpected detriment and punishment, and forced interactions.

4.1.1.1 Obscured and hidden privacy-intrusive selected defaults: User participants (n=3) experienced hidden privacy defaults that felt intrusive while setting up and using smart home products. U05 reportedly found pre-selected defaults enabled on their Amazon Echo after checking their 'Alexa Privacy' settings. U05 expressed disappointment after finding the *"use of voice recordings"* feature activated by default. The feature allowed Amazon Alexa to use customer voice recordings to develop new features as well as enable contractors to manually review the voice recordings. Similarly, U03 said they were shocked after discovering a privacy-invasive feature enabled by default on their Echo Show 5 called 'Amazon Hunches'. The feature allows Alexa to observe users' interactions with connected smart home devices like locks, lights and electricity outlets. In turn, Alexa would detect regular patterns and proactively offer to complete tasks around the house, such as turning off lights, based on habits and frequent requests. U03 said they found it '*creepy*' and '*disturbing*' that their detailed home activities were being analyzed and turned into patterns.

4.1.1.2 Frustration and difficulty in rejecting consent: Users (n=3) experienced difficulty while attempting to reject or withhold consent from cookies and device permissions. As a result, privacy-preserving options were more cumbersome. For instance, U02 reported that their Google Home constantly nudged them to give Bluetooth permissions to be able to easily set up the device. Similarly, U04 couldn't set up their Google Home Hub because it required consent to '*location services*'.

4.1.1.3 Facing unexpected detriment and punishment: Users (n=2) have reportedly experienced unexpected detriment from refusing to consent to specific permissions and services. Users facing privacy-invasive permissions said that permissions they attempted to reject turned into roadblocks (e.g., inability to set up the device). Those permissions are known as 'do-or-die' or 'take-it-or-leave-it' permissions, but do not always make it clear they are necessary. For instance, U04 could not play music on their Google Home Hub without consenting to '*Web and Tracking*' activity monitoring. U04 explained: '*I don't understand why it needs my Google browsing history to play music.*'.

4.1.1.4 Pressured consent interactions and limited timing: User participants (n=3) experienced consent interactions that pressured them to make consent decisions before using smart home products. Those interactions prohibited users from postponing their choices, giving impressions that users would be blocked from using the service. For instance U03, who was setting up their Google Home Mini, was presented with privacy preferences (e.g., location, activity tracking, personalisation) before proceeding with the installation of the Google Home. U03 said they were in a hurry and did not see a clear option to postpone their choices to a more convenient time. This added unnecessary urgency gave little time for U03 to reflect on the choices provided.

4.1.2 Dark Patterns when Exercising Legal Rights. Smart home users (n=2) experienced dark patterns when exercising their data protection rights (e.g., right of access). They found the process to be confusing, frustrating and couldn't easily authenticate or prove their identity. As such, they expressed a preference for automated data subject requests.

4.1.2.1 Frustration when making data subject access requests: Some users (n=2) who made data subject access requests found the process to be confusing or frustrating. They were not given any specific instructions for how to exercise their data access rights. U01 reported sending data subject access requests in the past made use of letter templates found online to facilitate the process. U01 said that the process of submitting and receiving data access requests was frustrating as they had to wait for weeks to receive an answer. Similarly, U05 who wanted to send data subject access requests found it difficult to get the contact details of the data protection officer. U05 said: "*It would be nice if organizations, for example, had the equivalent of a robots.txt file on their websites that would just list the data protection officer and their email address.*"

4.1.2.2 Preference for automated data subject access requests. Users who exercised their data right of access reported a strong preference for using automated data subject access requests. Users reported a positive experience over using automated platforms that made the experience smooth and efficient. For example, U05 found Google's data subject access request smooth. U05 explained: "*Google's right of access process is really smooth. I can press a single button and execute my right of access request whenever I want.*" Similarly, U01 who wanted to exercise their data access rights for Alexa and Echo devices described Amazon's automated '*Request My Data*' web page as '*convenient*' and '*easy to use*'.

4.1.2.3 Difficulty authenticating when making data access requests: Users who reported making data access requests experienced difficulty. For example, U05 who sent different data access requests in the past described their difficulties in authenticating. U05 expressed frustration over having to create new accounts with third parties to exercise their data access requests. They explained: "*I found that often I have to create a special account on a proprietary or a contracted out GDPR access type system to make requests [...], or I'd have to share documents with some third-party document server in order to prove my identity. There were often a lot of steps in the actual process from wanting to make a request to executing the request and then getting an answer.*"

4.1.3 Poor Data-Value Exchange.

Users experienced an imbalance in the perceived data-value exchange with smart home companies. They did not know which data was collected about them, how it was used or how much it was worth. As a result, they were not comfortable with sharing data and did not trust the exchange process.

4.1.3.1 Not knowing what data is collected and why: Smart home users (n=3) did not know what data was being collected about them; others (n=2) did not know why some data was collected. For instance, U06 stated that they wanted to know what data is collected by their Nest thermostat but they were unable to find out how to get that information. U06 said that there is no easy way to find out which data is collected and the only available information was Google's Privacy Policy which applies to Google's connected home devices and services. Moreover, some users who were worried about their privacy struggled to find concise, transparent, intelligible and accessible information. U01 explained that they were concerned about how audio interactions were being stored on their Amazon Echo. U01 visited Amazon's FAQ to find more details but they found the information vague. U01 said: '*Their FAQ only told me how to review recordings Alexa has about me and delete them. But nothing shows me how and if the data is stored on my own device and how long it is stored*

for.' Similarly, U07 expressed concerns over the lack of knowledge of motion data collected by Ring doorbells. In particular, they were unsure what kind of metadata is collected with every motion and what kind of interactions with the camera are recorded.

4.1.3.2 Not understanding how their data is being used: Interviewees (n=2) said that they don't understand how their data and information was being used by smart home companies. U07 who experienced annoyance over what happens with their Amazon Echo data stated that the company has been unhelpful in providing any type of personal information. Similarly, U07 said they don't understand how Google Assistant is using their location and making predictions. U07 said: "*I'd really like to know how Google is able to use my location, calendar or whatever to tell me when I should leave the house and which route I should take.*" Users experienced dissatisfaction in understanding how algorithmic decision-making works. It was difficult for them to understand where data comes from, how it is used by algorithms powering smart homes, and where algorithms send data. For instance, U05 experienced frustration over their device 'waking up' without them saying the wake word which caused serious concerns. U05 wanted to access more information about how Amazon detects and processes wake words but they couldn't find any helpful information through official documentation.

4.1.3.3 Not knowing how much their data is actually worth: Interviewees (n=2) said that they aren't aware of the true value of their personal data, but they believed it was worth more than what they are getting in exchange. Specifically, data that is not used to improve smart products is seen as offering a poor value exchange. For instance, U02 who shares their video footage, audio recordings and home environment sensor readings with Google said they would be curious to know how much their data is worth. U02 also said that they don't receive enough benefits for providing sensitive data which could be used for home personalization. Similarly, U06 who shared video footage with third-party apps and services within existing Google Home devices said they wanted to know the true value of their video footage to Google. U03 described receiving '*minimal value*' from their products and expressed the need for visualizations that can summarize all the data collected and how much Google is profiting out of it.

4.1.3.4 Lack of trust in the exchange process: Interviewees (n=4) reported a lack of trust for major smart home product manufacturers (e.g., Google, Amazon). U01 referred to Amazon as untrustworthy and said they were not sure whether they could fully trust whether Amazon Alexa would be collecting more data than agreed. Similarly, U07 who uses a Ring camera said they don't trust the company not to sell their personal data to third parties. U07 explained: "*I've always been wary of our Ring camera. It is quite funny. Going through their privacy page they clearly say they don't sell my personal data to third parties, I don't believe them.*"

4.2 Experience of Business Leaders

Business leaders found the costs of data protection to be unfair to smaller businesses and they lacked the necessary resources (e.g., labor) to address compliance needs. They were also confused due to a lack of consistency and clarity in data protection compliance. As such, they took 'necessary shortcuts' to comply with data protection.

4.2.1 Unfair Data Protection Costs.

Business leaders found the costs of data protection to be unfair to small businesses due to: lacking resources such as time and labor, perceiving fines and penalties to be unfairly distributed, and experiencing an unrecognized cost of compliance.

4.2.1.1 Data protection 'fundamentally unfair' to small businesses due to lack of resources: Participants (n=3) argued that data protection regulation is 'fundamentally unfair' to their businesses (e.g., small, mid-size) because larger companies have significantly more resources (e.g., time, labor and wealth) to address of data protection regulation challenges. For instance, B04 said that their lack of resources makes it challenging to overhaul their compliance processes and invest in appropriate long-term solutions. Other participants argued that data protection fines are unfair towards businesses because larger companies can afford fines whereas smaller ones would go bankrupt. For instance, B02 said: "*Companies just get away with way too much and there's no disincentive. [...] And I think that is why you need absolutely huge fines, but you need them to actually be used, because otherwise the companies will just treat it as the cost of doing business.*" B05 said that going through GDPR requirements was difficult for them because they're a small company with limited resources. He said: "*We went through this and the requirements and so on. It is quite difficult for a very, very small company to understand it and understand what the requirements are actually, but we did make an effort to go through that and to try and make sure we complied.*"

4.2.1.2 Fines and penalties applied unfairly across different sized businesses: Some participants state that data protection fines (e.g., GDPR) are unfair towards smaller businesses. In particular, fines projected against bigger companies tend to be too low. Technology lead B02 who runs a small company expressed disappointment over small fines imposed against big companies. He said: *"I think the enforcement in the UK is poor. The ICO is just pathetic. They just announced their Marriott Fine today. Marriott lost 340 million people's records. The ICO said they were going to charge them £100,000,000 and they've finally come through today and said they were actually only charging them £18,000,000. That's 5p per person. So then you can just kind of see the Marriott people going: 'Hey, it only cost us 5p to just do what the hell we like with people's data. That's fine, cost of doing business.' "* Moreover, business lead B01 claimed that his company can be fined as high as £20,000,000 which he described as '*nonsensical*'.

4.2.1.3 The cost of data protection compliance is unrecognized: Participants (n=3) stressed that the focus has been on the cost of fines and penalties; leaving little focus on the cost of compliance. The cost of compliance is reported as being prohibitive and unfair: while fines and penalties are proportional to the company turnover, the cost of compliance is not. Unrecognized compliance costs were reported originating from: educating staff, personal data mapping, reviewing data protection documentation, appointing a data protection officer (DPO), creating privacy notices, and facilitating data access requests and procedures. For instance, B01 expressed dissatisfaction over the high cost of compliance associated with complying with the 'right of access'. B01 invested in tools to comply with data access requests described high costs associated with authenticating users, reviewing the legitimacy of requests, gathering data securely and communicating to users.

4.2.2 Compliance Practices.

Business leaders found data protection inconsistent across countries, and lacked information over the implications of non-compliance. They were also confused whether compliance was needed in some cases. As a result, they took 'necessary shortcuts' to comply with data protection and outsourced responsibilities to third party vendors.

4.2.2.1 Lack of consistency in data protection regulation across countries: Our participants noted the lack of consistency in data protection regulation across different countries, and more specifically across Europe. B02 who sells smart cup technology in the UK and US described difficulties navigating data protection compliance in both countries citing inconsistencies between CCPA and GDPR. Specifically, B02 said that GDPR limits their capability from processing personal data when there is a legal ground (e.g., consent, contractual obligation), unlike CCPA, which requires consent

only when there is a 'financial incentive' out of personal data. Moreover, the 'right to opt out' in CCPA is an absolute right which means B02 cannot reject an opt-out request on the basis of their compelling legitimate grounds; unlike GDPR where legitimate grounds can be used to continue processing information. This finding is in line with Future of Privacy forum's [74] report which reports numerous inconsistencies amongst CCPA and GDPR.

4.2.2.2 Lack of clarity over legal implications of non-compliance: Participants (n=2) reported a lack of knowledge over the implication of non-compliance (e.g., amount of fines and type of penalties). For instance, B05 said while GDPR requirements are generally clear, the implications of breaching these regulations aren't. B05 explains: "*I also had the opportunity to read through the DSGVO, which was the German Data Protection Law before the GDPR. In general, it's very clear. The actors in the system, what their responsibilities and roles are, and what you need to do offering a product or service. I think what's not clear is the legal implications. That's still being sorted out in the courts and in the various jurisdictions.*"

4.2.2.3 Confusion whether data protection compliance is needed: Some participants (n=2) were unsure whether they are liable for GDPR compliance because they were not collecting personal data. For instance, B06, a business leader of a smart lock manufacturer in the UK, explained that GDPR compliance wasn't too relevant since his company did not collect or store personal data. B06 said: "*From a GDPR perspective, we don't gather personally identifiable information. We don't store any of that information that is recognizable to the individual. From that perspective, while we do comply with all of the regulations that are in place, they are less relevant to us because of the way that we don't actually gather data in the first place.*"

4.2.2.4 Taking 'necessary shortcuts' to comply with data protection: Some participants (n=3) struggled to find suitable processes and practices to address data protection. As a result, they reported taking 'necessary shortcuts' and cutting corners to comply with data protection. For example, B03 complied with data protection through his own judgment and reasoning instead of going through the official documentation. He explained: "*Probably complying with them is the easy part actually. The difficult part is almost certainly just reading and wading through the regulations and working out exactly what you have to do. Once you've done that, doing it is probably easy. We've decided that we'd shortcut our process and do what seems reasonable, which is not selling anyone's data, to keep it secure, to keep the minimum amount of data that we need to do the job.*"

4.2.2.5 Using third parties to comply with GDPR:. Participants (n=6) engaged with third-party suppliers to process or access personal data on their behalf which made their experience of dealing with GDPR easier. For instance, B04 reportedly chose to use Shopify to sell smart products in the UK citing GDPR-compliant features are built into Shopify's platform. B04 explained: "*Now, everything which is standard, for example, with Shopify, mail platforms, Amazon web services, everything complies. As long as you're using the standard builds of a lot of functions, and you have a very good legal counsel in-house, it is quite easy to comply with GDPR.*"

4.3 Experience of Designers

Designers managed data protection requirements through balancing user needs with business goals. However, they experienced challenges achieving that balance due to poor communication with business leaders. To manage the challenge of data protection design, they developed heuristics (i.e., rules of thumb) to navigate the complexity and constraints of data protection design. Moreover, they recommended that users should be better educated on business models.

4.3.1 Balancing User and Business Needs.

Designers balanced user needs with business goals to address data protection designs needs. However, they faced challenges due to difficulties aligning UX efforts with business goals and communicating to business leaders privacy issues and UX needs.

4.3.1.1 Obstacle in sensitizing business representatives towards privacy issues: UX Designers (n=3) faced obstacles communicating the security and privacy impacts of smart homes to business leaders. D05 said that they tend to research and provide summaries of privacy issues that might occur from the design of some features. D06, who worked in smart home product teams, said that privacy and security conversations are often "*sailed away with one privacy or security expert*". As such, security and privacy topics are not part of the regular conversations. D06 said that they make an effort to inform all stakeholders (specifically to business leaders) on possible security and privacy issues they are aware of.

4.3.1.2 Difficulty in explicitly aligning UX efforts with business goals: UX designers (n=2) said that business leaders often do not see the value of some investments in UX. In addition, explicitly translating the benefits of UX designs with business requirements (e.g., user retention, increased sales, conversation, and reduced costs) is not straightforward. For instance, UX designer D06 faced challenges in getting prototypes for a smart camera application approved by business executives. As such, they often identify selective design issues in their prototype that, if fixed, would help business executives better improve business goals (e.g., users purchasing a cloud storage solution for the video recordings). D06 said: "*The reality is that if you work as part of a large product team and your prototype does not move the needle, it will likely be thrown away.*" This finding adds more context to Lallemand et al.'s survey [114] which found that UX experts consider UX goals to extend beyond ones typically held by business leaders.

4.3.1.3 Frustration when involving business leaders in UX:. UX Designers (n=4) stressed that involving business and product stakeholders in UX is critical to balancing user and business goals. However, this can be a laborious and frustrating task. D01 explained that connecting business stakeholders into UX research and design is not always possible. This would lead to less commitment within teams and result in uncreative ideas. D01 said: "*The worst thing is people building stuff and designing stuff in isolation.*" Similarly, D04 said that enabling business leaders to experience the customer and to facilitate that cross-functional conversation about that experience is difficult. D04 strongly encourages product teams and business leaders within a team to learn and be involved in UX. D04 explains: "*UX is not exclusively a UX designers' job. Everyone is responsible for learning and connecting from customers, including CEOs and ultimate decision-makers. They should experience the customer and really have a sense of how they are interacting with the product.*"

4.3.2 Managing Challenges.

To manage the challenges and complexity of data protection regulation, designers used heuristics (e.g., rules of thumb, tried-and-tested solutions, learning in production) to find a cheap and fast way to achieve data protection compliance. In addition, they balanced different stakeholder interests (e.g., through visualizations, arranging meetings) to reduce problems and maximize benefits.

4.3.2.1 Using rules of thumb to overcome data protection design challenges: UX designers (n=3) reported using rules of thumb to address data protection design challenges. The rules of thumb aided designers with '*mental shortcuts*' when faced with time pressure or complex conditions. For instance, D06 introduced '*just-in-time*' privacy notices, a rule of thumb from an online UX practice guide for GDPR compliance, into a number of interactions (e.g., the registration page of a smart camera product). Similarly, D02 used two rules of thumb (clearly separating terms and conditions

from consent requests, allowing users to separately consent for different types of data collection) to introduce GDPR-compliant privacy notices for a smart heating mobile application. This allowed D02 to introduce a new privacy design without the need to conduct user testing and research.

4.3.2.2 Representing and visualizing business and user viewpoints: UX Designers (n=2) stressed that representing and visualizing user and business viewpoints can be crucial in finding a balanced solution experience, while being aligned with project constraints and business goals. D01 uses their visualization skills to sketch and paint an image that can help business leaders see different users' viewpoints within a project. Similarly, D02 said they regularly spend time representing and understanding different business goals and perspectives within a project. They stressed that business goals that help grow the company size and revenue improve the product experience for users in the long run. This finding confirms Schaffer and Lahiri's argument [160] that UX teams participate in practices of organizations developing new products or business ideas.

4.3.2.3 Relying on tried-and-tested techniques to move past strong opinions: UX Designers (n=3) relied on tried-and-tested techniques (e.g., usability testing) to move past subjective and conflicting opinions. These solutions reportedly raised awareness of user needs as they focus on gathering empirical user data instead of subjective opinions. When faced with strong and conflicting opinions, D01 raised the awareness of user needs through usability testing with the whole project team as observers. Similarly, D05 stated that they tend to demonstrate usability videos to business leaders when faced with opposition. Tried-and-tested solutions used in security design have been previously reported by Chalhoub et al. [43].

4.3.2.4 Balancing stakeholder interests to minimize problems and maximize benefits: UX designers (n=5) said that competing interests in a project can arise where stakeholders are not on the same page on data protection regulation or have disagreements over its implementation. As such, they resolve conflicts through 'satisficing' (aiming for a satisfactory result, rather than an optimal solution) or balancing the conflicting opinions of stakeholders. This would lead to a design approach that is pragmatic and rather than maximizing the benefits and minimizing the drawbacks for all stakeholders, aims to provide a good enough solution. For example, D06 held structured meetings to address disagreements occurring due to lack of consensus during the product design phase. D06 described organizing meetings with key stakeholders (e.g., business, development, regulatory) where they discussed their conflicts. Similarly, D03 explained that they feel responsible in participating in prioritization discussions where they bring their skills and offer a 'balanced perspective' that factors different stakeholder perspectives.

4.3.2.5 Continuous improvement of smart products (learning in production): UX designers (n=3) adopted an on-going design approach where they continuously measure, learn and improve from smart products that are released in production. In particular, UX designers are involved in continuous integration, deployment and improvement of smart home products. Designers set up feedback loops in production where they established a dialog with users and extracted insights and improved understanding of users. In return, they shared their insights with other stakeholders. As such, designers improve and change product features, and introduce new deliverables consistently over time. For instance, D04 who follows a '*continuous design*' approach when designing smart home products ensures that released smart products are over-provisioned to allow for features to be introduced in the future. He explained: "*You have this propensity to over-provision these initial hardware devices. That may mean additional sensors, that may mean additional processing power, additional things like microphones, things like that. Even if you're not using them in the beginning because it's much more expensive to do an exchange of those devices than it is to just put those things on the initial device and not use them.*"

4.3.3 Educating Users. Designers reported that educating users about the value proposition and business models (e.g., through conversational interfaces) is crucial in smart homes. However, this can be challenging due to the inability of some users to understand how technology works.

4.3.3.1 Users should be taught data monetization business models: UX designers stressed that users should have a clear understanding over business models and how their data is monetized, especially when the service is free. D01 explains that understanding business models is part of a user's experience: "*This might not necessarily be user experience designer's job, but the fairness or otherwise of the business model, and how well users understand it, and how they perceive value exchange is part of a person's experience of that product or service. If someone's monetizing your data for other things, it might allow them to charge you less as a customer. But then your data is being used in ways that you may not really have any control over.*"

4.3.3.2 Users should be educated through more conversational interfaces: Instead of communicating to users through text, UX designers (n=2) suggested that making smart home interfaces more conversational is likely to improve users' understanding of data use. D01 explains: "*This is off the top of my head, but let's say: 'It looks like you're out, but you haven't set the burglar alarm.' or 'It looks like you're out, maybe we should put the security cameras into motion detection mode. We can do that with your electricity data, but are you happy for us to use your electricity data to infer when you're at home or not?'* "

4.3.3.3 Difficulty for users to understand how technology works: Users who are unable to understand how technology works in general might struggle to understand how their data is processed. As a result, it is difficult to know if users are paying for a well-designed system or not. D05 explained: "*I came from an architectural background, and for me programming is secondary, my second life that I've come to be in contact with. One of the things that I could empathize very well is the fact that if you don't know technology yourself, it seems like a huge barrier to mentally understand what lies beyond the surface of it.*" Moreover, D06 stated that users who purchase smart speakers might not be aware that they might not work without a cloud back-end. He explained: "*If you buy an Amazon Echo, it's a peripheral for a piece of software running in a data center really, isn't it? I don't think people (a), realize that; then (b), realize they have an object in their home. They don't realize how connected it is to the servers and what data is being transmitted backwards and forwards.*" Furthermore, D04 explained that some users might be unable to assess whether the price they are paying is fair and represents good value. D04 explained: "*I think the issue here is that there's no way for an end consumer to know if I am considering purchasing or using a well-designed system? Or is this the cheapest possible thing that could be brought to the market?*"

5 DISCUSSION

In this section, we first discuss how our findings relate to the wider context of ethics, in particular how dark patterns evolved to fill a gap in regulation, and the role of *honesty* as a means of building trust in the relationship between users and companies. We then focus on UX data protection practices, exploring the principles behind discount data protection among designers and business leaders, and discussing the wider applicability of this concept. Finally, we discuss how our findings can lead to new implications for the design of data protection experiences.

5.1 Implications for Ethics and Data Protection

5.1.1 Dark Patterns arise from Conflicts of Interest: Users experienced a wide range of dark patterns (e.g., magnified sense of urgency and scarcity, manipulation to trick users into action, toying with

emotions). As a result, users reported wanting companies to demonstrate more accountability and transparency (e.g., U02 wanted to know what data they are giving away). In addition to experiencing dark patterns, users wanting to exercise their data rights online found the process to be frustrating (e.g., data rights requiring time and effort). Data protection regulation lacks explicit instructions over how easy it should be for users to exercise data rights online: while the exercise of legal rights is protected, the ease with which they can be exercised should be seen as an ethical choice by the business and UX designer.

Dark patterns can be seen as an instance of unethical design practice that has become extremely commonplace since data protection regulation took effect. In addition to employing persuasive design techniques to make it easy for users to agree and difficult for them to object, there are some instances of companies that refuse to offer their services unless the user consents to all data uses. For companies that choose to employ them, the appeal of dark patterns is to minimize the number of users who choose to partially consent to data uses, which can in turn lead to a reduction in data monetisation, but also lead to reduced functionality or worse user experiences. The prevailing perception of dark patterns is that they are objectionable and this has driven further regulation, e.g. California has legislated to outlaw their use under CCPA [148, 184].

Dark patterns are not accidental – they are deliberate acts of manipulative design. They have been described as '*willfully dishonest design*' [12], '*asshole design*' [115], '*diabolical*' [29], '*deceptive*' [113], '*unethical*' [90, 155], and '*manipulative user interfaces*' [58, 186]. We note that dark patterns arise out of a conflict of interest where the business in charge of designing and implementing the consent exchange has a material interest (e.g. data monetisation) in one particular outcome. As a result, the appeal of dark patterns is to facilitate the preservation of business imperatives and interests (e.g., collecting and using more data) at the detriment of user needs (e.g., respecting the data rights of users). Our results show that dark patterns are only one example of what can happen when business needs aren't aligned with data protection requirements, where the responsibility for implementation of data protection can lead to conflicts of interest, and where the incentives for respecting users' needs are insufficient when matched against business drivers not to.

The design community of smart homes could respond to the rise of dark patterns through crowdsourcing from users of what they perceive to be deceptive design patterns. This will help privacy advocates, policymakers, and agency enforcers hold businesses accountable for dishonest and harmful practices. For example, the Electronic Frontier Foundation released the Dark Patterns Tip Line[1], which is an online platform hosted by Consumer Reports that allows users to submit and highlight deceptive design patterns and dark patterns they experience in products, services and websites[2].

5.1.2 Honesty: Previous research in smart home security and privacy strongly advocates for building 'trusting relationships' with users [19, 80, 124, 189, 196]. However many smart tech companies have regularly failed to adequately gain the trust of users [42]. When Facebook released an AI-powered Smart Camera, Mozilla Foundation released a report stating '*given Facebook's terrible track record on privacy, we're worried a lot.*' [138] Research that has explored the impact of long-term customer-company relationships reported a '*trust crisis*' that costs companies $2.5 Trillion per year [64, 153].

Our user interviewees who consented to providing data perceived smart home interactions to be dishonest, poor and lacking transparency. Dishonest and non-transparent practices are harmful to a healthy and trusting relationship between users and service providers. In order for smart home companies to gain consumer trust and build affinity, they will need to consistently demonstrate

[1]https://darkpatternstipline.org/
[2]https://www.eff.org/deeplinks/2021/05/help-bring-dark-patterns-light

their social responsibility and develop core values such as honesty and trustworthiness. Designing honest and transparent smart home interactions is critical as honesty is a precursor to building trust, which cannot be designed or bought.

Our interviews with business leaders reveal that smart home manufacturers have little incentive to go beyond the bare minimum to comply with data protection regulation. Our participants described data protection regulation as a '*checklist*' and a '*box ticking exercise*' describing an evident lack of care and prioritization. For instance, B06 said: "*I think what it only does is it leads to a tick box exercise, because ultimately, what you want to show as an organization is that your software is complying with particular GDPR requirements, but does it actually lead to an improvement in privacy practices in software?*" We argue that smart home manufacturers should align more explicitly with transparent and demonstrably honest practices when complying with data protection. This would motivate all stakeholders to go beyond the minimum to develop honest interactions around data protection.

5.1.3 Value Exchange: With personal data being described as the "new oil" over the past decade (e.g., [93, 152]), we are entering an economy where personal information is the new currency (e.g., [47, 76]), however the value of this currency is not understood by many users [8, 9].

Our results show that smart home users do not perceive the data-value exchange in the same way that businesses do. Users expect smart home products that are respectful of their security, privacy and safety. Business leaders conversely are expected to find new opportunities to collect customer data and to monetize it.

In addition, our results reveal that users do not have a detailed understanding of the value of their personal information. Our participants had minimal information over the value of their personal data and frequently interacted with products that failed to explain what data they were giving away. The only real source of information about the value of personal data comes from mass media (e.g., news stories about data breaches). For instance, our Amazon Echo participants had to pay separately for the price of the device, audio-book plans and music services. However, they had no clue how much personal data is shared with Amazon, how valuable it is, and precisely what they are getting in exchange.

While some experts advocate for the use of personal data marketplaces to address value exchange imbalances (e.g., [102, 163]), these might not be suitable for smart homes users. While data marketplaces are helpful in business-to-business relations, business-to-customer relations aren't best framed as a financial exchange. Instead, they could be better framed as an ethical positioning (e.g., companies being trustworthy and acting honestly), and framed according to the value that the personal data of users can have for the wider society or the public good.

Future technologies with business models that aim to collect, manage, and monetize personal data should explicitly demonstrate how user data is being monetized. For instance, companies can redesign consent interactions to clearly demonstrate to users how much their data is worth and what value they are getting – instead of simply requesting consent to data use. This would allow users to learn the value of their customer data and make more mindful decisions about data use. Another option in this space could include moving away from individual consent interactions and towards standard data usage models that represent transparently negotiated and ethical data usage practices. Although this could be seen as undermining individual choice and agency, there are arguably advantages to this for communal spaces such as smart homes where individual data use decisions may affect bystanders or other users.

5.2 Implications for UX practices of Data Protection

5.2.1 Discount Data Protection Practices. We found that *discount data protection practices* cut across all stakeholders. Our results confirm that all stakeholders (e.g., users, designers, business leaders) developed processes and practices to address the challenges of data protection regulation and had a strong preference for approaches that have a good cost-benefit value. The propensity for users to take shortcuts and apply heuristics for dealing with security and privacy is already known, and our findings confirm that users are indeed behaving in a similar manner for data protection choices, e.g., users were confused about how consent notices function, and perceived them to be manipulative and meaningless. As a result, they deployed coping strategies to address them: they 'clicked away' privacy notices or regularly ignored them. In addition to this, our findings also highlight that taking shortcuts and using heuristics also extends to other stakeholder groups: designers and business leaders.

Business leaders of SMEs found the costs of data protection to be strategically limiting and lacked proper resources to address the data protection demands. As such, they took 'necessary shortcuts' (e.g., workarounds, common sense interpretations, cutting corners) and outsourced data protection duties to third-parties. UX designers also faced challenges in balancing user needs with business goals and conducting formal extensive processes to keep up with the need for speedy development in smart homes. They used rules of thumb and relied on tried-and-tested techniques to navigate the complexity of data protection design needs (see Section 4.3.2). We build on this to discuss the wider concept of discount data protection and how this relates to the needs of designers and business leaders:

5.2.1.1 Discount Data Protection Practices for Designers: Discount *usability* principles [146] have previously shown to provide a strong value proposition for usability designers. This allows them to perform quick, iterative, and cheap usability testing rather than full-on, expensive, or one-off user tests.

Our results demonstrate that the problems that inspired discount usability (e.g., lengthy, untimely, and expensive usability testing processes) are similar to the problems reported by our design participants dealing with data protection. As such, we argue that the principles that inspired *discount usability* can be used to frame discount data protection.

Discount usability design methods are highly compatible with Agile development principles [146]. For instance, the "*discount usability engineering*" movement has demonstrated that discount usability methods are the best way to increase UX because they are cheap and fast; and as a result designers can use them frequently [143]. Given that all our design participants followed an agile product development process during the design of smart home products, data protection techniques that fit into an iterative, fast, and agile context are highly desirable.

Discount usability methods have a strong emphasis on techniques that are cost effective, and can outperform more expensive (or deluxe) usability by focussing on early and rapid iteration with frequent usability input [145]. For example, narrowed-down prototypes, such as paper low-fidelity prototyping, can give a faster way for smart home designers to simulate a holistic user experience (e.g., testing very early, iterating through many rounds of design) [165]. Our findings suggest that designers also favor solutions that demonstrate a clear value to their UX efforts (e.g., by helping resolve conflicts, either through usability testing or satisficing rather than optimizing different stakeholder needs). As a result, data protection techniques that demonstrate a strong value to the designer, helping them to resolve problems or to align their UX efforts to business needs are very desirable.

Based on this, our view of discount data protection encompasses pragmatic solutions that help designers to apply, evaluate, and iterate through different UX designs for data protection in an

agile manner. While the benefits of early discount usability have become apparent, we believe that the benefits of early discount data protection will result in solutions that better suit the needs of different stakeholders and result in better data protection experiences.

To illustrate this, we propose the following example of a discount data protection method, which is inspired by the discount usability practice of using heuristic evaluation to assess user interface designs, instead of testing interfaces with users [144]. Heuristic evaluation allows designers to determine whether interfaces and interactions follow usability principles and achieves a high level of quality by combining the views of several designers to arrive at a consensus. This allows designers to gather early, quick and relatively inexpensive feedback to input into the design process [147]. We believe that a similar approach can be applied to the design of data protection experiences, and we propose the idea of a *heuristic evaluation of data protection experiences*. This technique would require several designers to reach a consensus in evaluating a data protection experience according to user, regulatory, and business perspectives. To do so, they would employ principles and apply heuristics to consider usability, honesty, fair data exchanges, and business alignment.

5.2.1.2 Discount Data Protection Practices in Business Leaders: Reports and studies have demonstrated that bigger companies provide better data rights exercising experiences [71, 108, 162, 168]. While larger companies (e.g., Google, Facebook) can afford to invest more into improving the experience of exercising data rights (e.g., enhanced privacy settings, increasing transparency with YouTube videos), small businesses leaders have reported lacking resources (e.g., labor, skills, budget) to facilitate the implementation of GDPR. With a clear emphasis on cost-effectiveness, discount data protection practices should help to introduce more tools and business-friendly solutions to facilitate the implementation of data protection by small businesses.

While a focus on suitability, efficiency and effectiveness are core to ensuring that techniques suit the budgets of all businesses, another facet offered by the concept of discount data protection lies in the possibility of using discounts to incentivise change. The current approach to data protection incentives is framed around using regulatory fines to punish breaches, however a more comprehensive approach could make use of discounts on the cost of compliance either to incentivise specific practices, or to address issues arising from the fixed overheads associated with compliance being too significant for small businesses. While the specifics of how such a funding model could be devised are beyond the scope of this paper, given that data protection costs are usually not borne by those who benefit from data protection improvements, we believe that this could prove to be a fruitful area of future work.

Finally, our results have highlighted that smaller businesses are keen to outsource as a means of complying with data protection regulation. As a result, discount data protection should also be aiming to be consistent with third party services and offerings. Such solutions can potentially reduce overheads (e.g. costs of tooling, training, hiring, etc.), provide industry standard solutions to common data protection needs, or be embedded and provide added value to other services. We discuss more detailed issues of outsourcing data protection in Section 5.2.2.

Overall, the concept of discount data protection aims to support business and designers in addressing the data protection problems that matter most. We have described how designers and business leader perspectives can be taken into account, and outlined a series of recommendations aimed at supporting those stakeholders.

5.2.2 Outsourcing in Data Protection. As a common form of outsourcing, many product manufacturers use third-party Consent Management Platforms (CMP) to solicit consent to tracking cookies. Nouwens et al. [148] reported that 75% of top 10,000 websites in the UK outsource their cookie consent processes to use third-party CMPs. However, they found that the vast majority of websites

outsourcing consent notifications through CMPs (e.g., QuantCast, OneTrust and Cookiebot) deployed dark patterns (e.g., rejecting all tracking was "substantially more difficult than accepting it"). Researchers noted that popular CMP implementation wizards allow their clients to configure consent preferences, which indicates that dark patterns configurations could have been created by business owners [125].

Data protection best practices are frequently reported and adopted by thousands of small businesses [5]. Data protection best practices often consist of checklists (e.g., [4, 67]), guides (e.g., [35, 46]), and frameworks (e.g., [188]). While best practices provide efficient or prudent courses of action, they are not universally applicable. Best practices tend to come from top performers in an industry, which prompts smaller companies to follow them [182]. Regulatory experts are skeptical over 'best practices' adopted as a law practice (e.g., data protection) [185]. Data protection best practices that have worked for certain companies wouldn't necessarily work for all companies. As a result, we argue that business leaders should develop a very critical eye of whether best practices are appropriate beyond the fact they're already in use [139]. Business leaders should avoid benchmarking and instead routinely test their best practices to check that they hold over time and address any problems that arise.

Our results reveal that many of our business leaders have outsourced aspects of data protection compliance. Reports show businesses are increasingly dependent on third parties to comply with data protection [130]. Outsourcing has been proven to be beneficial and sometimes essential for small business leaders. For instance, the appointment of a new employee to act as a Data Protection Officer (DPO) has been reported to be an unrealistic burden for small businesses. Business leaders with owner-operated businesses or small teams who act as their own DPO may not be effective in ensuring GDPR compliance due to "*conflict of interest with possible other tasks and duties.*" [6]. As such, outsourcing the role of DPO to third-parties would be beneficial for small business leaders.

However, outsourcing data protection duties to third parties should be addressed very carefully. Third party compliance vendors tend to market their products as a way to avoid GDPR compliance entirely [56]. However, data protection mandates that business leaders are responsible for their third-party vendors' GDPR compliance and could be liable for third-party breaches. Moreover, they should define areas and activities in which the GDPR is in scope, and have third-party vendors agree and provide signed contractual assurances [96]. In the UK, the ICO mandates that third-party vendors cross-handling data with outsourcing businesses would find themselves equally liable for data breaches [131]. Some argue business leaders delegating data protection duties to third parties are in a more vulnerable position, as they are paying to outsource, as opposed to training their own staff [131].

The effectiveness of data protection practices is a critical aspect in successfully navigating the complex space of regulation and protection. While 'best practices' aim to help identify the most effective solutions, in reality they largely document the most common solutions, and moreover these tend to be contributed by companies that may not be representative of the wider industry. To help improve how business leaders gauge effectiveness, we argue (i) that data protection solutions need to clearly document their source and target industry, and that (ii) the scope of outsourced solutions and their relevance to data protection requirements needs to be clearer and designed to help with comparison. While these need more research, both these proposals arise from existing problems in judging effectiveness: (i) in evaluating the relevance of proposed solutions, and (ii) in comparing different offerings.

5.2.3 Code of Practice for Data Protection. At the current moment, it is difficult to distinguish companies that have effective (e.g., ethical, useful) data protection practices from those that merely claim to. Moreover, given the desire to rely on third parties for data protection, there is a question

mark over whether a subcontracted interaction that seems unethical to a user (e.g., a dark pattern) is perceived as an indication of unethical data protection practices in the original company. As a result of the difficulty in identifying truly effective (e.g., ethical, useful) data protection practices, there is a disincentive for companies to embrace these without further ways of signaling their authenticity.

We suggest that a voluntary code of practice for data protection could be developed. For instance, data protection organizations could provide certification schemes or indicators which can demonstrate that companies are behaving reasonably (e.g., ethically, responsibly) with consumer privacy and regulatory needs. Such schemes would be more challenging in smart home contexts due to various sectors of ecosystems, suppliers, manufacturers and third parties. However, they would improve practices of transparency, freedom of information and honesty in smart home companies.

Moreover, such a code of practice could help to address the issues arising where companies are in a conflict between the best interests of users and the best interests of the business. Having well-founded trust in data protection practices is necessary to ensure that users engage and businesses thrive, and having a code of practice which enshrines the importance of ethical behavior could provide a foundation from which data protection professionals would serve as guarantors of honest data protection practices – much in the same way that chartered professionals are trusted to deliver competence and ethical standards.

Finally, a code of practice for data protection could bolster designer responsibility and prompt designers to incorporate ethical design as part of their code of conduct (e.g., moral principles). We argue that ethical design would have many benefits, both short and long-term, that can improve smart home brands, products, and the wider sector. Moreover, this could inform the wider interest and consideration for Ethical Design more generally: we note that there has been a significant rise in interest in defining Ethical UX and Ethical Data Protection as seen in panel and audience questions at the ICO's Data Protection Practitioners' Conference 2019[3] and the Nielsen Norman Virtual UX Conference of December 2020[4].

5.2.4 Summary and Conclusion on UX of Data Protection . Our findings strongly support the suitability of UX expertise and practices in tackling the challenges we face in data protection, such as trust and honesty, alignment with business and regulatory goals, and the necessity of integrating data protection into established development processes. From this we have proposed a number of recommendations: discount data protection as a collection of techniques and practices aimed at pragmatic, cost-effective solutions; formulating a code of practice to help build a solid foundation of trust in the data relationships between users and businesses; and working towards economically viable solutions that fit the business realities and budgets of enterprises of all sizes.

We believe that these recommendations offer several key benefits over existing approaches:

(1) By putting the combination of user, regulatory and business needs into the hands of UX designers, we provide an opportunity to address the conflicts of interest which drive solutions that favor businesses over the needs of users (e.g., dark patterns).
(2) While UX designers can still be pressured to prioritize business interests, we argue that the ethical aspects of data protection could be made part of a code of conduct for data protection professionals, similar to how chartered professionals have ethical standards to which they are expected to adhere to. This would have the additional benefit of providing a new mechanism for building trust between users and businesses;

[3]https://www.youtube.com/watch?v=q6PWdR4zBUk
[4]https://www.youtube.com/watch?v=avhyz187Ypo

(3) By placing a strong emphasis on cost effectiveness and pragmatic solutions, discount data protection techniques will help UX designers in identifying and resolving potential conflicts early and effectively;
(4) By aligning to agile principles, discount data protection will provide appropriate techniques to support designers in crafting better experiences of data protection in ways that fit their existing ways of working.
(5) Finally, by working to offer competitive, cost-effective, or even subsidized solutions to fit the budgets of even the smallest companies, we can start to address the issue of large overheads associated with data protection compliance.

5.3 Implications for Design

Our results demonstrate a desire for data protection to be more friendly and honest for users, easier to navigate for designers, and cheaper and fairer for smaller business leaders. As such, we argue for the identification and adoption of future data protection practices that are safe, efficient and ethical. Such practices need to embody informed and valid consent from users without killing business models. Moreover, valid discount practices need to have manageable costs for business leaders and introduce solutions that can be safely outsourced to third parties.

Many industries with potential to cause harm (e.g., environmental harm) have a regulatory or voluntary code of conduct for the field. Just like the Medical Code of Ethics, we argue that the smart home industry should develop an ethical code of conduct with honesty, respect, and privacy as the core values. These values should be reflected in any data protection practices, project goals, and product features. Framing this ethical code of conduct would also be very useful for designers during all phases of UX design (e.g., research, analysis, design and testing). Similarly, it would be useful for business leaders making executive or strategic decisions.

Our designer interviews demonstrated that designers experienced challenges in finding the right balance between user needs and business goals. Limited resources and competing objectives in organizations were previously reported by Becker et al. [24–28]. UX designers act as the user's advocate in the design space. As a result, while they have to fulfill the business objectives, they are also empowered to maximize user needs (e.g., respect, satisfaction, positive ethical engagement), and act as a focal point for interventions in this space. UX designers often come across tight deadlines and limited resources to complete projects.

They are sometimes pressured to design interactions that are not compliant with their own values or practices. Having a clearly framed ethical code of conduct can liberate UX designers to challenge situations where business imperatives are unfairly disadvantageous to the user's best interests. We argue that UX designers are key to building a trusting relationship with users: they are able to reflect ethical and honest user values that are consistent with business goals and requirements.

Just like business leaders, designers need tools and support to help navigate data protection requirements. For instance, D01 and D02 hoped for more concrete UX guidelines for addressing GDPR requirements. Business lead B02 expressed the need to make GDPR easier for designers: "*We also need to make it easier for designers and developers to really implement the provisions of GDPR within software, rather than just making it a tick box exercise.*" Tools and solutions could be in the form of best practices, common APIs, third party solutions, visualizations and automation tools. Such tools should allow designers the means to respect the ethical dimensions of data protection and value exchange perspectives. For instance, our results showed that users favored automated data subject access experiences. UX-friendly tools that are able to guarantee repeatable, scalable (to small businesses), secure, and positive UX data access interactions are likely to be helpful for UX designers.

Any tools to assist with the design of data protection interactions will likely require underlying data models to allow their use to work as intended. For instance, automated data subject access tools could be enabled through machine learning models that can identify the right information without risking leakage of wrong information.

Rapid product life cycles in smart home products create challenges for designers – especially when navigating data protection requirements. UX designers have to balance user and business needs, and design data protection solutions in an iterative rapid development process. More tools and guidelines should be developed to assist UX designers to comply with data protection regulation in ways that enhance the user experience and facilitate ethical business practices.

Finally, users expressed a preference for automation as it allowed them to easily exercise their data protection rights. Automation is also likely to reduce data protection costs for business leaders. A report by McKinsey & Company stated that automated data protection solutions would result in reduced costs in the long run [136]. As such, we argue that automation should be further explored as it is easier for users, a market differentiator for the business leaders.

6 CONCLUSION

Smart homes carry significant security and privacy risks for home users and all inhabitants. Past work in smart homes often omits the interests of business leaders and the challenges of designing solutions in this space. To address this gap, we conducted a qualitative study with 7 users, 6 designers and 6 business leaders to investigate how they experience data protection from their perspectives. We found that business leaders and designers experienced significant difficulties in navigating data protection requirements and proposed the idea of discount data protection to address them. We conclude with the following recommendations:

6.1 Reframe data privacy as an ethical business dimension

Our business leader interviewees framed consent as a purely regulatory obligation. We recommend that smart home businesses reframe data practices as an ethical business dimension, instead of a regulatory overhead. For instance, data consent interactions can be approached from an ethical standpoint in addition to being a business and a regulatory one. Moreover, both designers and business leaders adopt discount practices (e.g., creating heuristics, taking shortcuts) to navigate the complexity of data protection regulation. Designers and business leaders should ensure that discount practices abide by ethical values (e.g., honesty, respect) that don't negatively affect users.

6.2 Improve the value proposition of data protection regulation

Our results showed that the value proposition of data protection could be more closely aligned with the needs of users, designers and business leaders. Data protection should provide a solid value proposition for all stakeholders: users, designers, and business leaders. Data protection practices should clearly explain to users the value of their personal information, be compatible with the strategic needs (e.g., reasonable cost) and resources (e.g., labor) of business leaders and incorporate discount usability principles (e.g., using low-fidelity prototyping) for designers.

6.3 Ensure that data protection best practices are effective

Our designer and business leader participants used best practices to address data protection requirements. Best practices tend to be contributed by larger companies, and may not be representative of e.g., the wider smart home industry. The practice of documenting and communicating best practices should be improved with more information about the provenance and applicability of the recommendations, to help designers and business leaders to critically evaluate and routinely examine the latest trends. Moreover, given the significant interest in outsourcing data protection

functions, greater efforts should be placed in providing sufficient information to allow comparison between different offerings.

6.4 Provide support for discount data protection practices

The practices reported by designers and business leaders reflect an appetite for cheaper, more cost effective solutions for data protection. While there is a perception among data protection experts that good data protection comes at a cost, our data suggests that business leaders and designers of smart home products perceive a gap in the current market for data protection solutions which offer effective options that are better suited to their budgets, timescales, and constraints. More support should be provided for discount data protection practices that fit the needs of business leaders and designers.

6.5 Support UX designers in balancing competing needs

Our UX Design interviewees balanced two different needs: business needs and user needs. UX designers are key to building a trusting relationship with users: they are able to reflect ethical values that are consistent with user and business needs. All our designers also worked in an agile manner, and needed appropriate practices and tools to represent the ethical dimension of data protection in a fair, open, and honest way.

ACKNOWLEDGMENTS

This research was supported by the 2018-2019 Information Commissioner's Office's (ICO) Grants Programme. George Chalhoub is funded by Fondation Sesam. The authors would like to thank Martin J. Kraemer, Ruba Abu-Salma, and the anonymous CSCW reviewers for their valuable input. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ICO, or any sponsor.

REFERENCES

[1] 2006. Self-Report Study. In *The SAGE Dictionary of Social Research Methods*. SAGE Publications, Ltd, 1 Oliver's Yard, 55 City Road, London England EC1Y 1SP United Kingdom. https://doi.org/10.4135/9780857020116.n186
[2] 2011. W3C Tracking Protection Working Group. https://www.w3.org/2011/tracking-protection/
[3] 2018. *EDPS Opinion on the legislative package 'A New Deal for Consumers'*. Technical Report. https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf
[4] 2018. GDPR best practices in 7 steps. https://blog.back4app.com/gdpr-best-practices/
[5] 2020. GDPR Best Practices. https://www.compliancejunction.com/gdpr-best-practices/
[6] A29 WP. 2021. WP243 ANNEX - FREQUENTLY ASKED QUESTIONS. https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf
[7] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*.
[8] Alessandro Acquisti. 2004. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce*. 21–29.
[9] Alessandro Acquisti, Leslie K. John, and George Loewenstein. 2013. What is privacy worth? *The Journal of Legal Studies* 42, 2 (2013), 249–274. Publisher: University of Chicago Press Chicago, IL.
[10] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. 2016. The economics of privacy. *Journal of economic Literature* 54, 2 (2016), 442–92.
[11] Noura Aleisa and Karen Renaud. 2017. Privacy of the Internet of Things: a systematic literature review. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.
[12] Alfonso Gómez-Arzola. 2018. Going Dark: The Ethical Implications of Willfully Dishonest Design. https://events.drupal.org/seattle2019/sessions/going-dark-ethical-implications-willfully-dishonest-design
[13] Sahar Allegue, Mouna Rhahla, and Takoua Abdellatif. 2019. Toward gdpr compliance in iot systems. In *International Conference on Service-Oriented Computing*. Springer, 130–141.
[14] Daniel Anderson and Richard von Seck. 2020. The GDPR and its impact on the web. *Network* 1 (2020).

[15] Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2017. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805* (2017).
[16] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. 2017. Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. *arXiv preprint arXiv:1708.05044* (2017).
[17] Rowland Atkinson and John Flint. 2001. Accessing hidden and hard-to-reach populations: Snowball research strategies. *Social research update* 33, 1 (2001), 1–4. Publisher: Guildord.
[18] Rebecca Balebako, Richard Shay, and Lorrie Faith Cranor. 2014. Is your inseam a biometric? a case study on the role of usability studies in developing public policy. *Proc. USEC* 14 (2014).
[19] 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. *European Journal of Information Systems* 24, 6 (2015), 624–644.
[20] Natã Miccael Barbosa, Joon S. Park, Yaxing Yao, and Yang Wang. 2019. " What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes. *Proc. Priv. Enhancing Technol.* 2019, 4 (2019), 211–231.
[21] Daniel Bastos, Fabio Giubilo, Mark Shackleton, and Fadi El-Moussa. 2018. GDPR privacy implications for the Internet of Things. In *4th Annual IoT Security Foundation Conference*, Vol. 4. 1–8.
[22] Lujo Bauer, Lorrie Faith Cranor, Simson L. Garfinkel, and David Gordon. 2020. *An Introduction to Privacy for Technology Professionals*. International Association of Privacy Professionals. Google-Books-ID: aubIygEACAAJ.
[23] Kathy Baxter, Catherine Courage, and Kelly Caine. 2015. *Understanding your users: a practical guide to user research methods*. Morgan Kaufmann.
[24] Adam Beautement, M. Angela Sasse, and Mike Wonham. 2008. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop (NSPW '08)*. ACM, NY, NY, USA, 47–58. https://doi.org/10.1145/1595676.1595684
[25] Ingolf Becker. 2019. *Measuring and Understanding Security Behaviours*. PhD Thesis. UCL (University College London).
[26] Ingolf Becker, Simon Parkin, and M. Angela Sasse. 2016. Combining Qualitative Coding and Sentiment Analysis: Deconstructing Perceptions of Usable Security in Organisations. 43–53. https://www.usenix.org/conference/laser2016/program/presentation/becker
[27] Ingolf Becker, Simon Parkin, and M. Angela Sasse. 2017. Finding security champions in blends of organisational culture. *Proc. USEC* 11 (2017).
[28] Ingolf Becker, Simon Parkin, and M. Angela Sasse. 2017. Measuring the Success of Context-Aware Security Behaviour Surveys. 77–86. https://www.usenix.org/conference/laser2017/presentation/becker
[29] Greg Bensinger. 2021. Opinion | Stopping the Manipulation Machines. *The NY Times* (April 2021). https://www.nytimes.com/2021/04/30/opinion/dark-pattern-internet-ecommerce-regulation.html
[30] Ross Bentley. 2008. Data protection: strictly confidential. https://www.personneltoday.com/hr/data-protection-strictly-confidential/
[31] Johanna Bergman, Thomas Olsson, Isabelle Johansson, and Kirsten Rassmus-Gröhn. 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, 20–36.
[32] H. Russell Bernard and Harvey Russell Bernard. 2013. *Social Research Methods: Qualitative and Quantitative Approaches*. SAGE. Google-Books-ID: 7sZHuhyzBNQC.
[33] Stefan Berthold and Rainer Böhme. 2010. Valuating privacy with option pricing theory. In *Economics of information security and privacy*. Springer, 187–209.
[34] Peter Birmingham and David Wilkinson. 2003. *Using research instruments: A guide for researchers*. Routledge.
[35] Bridgeline Digital. 2018. GDPR Compliance Best Practices Guide. https://www.bridgeline.com/resources/gdpr-best-practices-guide
[36] Dennis Basil Bromley and Dennis Basil Bromley. 1986. *The case-study method in psychology and related disciplines*. Wiley Chichester.
[37] Ian Buckley. 2018. How Could the GDPR Affect Smart Home Devices? 2 Examples of Downed Services. https://www.makeuseof.com/tag/smart-home-devices-gdpr/ Section: Security.
[38] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2016. On Privacy and Security Challenges in Smart Connected Homes. In *2016 European Intelligence and Security Informatics Conference (EISIC)*. 172–175. https://doi.org/10.1109/EISIC.2016.044
[39] Rainer Böhme and Stefan Köpsell. 2010. Trained to accept? a field experiment on consent dialogs. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, NY, NY, USA, 2403–2406. https://doi.org/10.1145/1753326.1753689
[40] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (2016), 237–254.

[41] C N Trueman. 2015. Structured Interviews. https://www.historylearningsite.co.uk/sociology/research-methods-in-sociology/structured-interviews/
[42] Sara Cannizzaro, Rob Procter, Sinong Ma, and Carsten Maple. 2020. Trust in the smart home: Findings from a nationally representative survey in the UK. *Plos one* 15, 5 (2020), e0231615. Publisher: Public Library of Science San Francisco, CA USA.
[43] George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. 2020. 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)*. 185–204.
[44] Kathy Charmaz. 2006. *Constructing grounded theory: A practical guide through qualitative analysis*. sage.
[45] Abhik Chaudhuri. 2016. Internet of things data protection and privacy in the era of the General Data Protection Regulation. *Journal of Data Protection & Privacy* 1, 1 (Dec. 2016), 64–75.
[46] claudiu. 2018. 6 Key Steps to Ensure GDPR Compliance - The Steps You Need to Take. https://www.codeinwp.com/blog/gdpr-compliance/
[47] Gary Clayton. 2002. Safeguarding the world's new currency. *Information Management Journal* 36, 3 (June 2002), 18–24. https://www.proquest.com/docview/227759723/abstract/E13F13BB279143E7PQ/1 Num Pages: 6 Place: Lenexa, United States Publisher: ARMA International.
[48] Federal Trade Commission. 2015. Internet of things: Privacy & security in a connected world. *Washington, DC: Federal Trade Commission* (2015).
[49] Gregory Conti and Edward Sobiesk. 2010. Malicious interface design: exploiting the user. In *Proceedings of the 19th international conference on World wide web (WWW '10)*. ACM, NY, NY, USA, 271–280. https://doi.org/10.1145/1772690.1772719
[50] Juliet Corbin and Anselm Strauss. 2014. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications.
[51] Norwegian Consumer Council. 2018. Deceived by design, How tech companies use dark patterns to discourage us from exercising our rights to privacy. *Norwegian Consumer Council Report* (2018).
[52] K. L. Courtney. 2008. Privacy and Senior Willingness to Adopt Smart Home Information Technology in Residential Care Facilities. *Methods of Information in Medicine* 47, 1 (2008), 76–81. https://doi.org/10.3414/ME9104 Publisher: Schattauer GmbH.
[53] L. Cranor, T. Rabin, V. Shmatikov, S. Vadhan, and D. Weitzner. 2015. Towards a Privacy Research Roadmap for the Computing Community: A white paper prepared for the computing community consortium committee of the computing research association. (2015).
[54] Lorrie Faith Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.* 10 (2012), 273.
[55] Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. 2006. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction* 13, 2 (June 2006), 135–178. https://doi.org/10.1145/1165734.1165735
[56] Joe Curtis. 2017. Don't outsource your GDPR compliance. https://www.cloudpro.co.uk/leadership/6834/dont-outsource-your-gdpr-compliance
[57] Victor Dahl and Marco Österlin. 2020. *Impact of GDPR on Data Sharing Behavior of Smart Home Users*. Malmö universitet/Teknik och samhälle. http://urn.kb.se/resolve?urn=urn:nbn:se:mau:diva-20336
[58] Cindy Dampier. 2019. Cyber Week shoppers sign up, impulse buy like crazy - City. https://digitaledition.chicagotribune.com/tribune/article_popover.aspx?guid=0affa34d-2165-4424-a65a-6d6d2111d1e0
[59] Avirup Dasgupta, Asif Qumer Gill, and Farookh Hussain. 2019. Privacy of IoT-enabled smart home systems. In *Internet of Things (IoT) for automated and smart applications*. IntechOpen.
[60] Scott Davidoff, Min Kyung Lee, Charles Yiu, John Zimmerman, and Anind K. Dey. 2006. Principles of Smart Home Control. In *UbiComp 2006: Ubiquitous Computing (Lecture Notes in Computer Science)*, Paul Dourish and Adrian Friday (Eds.). Springer, Berlin, Heidelberg, 19–34. https://doi.org/10.1007/11853565_2
[61] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2018. We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. *arXiv preprint arXiv:1808.05096* (2018).
[62] John Deighton and Peter A. Johnson. 2013. The Value of Data: Consequences for insight, innovation and efficiency in the US economy. *Data-Driven Marketing Institute* 14 (2013), 1–105.
[63] Nicola Dell, Vidya Vaidyanathan, Indrani Medhi, Edward Cutrell, and William Thies. 2012. "Yours is better!": participant response bias in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, NY, NY, USA, 1321–1330. https://doi.org/10.1145/2207676.2208589
[64] Círculo de Directores. 2019. The trust crisis: Facebook, Boeing and too many other firms are losing the public's faith. Can they regain it? http://www.circulodedirectores.org/2019/07/18/the-trust-crisis-facebook-boeing-and-too-many-other-firms-are-losing-the-publics-faith-can-they-regain-it/ Section: Governance.

[65] ISO DIS. 2010. 9241-210: 2010. Ergonomics of human system interaction-Part 210: Human-centred design for interactive systems (formerly known as 13407). *International Standardization Organization (ISO). Switzerland* (2010).
[66] Stuart E. Dreyfus and Hubert L. Dreyfus. 1980. *A five-stage model of the mental activities involved in directed skill acquisition.* Technical Report. California Univ Berkeley Operations Research Center.
[67] DUN & BRADSTREET. 2017. 7 Best Practices for Effective GDPR Compliance. https://www.dnb.co.uk/perspectives/finance-credit-risk/7-best-practices-gdpr-compliance.html
[68] Stacy-Ann Elvy. 2017. Paying for privacy and the personal data economy. *Colum. L. Rev.* 117 (2017), 1369.
[69] Jean Faugier and Mary Sargeant. 1997. Sampling hard to reach populations. *Journal of Advanced Nursing* 26, 4 (1997), 790–797. https://doi.org/10.1046/j.1365-2648.1997.00371.x _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1046/j.1365-2648.1997.00371.x.
[70] Adrienne Porter Felt, Serge Egelman, Matthew Finifter, Devdatta Akhawe, and David A. Wagner. 2012. How to Ask for Permission. *HotSec* 12 (2012), 7–7.
[71] Finjan Team. 2018. Who Benefits from GDPR? Large American Tech Companies for one. https://blog.finjan.com/who-benefits-from-gdpr/
[72] Huiqing Fu, Yulong Yang, Nileema Shingte, Janne Lindqvist, and Marco Gruteser. 2014. A field study of run-time location access disclosures on android smartphones. *Proc. USEC* 14 (2014).
[73] Eoghan Furey and Juanita Blue. 2019. Can i trust her? Intelligent personal assistants and GDPR. In *2019 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 1–6.
[74] DataGuidance Future of Privacy Forum. 2019. Comparing privacy laws: GDPR v. CCPA. *Comparing Privacy Laws: GDPR vs CCPA* (2019), 9. https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf
[75] Anuroop Gaddam, Subhas Chandra Mukhopadhyay, and Gourab Sen Gupta. 2011. Trial & experimentation of a smart home monitoring system for elderly. In *2011 IEEE International Instrumentation and Measurement Technology Conference*. IEEE, 1–6.
[76] Carrie Gates and Peter Matthews. 2014. Data Is the New Currency. In *Proceedings of the 2014 New Security Paradigms Workshop (NSPW '14)*. ACM, NY, NY, USA, 105–116. https://doi.org/10.1145/2683467.2683477
[77] Christine Geeng and Franziska Roesner. 2019. Who's In Control?: Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 268.
[78] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri, and Gianmarco Baldini. 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)*. 1292–1297. https://doi.org/10.23919/MIPRO.2017.7973622
[79] Kambiz Ghazinour and Emil Shirima. 2018. Privacy for Security Monitoring Systems. *3rd Workshop on Inclusive Privacy and Security (WIPS)* (Aug. 2018).
[80] Marco Ghiglieri, Melanie Volkamer, and Karen Renaud. 2017. Exploring consumers' attitudes of smart TV related privacy risks. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 656–674.
[81] Olga Gkotsopoulou, Elisavet Charalambous, Konstantinos Limniotis, Paul Quinn, Dimitris Kavallieros, Gohar Sargsyan, Stavros Shiaeles, and Nicholas Kolokotronis. 2019. Data Protection by Design for cybersecurity systems in a Smart Home environment. In *2019 IEEE Conference on Network Softwarization (NetSoft)*. 101–109. https://doi.org/10.1109/NETSOFT.2019.8806694
[82] Avi Goldfarb and Catherine E. Tucker. 2011. Online advertising, behavioral targeting, and privacy. *Commun. ACM* 54, 5 (2011), 25–27.
[83] Leo A. Goodman. 1961. Snowball sampling. *The annals of mathematical statistics* (1961), 148–170.
[84] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, NY, NY, USA, 1–14. https://doi.org/10.1145/3173574.3174108
[85] Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. 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)*. ACM, NY, NY, USA, 1–18. https://doi.org/10.1145/3411764.3445779
[86] Jens Grossklags and Alessandro Acquisti. 2007. When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information.. In *WEIS*.
[87] Jens Grossklags and Nathan Good. 2007. Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers. In *Financial Cryptography and Data Security (Lecture Notes in Computer Science)*, Sven Dietrich and Rachna Dhamija (Eds.). Springer, Berlin, Heidelberg, 341–355. https://doi.org/10.1007/978-3-540-77366-5_31
[88] Greg Guest, Arwen Bunce, and Laura Johnson. 2006. How many interviews are enough? An experiment with data saturation and variability. *Field methods* 18, 1 (2006), 59–82.

[89] Manu Gupta, Stephen S. Intille, and Kent Larson. 2009. Adding GPS-Control to Traditional Thermostats: An Exploration of Potential Energy Savings and Design Challenges. In *Pervasive Computing (Lecture Notes in Computer Science)*, Hideyuki Tokuda, Michael Beigl, Adrian Friday, A. J. Bernheim Brush, and Yoshito Tobe (Eds.). Springer, Berlin, Heidelberg, 95–114. https://doi.org/10.1007/978-3-642-01516-8_8

[90] Hatchd. 2017. The dangers of dishonest design. https://www.hatchd.com.au/blog/the-dangers-of-dishonest-design

[91] 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). 255–272. https://www.usenix.org/conference/usenixsecurity18/presentation/he

[92] Weijia He, Valerie Zhao, Olivia Morkved, Sabeeka Siddiqui, Earlence Fernandes, Josiah Hester, and Blase Ur. [n.d.]. SoK: Context Sensing for Access Control in the Adversarial Home IoT. ([n. d.]).

[93] Dennis D. Hirsch. 2013. The glass house effect: Big Data, the new oil, and the power of analogy. *Me. L. Rev.* 66 (2013), 373.

[94] Beth Hutchens, Gavin Keene, and David Stieber. 2017. Regulating the Internet of Things: Protecting the" Smart" Home. (2017). Publisher: University of Washington Technology Law and Public Policy Clinic.

[95] S.S. Intille. 2002. Designing a home of the future. *IEEE Pervasive Computing* 1, 2 (April 2002), 76–82. https://doi.org/10.1109/MPRV.2002.1012340

[96] Luke Irwin. 2020. The GDPR: Why you need to review your third-party service providers' security. https://www.itgovernance.eu/blog/en/the-gdpr-why-you-need-to-review-your-third-party-service-providers-security

[97] Dean Ivancevic. 2020. *Privacy and security of IoT : A smart home perspective.* http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-99071

[98] 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. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (Dec. 2018), 171:1–171:28. https://doi.org/10.1145/3287049

[99] Carlos Jensen and Colin Potts. 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '04)*. ACM, NY, NY, USA, 471–478. https://doi.org/10.1145/985692.985752

[100] Nicola Jentzsch, Sören Preibusch, and Andreas Harasser. 2012. Study on monetising privacy: An economic model for pricing personal information. *ENISA, Feb* 1, 1 (2012).

[101] Annabel Bhamani Kajornboon. 2005. Using interviews as research instruments. *E-journal for Research Teachers* 2, 1 (2005), 1–9.

[102] C. Kalapesi. 2013. Unlocking the value of personal data: From collection to usage. In *World Economic Forum technical report.*

[103] Smirity Kaushik, Yaxing Yao, Pierre Dewitte, and Yang Wang. 2021. "How I Know For Sure": People's Perspectives on Solely Automated {Decision-Making} ({{{{{SADM}}}}}). 159–180. https://www.usenix.org/conference/soups2021/presentation/kaushik

[104] Eddie Keane. 2018. The GDPR and Employee's Privacy: Much Ado but Nothing New. *King's Law Journal* 29, 3 (2018), 354–363. Publisher: Taylor & Francis.

[105] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, NY, NY, USA, 1573–1582. https://doi.org/10.1145/1753326.1753561

[106] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, NY, NY, USA, 3393–3402. https://doi.org/10.1145/2470654.2466466

[107] Cameron F. Kerry and John B. Morris. 2019. Why Data Ownership Is the Wrong Approach to Protecting Privacy. *Brookings Institution, June* 26 (2019).

[108] Keumars Afifi-Sabet. 2019. Research unearths inadvertent GDPR business benefits. https://www.itpro.co.uk/general-data-protection-regulation-gdpr/33154/research-unearths-inadvertent-gdpr-business-benefits

[109] Cory D. Kidd, Robert Orr, Gregory D. Abowd, Christopher G. Atkeson, Irfan A. Essa, Blair MacIntyre, Elizabeth Mynatt, Thad E. Starner, and Wendy Newstetter. 1999. The Aware Home: A Living Laboratory for Ubiquitous Computing Research. In *Cooperative Buildings. Integrating Information, Organizations, and Architecture (Lecture Notes in Computer Science)*, Norbert A. Streitz, Jane Siegel, Volker Hartkopf, and Shin'ichi Konomi (Eds.). Springer, Berlin, Heidelberg, 191–198. https://doi.org/10.1007/10705432_17

[110] Benjamin Koskei and Catherine Simiyu. 2015. Role of interviews, observation, pitfalls and ethical issues in qualitative research methods. *Journal of Educational Policy and Entrepreneurial Research* 2, 3 (2015), 108–117.

[111] Oksana Kulyk, Annika Hilt, Nina Gerber, and Melanie Volkamer. 2018. this website uses cookies": Users' perceptions and reactions to the cookie disclaimer. In *European Workshop on Usable Security (EuroUSEC)*.

[112] Sri Kurniawan. 2004. Interaction design: Beyond human–computer interaction by Preece, Sharp and Rogers (2001), ISBN 0471492787. *Universal Access in the Information Society* 3, 3 (Oct. 2004), 289–289. https://doi.org/10.1007/s10209-004-0102-1

[113] Kyle Gawley. 2013. Dark Patterns - The Art of Online Deception. https://blog.kylegawley.com/dark-patterns-the-art-of-online-deception/

[114] Carine Lallemand, Guillaume Gronier, and Vincent Koenig. 2015. User experience: A concept without consensus? Exploring practitioners' perspectives through an international survey. *Computers in Human Behavior* 43 (Feb. 2015), 35–48. https://doi.org/10.1016/j.chb.2014.10.048

[115] Flavio Lamenza. 2020. Stop calling these Dark Design Patterns or Dark UX — these are simply a**hole designs. https://uxdesign.cc/stop-calling-these-dark-design-patterns-or-dark-ux-these-are-simply-asshole-designs-bb02df378ba

[116] Marc Langheinrich. 2001. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. In *Ubicomp 2001: Ubiquitous Computing (Lecture Notes in Computer Science)*, Gregory D. Abowd, Barry Brumitt, and Steven Shafer (Eds.). Springer, Berlin, Heidelberg, 273–291. https://doi.org/10.1007/3-540-45427-6_23

[117] Marc Langheinrich. 2002. A Privacy Awareness System for Ubiquitous Computing Environments. In *UbiComp 2002: Ubiquitous Computing (Lecture Notes in Computer Science)*, Gaetano Borriello and Lars Erik Holmquist (Eds.). Springer, Berlin, Heidelberg, 237–245. https://doi.org/10.1007/3-540-45809-3_19

[118] Kenneth C. Laudon. 1996. Markets and privacy. *Commun. ACM* 39, 9 (1996), 92–104. Publisher: ACM NY, NY, USA.

[119] Michael Lesk. 2012. The Price of Privacy. *IEEE Security Privacy* 10, 5 (Sept. 2012), 79–81. https://doi.org/10.1109/MSP.2012.133 Conference Name: IEEE Security Privacy.

[120] Brian Y. Lim, Anind K. Dey, and Daniel Avrahami. 2009. *Why and why not* explanations improve the intelligibility of context-aware intelligent systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. ACM, Boston, MA, USA, 2119–2128. https://doi.org/10.1145/1518701.1519023

[121] Joseph Galen Lindley, Paul Coulton, Haider Akmal, and Brandin Hanson Knowles. 2017. Anticipating GDPR in Smart Homes Through Fictional Conversational Objects. (2017).

[122] Nicole Lindsey. 2019. Personal Data Marketplaces Might Not Be the Best Solution for Data Privacy. https://www.cpomagazine.com/data-privacy/personal-data-marketplaces-might-not-be-the-best-solution-for-data-privacy/ Section: Data Privacy.

[123] John Liu. 2018. Europe's GDPR causes malfunction of smart home devices: Report - asmag.com. https://www.asmag.com/showpost/26577.aspx

[124] Yuqi Liu, Yan Gan, Yao Song, and Jing Liu. 2021. What Influences the Perceived Trust of a Voice-Enabled Smart Home System: An Empirical Study. *Sensors* 21, 6 (Jan. 2021), 2037. https://doi.org/10.3390/s21062037 Number: 6 Publisher: Multidisciplinary Digital Publishing Institute.

[125] Natasha Lomas. 2020. Cookie consent tools are being used to undermine EU privacy rules, study suggests. https://social.techcrunch.com/2020/01/10/cookie-consent-tools-are-being-used-to-undermine-eu-privacy-rules-study-suggests/

[126] Mark MacCarthy. 2018. Privacy Is Not A Property Right In Personal Information. https://www.forbes.com/sites/washingtonbytes/2018/11/02/privacy-is-not-a-property-right-in-personal-information/

[127] Dominique Machuletz and Rainer Böhme. 2020. Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020), 481–498. https://doi.org/doi:10.2478/popets-2020-0037

[128] Vincenzo Mangini, Irina Tal, and Arghir-Nicolae Moldovan. 2020. An empirical study on the impact of GDPR and right to be forgotten - organisations and users perspective. In *Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20)*. ACM, NY, NY, USA, 1–9. https://doi.org/10.1145/3407023.3407080

[129] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–32.

[130] Kevin F Mccloskey. 2019. Current trends in outsourcing and addressing third party risk. (2019), 5. https://www2.deloitte.com/content/dam/Deloitte/no/Documents/risk/Current%20trends%20in%20outsourcing%20and%20addressing%20third%20party%20risk.pdf

[131] Grant McGregor. 2018. GDPR, Outsourcing and Third-Party Data - what you need to know. https://blog.grantmcgregor.co.uk/2018/gdpr-outsourcing-and-third-party-data-what-you-need-to-know-before-the-sky-falls-in-this-friday

[132] Mary L. McHugh. 2012. Interrater reliability: the kappa statistic. *Biochemia medica: Biochemia medica* 22, 3 (2012), 276–282. Publisher: Medicinska naklada.

[133] 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. In *Pervasive Computing (Lecture Notes in Computer Science)*, Judy Kay, Paul Lukowicz, Hideyuki Tokuda, Patrick Olivier, and Antonio Krüger (Eds.). Springer, Berlin, Heidelberg, 143–160. https://doi.org/10.1007/978-3-642-31205-2_10

[134] Sharan B. Merriam. 1988. *Case study research in education: A qualitative approach.* Jossey-Bass, San Francisco, CA, US.
[135] Sharan B. Merriam. 1998. *Qualitative Research and Case Study Applications in Education. Revised and Expanded from" Case Study Research in Education.".* ERIC.
[136] Daniel Mikkelsen, Kayvaun Rowshankish, Henning Soller, and Kalin Stamenov. 2017. *Tackling GDPR compliance before time runs out.* Technical Report. McKinsey Global Institute.
[137] Luke Miller. 2015. *The Practitioner's Guide to User Experience Design.* Grand Central Publishing. Google-Books-ID: zCLqBQAAQBAJ.
[138] Mozilla Foundation. 2020. *Privacy Not Included: A Buyer's Guide for Connected Products. https://foundation.mozilla.org/en/privacynotincluded/facebook-portal/
[139] Mike Myatt. 2012. Best Practices - Aren't. https://www.forbes.com/sites/mikemyatt/2012/08/15/best-practices-arent/ Section: Leadership.
[140] 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. In *Thirteenth Symposium on Usable Privacy and Security (${SOUPS$}$ 2017)*. 399–412.
[141] Arvind Narayanan, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. 2020. Dark patterns: past, present, and future. *Commun. ACM* 63, 9 (Aug. 2020), 42–47. https://doi.org/10.1145/3397884
[142] Jack Narcotta. 2018. Smart Home Surveillance Camera Market Analysis and Forecast.
[143] Jakob Nielsen. 1989. Usability engineering at a discount. In *Proceedings of the third international conference on human-computer interaction on Designing and using human-computer interfaces and knowledge based systems (2nd ed.)*. Elsevier Science Inc., USA, 394–401.
[144] Jakob Nielsen. 1994. *Usability engineering.* Morgan Kaufmann.
[145] Jakob Nielsen. 2009. Discount usability: 20 years. *Jakob Nielsen's Alertbox Available at http://www. useit. com/alertbox/discount-usability. html [Accessed 23 January 2012]* (2009).
[146] Jacob Nielsen. 2018. Agile Development Projects and Usability. https://www.nngroup.com/articles/agile-development-and-usability/
[147] Jakob Nielsen and Rolf Molich. 1990. Heuristic evaluation of user interfaces. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 249–256.
[148] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. ACM, NY, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376321
[149] Norbert Nthala and Ivan Flechais. 2018. Informal support networks: an investigation into home data security practices. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 63–82.
[150] OECD. 2013. Exploring the economics of personal data. *OECD Digital Economy Papers 220* (2013). Publisher: Paris, France: OECD.
[151] Jeungmin Oh and Uichin Lee. 2015. Exploring UX issues in Quantified Self technologies. In *2015 Eighth International Conference on Mobile Computing and Ubiquitous Networking (ICMU)*. 53–59. https://doi.org/10.1109/ICMU.2015.7061028
[152] David Parkins. 2017. The world's most valuable resource is no longer oil, but data. *The economist* 6 (2017).
[153] Erica Perry. 2018. Lack Of Trust Costs Brands $2.5 Trillion Per Year: Study. https://socialmediaweek.org/blog/2018/02/lack-trust-costs-brands-2-5-trillion-per-year-study/ Section: Business.
[154] Edith Ramirez, Maureen K. Ohlhausen, and Terrell McSweeny. 2017. *Cross-Device Tracking.* Technical Report. An FTC Staff Report, FEDERAL TRADE COMMISSION.
[155] Sebastian Rieger and Caroline Sinders. 2020. Dark Patterns: Regulating Digital Design. (2020), 28. https://www.stiftung-nv.de/sites/default/files/dark.patterns.english.pdf
[156] Biljana L. Risteska Stojkoska and Kire V. Trivodaliev. 2017. A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production* 140 (Jan. 2017), 1454–1464. https://doi.org/10.1016/j.jclepro.2016.10.006
[157] Jeffrey Ritter and Anna Mayer. 2017. Regulating data as property: a new construct for moving forward. *Duke L. & Tech. Rev.* 16 (2017), 220.
[158] Claire Rowland. 2018. UX AND SERVICE DESIGN FOR CONNECTED PRODUCTS. https://iotuk.org.uk/wp-content/uploads/2018/06/UX-and-Service-Design-IoTUK.pdf
[159] Georgia Robins Sadler, Hau-Chen Lee, Rod Seung-Hwan Lim, and Judith Fullerton. 2010. Research Article: Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy. *Nursing & Health Sciences* 12, 3 (2010), 369–374. https://doi.org/10.1111/j.1442-2018.2010.00541.x _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1442-2018.2010.00541.x.
[160] Eric Schaffer and Apala Lahiri. 2013. *Institutionalization of UX: A Step-by-Step Guide to a User Experience Practice.* Addison-Wesley. Google-Books-ID: XIpTAgAAQBAJ.

[161] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security (${$SOUPS$}$ 2015)*. 1–17.
[162] Nick Kostov and Sam Schechner. 2019. GDPR Has Been a Boon for Google and Facebook. *Wall Street Journal* (June 2019). https://www.wsj.com/articles/gdpr-has-been-a-boon-for-google-and-facebook-11560789219
[163] Klaus Schwab, Alan Marcus, J. O. Oyola, William Hoffman, and Michele Luzi. 2011. Personal data: The emergence of a new asset class. In *An Initiative of the World Economic Forum*.
[164] Clive Seale. 1999. Quality in qualitative research. *Qualitative inquiry* 5, 4 (1999), 465–478.
[165] Reinhard Sefelin, Manfred Tscheligi, and Verena Giller. 2003. Paper prototyping - what is it good for? a comparison of paper- and computer-based low-fidelity prototyping. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems (CHI EA '03)*. ACM, NY, NY, USA, 778–779. https://doi.org/10.1145/765891.765986
[166] Xiuyan Shao and Harri Oinas-Kukkonen. 2019. How Does GDPR (General Data Protection Regulation) Affect Persuasive System Design: Design Requirements and Cost Implications. In *Persuasive Technology: Development of Persuasive and Behavior Change Support Systems (Lecture Notes in Computer Science)*, Harri Oinas-Kukkonen, Khin Than Win, Evangelos Karapanos, Pasi Karppinen, and Eleni Kyza (Eds.). Springer International Publishing, Cham, 168–173. https://doi.org/10.1007/978-3-030-17287-9_14
[167] Natasha Singer. 2016. When Websites Won't Take No for an Answer. *The NY Times* (May 2016). https://www.nytimes.com/2016/05/15/technology/personaltech/when-websites-wont-take-no-for-an-answer.html
[168] Rob Sobers. 2019. GDPR's Impact So Far: Must-Know Stats and Takeaways - Varonis. https://www.varonis.com/blog/gdpr-effect-review/ Section: Compliance & Regulation.
[169] Than Htut Soe, Oda Elise Nordberg, Frode Guribye, and Marija Slavkovik. 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)*. ACM, NY, NY, USA, 1–12. https://doi.org/10.1145/3419249.3420132
[170] John M. Spartz and Ryan P. Weber. 2016. User experience as a driver of entrepreneurial innovation. In *2016 IEEE International Professional Communication Conference (IPCC)*. 1–7. https://doi.org/10.1109/IPCC.2016.7740486
[171] Sarah Spiekermann, Alessandro Acquisti, Rainer Böhme, and Kai-Lung Hui. 2015. The challenges of personal data markets and privacy. *Electronic markets* 25, 2 (2015), 161–167.
[172] Ivan Stepanov. 2020. Introducing a property right over data in the EU: the data producer's right – an evaluation. *International Review of Law, Computers & Technology* 34, 1 (Jan. 2020), 65–86. https://doi.org/10.1080/13600869.2019.1631621
[173] Anselm Strauss and Juliet Corbin. 1998. *Basics of qualitative research techniques*. Sage publications Thousand Oaks, CA.
[174] Anselm Strauss and Juliet M. Corbin. 1997. *Grounded theory in practice*. Sage.
[175] IT Governance Privacy Team. 2020. *EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition*. IT Governance Ltd. Google-Books-ID: LicDEAAAQBAJ.
[176] Max-R. Ulbricht and Frank Pallas. 2018. YaPPL - A Lightweight Privacy Preference Language for Legally Sufficient and Automated Consent Provision in IoT Scenarios. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology (Lecture Notes in Computer Science)*, Joaquin Garcia-Alfaro, Jordi Herrera-Joancomartí, Giovanni Livraga, and Ruben Rios (Eds.). Springer International Publishing, Cham, 329–344. https://doi.org/10.1007/978-3-030-00305-0_23
[177] Lachlan Urquhart and Jiahong Chen. 2020. *On the Principle of Accountability: Challenges for Smart Homes & Cybersecurity*. SSRN Scholarly Paper ID 3629119. Social Science Research Network, Rochester, NY. https://papers.ssrn.com/abstract=3629119
[178] Lachlan Urquhart and Jiahong Chen. 2020. Stuck in The Middle With U (Sers): Domestic Data Controllers & Demonstrations of Accountability in Smart Homes. *ETHICOMP 2020* (2020), 211.
[179] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 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)*. ACM, NY, NY, USA, 973–990. https://doi.org/10.1145/3319535.3354212
[180] Marc van Lieshout. 2014. The value of personal data. In *IFIP International Summer School on Privacy and Identity Management*. Springer, 26–38.
[181] Winfried Veil. 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. https://papers.ssrn.com/abstract=3305056
[182] Freek Vermeulen. 2017. When 'Best Practices' Backfire. *Harvard Business Review* (Nov. 2017). https://hbr.org/podcast/2017/11/when-best-practices-backfire Section: Business processes.
[183] Tony Vila, Rachel Greenstadt, and David Molnar. 2003. Why we can't be bothered to read privacy policies models of privacy economics as a lemons market. In *Proceedings of the 5th international conference on Electronic commerce (ICEC*

'03). ACM, NY, NY, USA, 403–407. https://doi.org/10.1145/948005.948057

[184] James Vincent. 2021. California bans 'dark patterns' that trick users into giving away their personal data. https://www.theverge.com/2021/3/16/22333506/california-bans-dark-patterns-opt-out-selling-data

[185] William Vogeler. 2017. Can 'Best Practices' Be Bad for Your Law Practice? https://blogs.findlaw.com/strategist/2017/11/can-best-practices-be-bad-for-your-law-practice.html

[186] Mark Warner and Debra Fischer. 2020. *Senators Introduce Bipartisan Legislation to Ban Manipulative "Dark Patterns"*.

[187] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2017. Benefits and risks of smart home technologies. *Energy Policy* 103 (2017), 72–83.

[188] Simon Wilson. 2018. A framework for security technology cohesion in the era of the GDPR. *Computer Fraud & Security* 2018, 12 (Dec. 2018), 8–11. https://doi.org/10.1016/S1361-3723(18)30119-2

[189] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust Me: Doubts and Concerns Living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems (DIS '16)*. ACM, NY, NY, USA, 427–434. https://doi.org/10.1145/2901790.2901890

[190] Yaxing Yao. 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)*. ACM, NY, NY, USA, 98–101. https://doi.org/10.1145/3311957.3361863

[191] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. 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*. ACM, NY, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428

[192] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 59:1–59:24. https://doi.org/10.1145/3359161

[193] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 65–80.

[194] 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. In *28th USENIX Security Symposium (USENIX Security 19)*. 159–176.

[195] Kai Zhao and Lina Ge. 2013. A survey on the internet of things security. In *2013 Ninth international conference on computational intelligence and security*. IEEE, 663–667.

[196] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 200.

Received January 2022; revised April 2022; accepted May 2022

A GROUNDED THEORY CODEBOOK

Users	Designers	Business Leaders
automated data access requests	agile product development	amount of fines of non-compliance
awareness of company practices	arranging structured meetings	appointing a data protection officer
awareness of data collection practices	communicating UX benefits	automated decision
becoming more aware of data rights	communicating user behaviors	automatically authenticating users
blurring privacy	communicating user needs	collecting personal data
comprehension of requested permissions	communicating user privacy concerns	communicating to users
consumer privacy preferences	communicating with stakeholders	compliance overhead
cumbersome privacy options	conducting heuristic evaluation	cost of compliance is high
data breach concerns	conducting user research	cost of compliance is manageable
data privacy concerns	conducting design workshops	cost of compliance is unknown
device installation	conducting user interviews	cost of compliance is unrecognized
difficulty authenticating	recruiting users	creating privacy notices
difficulty rejecting consent	prototyping products	cutting corners
distrust of data collection practices	testing products	data protection by design
distrust of data processing practices	safeguarding individual rights	data protection compliance
distrust of smart home manufacturers	understanding technical limitations	data protection inconsistent between EU countries
erosion of trust	understanding organizational limitations	data protection inconsistent between UK and US
excessive permission requests	continuously improving smart products	data protection not applicable
exercising data rights	continuously conducting user research	data protection not relevant
experiencing dark patterns	improving user trust	data protection practices
experiencing detriment	improve consent interactions	data protection requirements
experiencing forced interactions	improve transparency	data protection roles
experiencing 'creepy' interactions	data protection compliance	data protection tools
fearing personal data will be sold	data protection features	educating staff
fear over collected personal data	data protection by design	facilitating data access procedures
feeling confused	data protection requirements	facilitating data access requests
feeling disappointed	privacy requirements	fines and penalties
feeling frustrated	privacy settings	gathering data securely
feeling overwhelmed	privacy threats	good judgment
feeling tricked	data protection responsibilities	hiring regulatory staff
hidden privacy defaults	determining a product's usability	implications of non-compliance
inaccessible privacy information	difficulty communicating with business leaders	in-house legal counsel
intrusive privacy defaults	difficulty balancing user needs and business requirements	lacking expertise
lack of awareness	difficulty conducting extensive UX processes	lacking funding
lack of awareness of worth of personal data	communicating UX efforts	lacking human labor
lack of concise privacy policies	communicating with business stakeholders	lacking knowledge
lack of transparent practices	educating users about business models	lacking resources
lack of transparent privacy policies	educating users about data monetization	lacking time
lack of trust	educating users about technology	manually authenticating users
learning about data rights	educating users about privacy	need for clear guidelines
making informed decisions	educating users about data protection	need for cost-effectiveness
managing consent	end-user compliance	need for government support
managing device permissions	experiencing complex conditions	not collecting personal data
manual data access requests	experiencing time pressure	outsourcing
need for anonymized data collection	experiencing work pressure	personal data mapping
need for brevity	feedback loops in production	prohibitive fines
need for personal data control	learning in production	purchasing services
need for transparency	learning about data protection guidance	regulatory fines
need for visualized privacy policies	making devices more conversational	responding to requests
not knowing how personal data was stored	on-going design approach	reviewing documentation
not understanding how smart homes work	over-provisioning devices	reviewing the legitimacy of requests
perceived ease of use	overcoming design challenges	right of access
perceived intrusion	raising awareness of user needs	right to be informed
perceived surveillance	raising awareness of privacy concerns	right to data portability
perceived usability	raising awareness of data protection requirements	right to erasure
perceived usefulness	representing and visualizing business viewpoints	right to object
perceived utility	representing and visualizing user viewpoints	right to rectification
positive experiences	researching data protection requirements	right to restrict processing
pressured consent interactions	researching privacy concerns	smaller businesses
privacy roadblocks	researching security concerns	strategic limitations
providing access to personal information	researching user pain points	taking necessary shortcuts
providing consent	satisficing conflicting opinions	tooling costs
security roadblocks	using design rules of thumb	training staff
unhelpful company responses	using heuristics	type of penalties non-compliance
unintelligible privacy information	using mental shortcuts	understanding requirements
unreliable smart home devices	using discount practices	unfair fines
using templates for data access requests	using best practices	using best practices
using third parties for data access requests	using tried-and-tested techniques	using common sense interpretations
vulnerable smart home devices	using usability testing	using own reasoning
withdrawing consent	using visualizations and graphs	using third parties

Table 4. Codebook (Grounded Theory).